ИЗМЕНЕНИЕ № 22/2143-Д-21 ДОГОВОРА ПРИСОЕДИНЕНИЯ

№ 22/2143-Д от 06 июля 2012 г.

на оказание услуг, составляющих
лицензируемую деятельность, в отношении шифровальных
(криптографических) средств

г. Москва «06» июня 2021 года

В соответствии с пунктом 3.3.1 настоящего договора присоединения Исполнитель вносит изменения (дополнения), которые являются неотъемлемой частью Договора присоединения. Все изменения (дополнения) в Договор вступают в силу и становятся обязательными по истечении 30 (тридцати) суток с даты размещения указанных изменений и дополнений на сайте Исполнителя. Текст Договора присоединения изменяется и излагается в следующей редакции:

Статья 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. Исполнитель – Акционерное общество «Гринатом» (АО «Гринатом»).
1.2. Заказчик – Предприятие/организация, присоединившееся к настоящему Договору в целом.
1.3. Договор – настоящий Договор присоединения на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, заключение которого осуществляется путем присоединения Заказчика в целом к условиям Договора в соответствии с статьей 428 Гражданского кодекса Российской Федерации.
1.4. Стороны – Исполнитель и Заказчик.
1.5. Заявление о присоединении – документ о присоединении Заказчика к настоящему Договору в целом, составленный по форме Приложения №1 к Договору.
1.6. Сайт Исполнителя – официальная страница Корпоративного удостоверяющего центра Госкорпорации «Росатом» в сети интернет - https://crypto.rosatom.ru.

Статья 2. ПРЕДМЕТ ДОГОВОРА

2.1. Исполнитель предоставляет Заказчику, а Заказчик обязуется принять и оплатить услуги, составляющие лицензируемую деятельность, в отношении шифровальных (криптографических) средств (далее по тексту «Услуги»), оказанные в соответствии с порядком и сроками, установленными Договором.

Статья 3. УСЛОВИЯ ДОГОВОРА ПРИСОЕДИНЕНИЯ

3.1. Присоединение к Договору.
3.1.1. Текст Договора опубликован на сайте Исполнителя
3.1.2. Заказчик присоединяется к Договору в целом.
3.1.3. Присоединение к настоящему Договору осуществляется путем подписания и предоставления Заказчиком Исполнителю двух экземпляров Заявления

о присоединении. Исполнитель, получивший Заявление о присоединении, акцептует Заявление о присоединении Заказчика, либо направляет отказ от акцепта (молчание Исполнителя не является акцептом).

3.1.4. Акцепт Заявления о присоединении происходит путем направления одного экземпляра Заявления о присоединении с отметкой о регистрации Исполнителем в адрес Заказчика. Дополнительно Исполнитель в течении 24 часов после регистрации Заявления о присоединении направляет скан - копию подписанного Заявления о присоединении по электронной почте или факсу, указанных в Заявлении о присоединении.

3.1.5. С даты регистрации и направления Исполнителем Заявления о присоединении, сторона, подавшая Заявление о присоединении, считается присоединившейся к Договору и является Стороной по Договору (Заказчик).

3.1.6. Исполнитель вправе отказать любому лицу в приёме и регистрации Заявления о присоединении. Отказ от акцепта Заявления о присоединении происходит путем возврата Исполнителем заявления о присоединении в адрес Заказчика с отметкой «Отказано в регистрации».

3.1.7. Факт присоединения стороны к Договору является принятием им условий настоящего Договора и всех его приложений в редакции, действующей на момент регистрации Заявления о присоединении в реестре Исполнителя. Заказчик принимает дальнейшие изменения (дополнения), вносимые в Договор и его приложения, в соответствии с условиями настоящего Договора.

3.1.8. После присоединения к Договору Стороны вступают в соответствующие договорные отношения на 10 (десять) лет, если ни одна из Сторон не выразит желание расторгнуть договор.

3.2. Расторжение Договора.

3.2.1. Действие настоящего Договора может быть досрочно прекращено по инициативе одной из Сторон в следующих случаях:

- по собственному желанию одной из Сторон;
- нарушения одной из Сторон условий настоящего Договора.

3.2.2. В случае расторжения Договора Сторона инициатор письменно уведомляет другую Сторону о своих намерениях за 30 (тридцать) календарных дней до даты расторжения Договора. Договор считается расторгнутым после выполнения Сторонами своих обязательств и проведения взаиморасчетов согласно условиям Договора.

3.2.3. Прекращение действия Договора или односторонний отказ от исполнения Договора согласно п.3.2.1 Договора или расторжение Договора по иным основаниям не освобождает Стороны от исполнения их обязательств по Договору, в том числе финансовых, возникших во время его действия и от ответственности за нарушение договорных обязательств, допущенные в период действия Договора.

3.2.4. В случае расторжения Договора Стороны предпринимают действия, определенные в Приложениях №2,3 к Договору.

3.3. Изменение (дополнения) Договора.

3.3.1. Внесение изменений (дополнений) в Договор, включая приложения к нему, производится Исполнителем.

3.3.2. Уведомление о внесении изменений (дополнений) в Договор осуществляется Исполнителем путем обязательного размещения указанных изменений (дополнений) на сайте Исполнителя.

3.3.3. Все изменения (дополнения), вносимые Исполнителем в Договор по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении тридцати календарных дней с даты размещения указанных изменений и дополнений в Договоре на сайте Исполнителя.

3.3.4. Все изменения (дополнения), вносимые Исполнителем в Договор в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

3.3.5. Любые изменения и дополнения в Договоре с момента вступления в силу равно распространяются на все Стороны, присоединившиеся к Договору, в том числе присоединившиеся к Договору ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) Сторона Договора имеет право до вступления в силу таких изменений (дополнений) на расторжение Договора в порядке, предусмотренном п.3.2. настоящего Договора.

3.3.6. Все приложения, изменения и дополнения к настоящему Договору являются его составной и неотъемлемой частью.

3.4. Применение Договора.

3.4.1. Стороны понимают термины, применяемые в настоящем Договоре, строго в контексте общего смысла Договора.

3.4.2. В случае противоречия и/или расхождения названия какого-либо раздела Договора со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

3.4.3. В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Договору с положениями собственно Договора, Стороны считают доминирующим смысл и формулировки Договора.

Статья 4. ПОРЯДОК ОКАЗАНИЯ УСЛУГ

4.1. Услуги оказываются после присоединения Заказчика к Договору.

4.2. Полный перечень, состав, стоимость и описание оказываемых Исполнителем Услуг указаны в Приложениях №2,3,5,6,7,8,9,12,13,14,16,17,18 к Договору.

4.3. Услуги оказываются в соответствии с Регламентом и Порядками услуг.

4.4. Заказчик самостоятельно определяет вид и объем запрашиваемых услуг исходя из потребности в обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации (далее – СКЗИ) конфиденциальной информации Заказчика и обеспечения ключевой документацией.

4.5. Заказчик вправе выбрать способ оказания услуг:

- без использования Информационной системы Органа криптографической защиты и Платформы доверенных сервисов Госкорпорации «Росатом», Порядками оказания услуг (Приложения № 2,3,6,7) и Регламентом (Приложение №16);

- с использованием Информационной системы органа криптографической защиты, Порядки оказания услуг (Приложения №8,9), при условии предоставления листа исполнения Приложение №11 и присоединении к соглашению о применении простой и усиленной неквалифицированной электронных подписей в Информационной системе органа криптографической защиты АО «Гринатом» в соответствии с Приложением №10;
- с использованием Платформы доверенных сервисов Госкорпорации «Росатом», Порядки оказания услуг (Приложения №12,13,14,17,18), при условии предоставления листа исполнения Приложение №11 и присоединении к соглашению об использовании усиленной неквалифицированной электронной подписи в соответствии с Приложением №15.

4.6. Расчетной датой начала оказания услуг является дата регистрации оригиналов заявлений, определяющих вид и объем запрашиваемых Заказчиком услуг.

Статья 5. ПРАВА И ОБЯЗАННОСТИ СТОРОН

5.1. Права и Обязанности Исполнителя:

5.1.1. Исполнитель имеет право запрашивать и получать от Заказчика любую документацию, информацию, разъяснения либо подтверждения, если такая информация, разъяснения либо подтверждения необходимы Исполнителю для надлежащего выполнения своих обязательств в соответствии с Регламентом и Порядками оказания услуг в согласованные Сторонами сроки. Ответственность за полноту, актуальность и достоверность передаваемой Заказчиком информации по Договору возлагается на Заказчика.

5.1.2. Исполнитель имеет право контролировать организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, а также соблюдение условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ.

5.1.3. Исполнитель обязуется своевременно и качественно оказывать Услуги в соответствии со Статьей 2 Договора.

5.1.4. Исполнитель обязуется информировать Заказчика о результат всех видов контроля, анализировать причины выявленных недостатков, разрабатывать меры по их профилактике, контролировать выполнение рекомендаций, содержащихся в актах проверок.

5.2. Права и Обязанности Заказчика:

5.2.1. Заказчик имеет право запрашивать и получать от Исполнителя надлежащим образом заверенные копии документов, подтверждающие наличие у него специальных разрешений (лицензий).

5.2.2. Заказчик имеет право запрашивать от Исполнителя проведение контрольных мероприятий за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

5.2.3. Заказчик имеет право передать СКЗИ своему правопреемнику при реорганизации юридического лица (слияние, присоединение, разделение, выделение, преобразование) по Акту приема-передачи, согласовав передачу

с Исполнителем, если информация в полученных ранее сертификатах и схеме криптографической защиты не изменяется.

5.2.4. Если при реорганизации юридического лица (слияние, присоединение, разделение, выделение, преобразование) информация в полученных ранее сертификатах и схеме криптографической защиты становится недостоверной, то Заказчик обязан уничтожить все выданные Исполнителем СКЗИ и предоставить Исполнителю заявления об аннулировании сертификатов. В случае отсутствия заявления об аннулировании сертификатов Исполнитель аннулирует сертификаты и отзывает лицензии на СКЗИ с даты получения официальных документов о реорганизации юридического лица (слияние, присоединение, разделение, выделение, преобразование) Заказчика.

5.2.5. В случае прекращения деятельности Заказчик обязан предоставить Исполнителю заявление об аннулировании сертификатов до момента внесения в единый государственный реестр юридических лиц записи о прекращении деятельности Заказчика.

5.2.6. Заказчик обязуется не препятствовать проведению контроля Исполнителем за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

5.2.7. В рамках действующего Договора Заказчик обязан выполнять указания соответствующих органов криптографической защиты по всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

5.2.8. Заказчик обязуется в установленные Договором сроки принимать и оплачивать оказанные Услуги в соответствии с порядком и сроками, установленными Договором.

5.2.9. Заказчик обязуется соблюдать условия Договора при пользовании Услугами, предоставляемыми Исполнителем.

5.3. Стороны обязуются незамедлительно информировать друг друга об обстоятельствах, препятствующих надлежащему исполнению обязательств по Договору для своевременного принятия необходимых мер и устранения имеющихся недостатков. В случае если непредставление информации о таких обстоятельствах привело к возникновению неблагоприятных имущественных последствий у одной из Сторон, то такие неблагоприятные последствия относятся на Сторону, нарушившую такую обязанность.

Статья 6. ПОРЯДОК ПОДТВЕРЖДЕНИЯ ВЫПОЛНЕНИЯ ОБЯЗАТЕЛЬСТВ

6.1. Заказчик осуществляет приёмку оказанных Услуг в соответствии с Договором, в порядке, установленном настоящей Статьей.

6.2. Отчётным периодом оказания Услуг является календарный квартал.

6.3. Исполнитель, после оказания Услуг представляет Заказчику Акт сдачи-приемки оказанных Услуг по форме, указанной в Приложении №4 к Договору (далее по тексту – «Акт») в двух экземплярах, подписанный со стороны Исполнителя, а также счёт-фактуру и счёт на сумму, причитающуюся к уплате Исполнителю, в срок, не позднее 2 (второго) рабочего дня месяца, следующего за отчётным периодом оказания Услуг.

6.4. Заказчик, не позднее 5 (пяти) рабочих дней после получения документов согласно п. 6.3. Договора, обязан рассмотреть и подписать Акт и направить Исполнителю один экземпляр подписанного Акта, либо направить Исполнителю в письменном виде обоснованный (мотивированный) отказ от подписания Акта.

6.5. В случае отказа от подписания Акта Заказчик обязан обосновать свой отказ, указав на несоответствие оказанных Исполнителем Услуг условиям Договора и действующему законодательству Российской Федерации. В этом случае Заказчик обязан направить Исполнителю перечень обнаруженных несоответствий.

6.6. В случае необоснованного (немотивированного) отказа Заказчика от подписания или не подписания Заказчиком Акта в указанный срок с момента его получения Заказчиком, Акт, подписанный лишь Исполнителем, признается надлежаще оформленным, подтверждает выполнение Исполнителем обязательств, а оказанные Исполнителем Услуги в соответствии с Договором будут считаться принятыми Заказчиком на дату истечения срока, предусмотренного п. 6.4. Договора.

6.7. Заказчик обязан выслать дополнительно скан - копию подписанного Акта по электронной почте, указанной в Статье 14 Договора в течение 1(одного) рабочего дня с даты подписания.

6.8. В случае признания Исполнителем мотивированного отказа Заказчика от подписания Акта, Исполнитель обязуется за свой счет устранить причины мотивированного отказа. После исправления обнаруженных несоответствий Исполнителем, повторная приемка услуг Заказчиком производится в порядке, предусмотренном в п.п. 6.3, 6.4 Договора. При невозможности для Сторон достичь соглашения, споры рассматриваются в соответствии со Статьей 10 Договора.

6.9. Услуги считаются принятыми с момента подписания Акта, либо истечения срока для предоставления мотивированного отказа, установленного в п. 6.4. Договора.

Статья 7. СТОИМОСТЬ И ОПЛАТА УСЛУГ

7.1. Стоимость Услуг, оказываемых Исполнителем по Договору, установлена в Приложении № 5 к Договору.

7.2. Исполнитель устанавливает расчётный период с 21 числа предыдущего отчётного периоду месяца по 20 число последнего месяца текущего отчётного периода.

7.3. Стоимость Услуг, оказываемых Исполнителем в соответствии с условиями Договора, включает в себя все издержки, расходы и вознаграждение Исполнителя.

7.4. В случае оказания Услуг в течение неполного календарного квартала стоимость Услуг за оказанный период рассчитывается пропорционально количеству календарных дней, в течение которых Исполнитель оказывал Услуги Заказчику, за исключением единовременно оказываемых Услуг.

7.5. Оплата оказываемых по Договору Услуг осуществляется Заказчиком путем перечисления денежных средств на расчетный счет Исполнителя на основании выставленного Исполнителем счета на оплату в соответствии с п. 6.3. Договора в течение 10 (десяти) рабочих дней с момента подписания Акта.

7.6. Обязанность Заказчика по оплате Услуг Исполнителю по Договору считается исполненной надлежащим образом с даты поступления соответствующих денежных средств на корреспондентский счет банка Исполнителя.

7.7. В случае неисполнения или ненадлежащего исполнения Заказчиком п.7.5 настоящего Договора Исполнитель вправе приостановить действие всех сертификатов и СКЗИ Заказчика до устранения нарушений, письменно уведомив об этом Заказчика за 3 (три) рабочих дня до момента приостановки оказания Услуг.

7.8. Восстановление (возобновление) оказания Услуг производится Исполнителем в течение суток с даты поступления денежных средств на расчётный счёт Исполнителя при условии предоставления документов, подтверждающих оплату Услуг в полном объёме.

7.9. Стороны по состоянию на конец календарного года проводят сверку расчетов. Заказчик, в течение 5 (пяти) календарных дней со дня получения Акта сверки расчетов от Исполнителя обязан его подписать или направить протокол расхождений с приложенным встречным Актом сверки расчетов

Статья 8. КОНФИДЕНЦИАЛЬНОСТЬ

8.1. Передача информации ограниченного доступа между Сторонами может осуществляться только после подписания Соглашения (Договора) о конфиденциальности.

Статья 9. ОТВЕТСТВЕННОСТЬ СТОРОН

9.1. Стороны не несут ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Договору, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Договора своих обязательств.

9.2. Исполнитель не несет ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Договору, а также возникшие в связи с этим убытки в случае, если Исполнитель обоснованно полагался на сведения, указанные Стороной, присоединившейся к Договору.

9.3. Исполнитель несет ответственность за убытки при использовании ключа электронной подписи и сертификата ключа проверки электронной подписи только в случае, если данные убытки возникли при компрометации ключа подписи Корпоративного Удостоверяющего центра Госкорпорации «Росатом».

9.4. В случае невозможности исполнения обязательств по Договору, возникшей по вине Заказчика, Заказчик обязан выплатить Исполнителю вознаграждение за Услуги по Договору, фактически оказанных на момент установления невозможности дальнейшего исполнения обязательств, в согласованном Сторонами размере.

9.5. Предел ответственности Исполнителя перед Заказчиком относительно выполнения или невыполнения Исполнителем своих обязательств по Договору, или каким-либо иным образом связанной с Договором, по любым и всем претензиям, ограничивается возмещением реального доказанного ущерба. Данное ограничение ответственности не применяется в отношении обязательств Исполнителя в связи с нарушением Исполнителем условий конфиденциальности. Ни одна из Сторон не отвечает

за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

9.6. По обязательствам в отношении конфиденциальной информации обе Стороны несут полную ответственность в соответствии с Соглашением о конфиденциальности и действующим законодательством Российской Федерации.

9.7. Стороны освобождаются от ответственности за полное или частичное неисполнение обязательств по Договору, если они явились следствием действия обстоятельств непреодолимой силы, носящих чрезвычайный и непредотвратимый в данных конкретных условиях характер, которые соответствующая Сторона по объективным причинам не могла предвидеть, предотвратить либо контролировать. При этом освобождение от ответственности, предусмотренное настоящим пунктом Договора, распространяется лишь на тот период, в течение которого действуют обстоятельства непреодолимой силы. Если обстоятельства непреодолимой силы длятся свыше тридцати календарных дней, то Стороны обязуются провести переговоры с целью урегулирования данной проблемы приемлемым для обеих Сторон образом.

9.8. Исполнитель не несет ответственности за изменение требований органов государственной власти к совместимости со средствами электронной подписи органов государственной власти, форматам сертификатов ключа проверки электронной подписи, и возникшей в этой связи невозможности использования сертификатов ключа проверки электронной подписи в соответствующей области правоотношений.

9.9. Исполнитель не несет ответственность и не возмещает убытки Заказчика или третьих лиц в случае не выполнения Заказчиком законодательства Российской Федерации, регулирующего порядок, правила обработки, передачи и хранения персональных данных работников Заказчика в целях исполнения условий настоящего Договора.

Статья 10. РАЗРЕШЕНИЕ СПОРОВ

10.1. В случае возникновения споров между Заказчиком и Исполнителем, относящихся к настоящему Договору, Стороны приложат максимум усилий для урегулирования спора путем переговоров уполномоченных представителей или руководителей Сторон.

10.2. Если одна из Сторон имеет к другой Стороне обоснованные претензии по выполнению обязательств по настоящему Договору, то ответственное лицо такой Стороны в срок не позднее 5 (пяти) рабочих дней с момента возникновения спорной ситуации излагает суть претензий в письменном виде, на которые ответственное лицо другой Стороны в срок до 5-ти (пяти) рабочих дней с момента получения претензии должно дать либо аргументированный ответ, либо согласовать срок устранения замечаний со Стороной, направившей претензию.

10.3. Споры и разногласия, возникающие по настоящему Договору или в связи с ним, решаются Сторонами, прежде всего путем переговоров в соответствии с действующим законодательством Российской Федерации.

10.4. Любой спор, разногласие или претензия, вытекающие из настоящего Договора и возникающие в связи с ним, в том числе связанные с его нарушением, заключением, изменением, прекращением или недействительностью, разрешаются путем арбитража, администрируемого Российским арбитражным центром при автономной некоммерческой организации «Российский институт современного арбитража» в соответствии с Правилами Отделения Российского арбитражного центра при автономной некоммерческой организации «Российский институт современного арбитража» по разрешению споров в атомной отрасли.

Стороны соглашаются, что для целей направления письменных заявлений, сообщений и иных письменных документов будут использоваться следующие адреса электронной почты:

Исполнитель: адрес, указанный в ст. 14 Договора.

Заказчик: адрес, указанный в Приложении №1 к Договору.

В случае изменения указанного выше адреса электронной почты Сторона обязуется незамедлительно сообщить о таком изменении другой Стороне, а в случае, если арбитраж уже начат, также Отделению Российского арбитражного центра при автономной некоммерческой организации «Российский институт современного арбитража» по разрешению споров в атомной отрасли. В ином случае Сторона несет все негативные последствия направления письменных заявлений, сообщений и иных письменных документов по неактуальному адресу электронной почты.

Стороны принимают на себя обязанность добровольно исполнять арбитражное решение.

Стороны прямо соглашаются, что в случае, если заявление об отводе арбитра не было удовлетворено Президиумом Российского арбитражного центра в соответствии с Правилами Отделения Российского арбитражного центра при автономной некоммерческой организации «Российский институт современного арбитража» по разрешению споров в атомной отрасли, Сторона, заявляющая отвод, не вправе подавать в компетентный суд заявление об удовлетворении отвода.

Стороны прямо соглашаются, что в случае, если Состав арбитража выносит постановление о наличии у него компетенции в качестве вопроса предварительного характера, Стороны не вправе подавать в компетентный суд заявление об отсутствии у Состава арбитража компетенции.

Стороны прямо соглашаются, что арбитражное решение является окончательным для Сторон и отмене не подлежит.

В случаях, предусмотренных статьёй 25 Правил Отделения Российского арбитражного центра при автономной некоммерческой организации «Российский институт современного арбитража» по разрешению споров в атомной отрасли, Сторонами может быть заключено соглашение о рассмотрении спора в рамках ускоренной процедуры арбитража

10.5. Сторона, намеренная передать спор в указанный суд, должна письменно уведомить об этом, а также о предмете спора другую Сторону за 10 (десять) рабочих дней до подачи исковых материалов в суд.

Статья 11. ИНЫЕ УСЛОВИЯ

11.1. Если в течение срока действия Договора одно либо несколько установленных им положений становятся недействительными (ничтожными), либо не имеющими юридической силы в соответствии с законодательством Российской Федерации, то это обстоятельство не делает недействительными (ничтожными) либо не имеющими юридической силы иные положения Договора, который продолжает действовать в соответствующей части, но может служить основанием для пересмотра Договора целиком либо его отдельных частей.

11.2. Стороны обязуются предоставлять друг другу в полном объеме информацию в случаях изменения реквизитов, организационной структуры, формы собственности и прочих условий, имеющих влияние на порядок оказания Услуг по Договору, в срок не позднее 3 (трех) рабочих дней с даты вступления в силу соответствующих изменений путем направления сообщения на электронный адрес другой Стороны, указанный в Статье 14 Договора.

11.3. Стороны гарантируют друг другу и несут ответственность за полноту, точность и актуализацию предоставленных в Единой отраслевой системе управления нормативно – справочной информацией (ЕОС НСИ) сведений в отношении всей цепочки собственников и руководителей, включая бенефициаров (в том числе конечных).

11.4. При исполнении настоящего Договора Стороны соблюдают и будут соблюдать в дальнейшем все применимые законы и нормативные акты, включая любые законы о противодействии взяточничеству и коррупции.

11.5. Стороны и любые их должностные лица, работники, акционеры, представители, агенты, или любые лица, действующие от имени или в интересах или по просьбе какой либо из Сторон в связи с настоящим Договором, не будут прямо или косвенно, в рамках деловых отношений в сфере предпринимательской деятельности или в рамках деловых отношений с государственным сектором, предлагать, вручать или осуществлять, а также соглашаться на предложение, вручение или осуществление (самостоятельно или в согласии с другими лицами) какого-либо платежа, подарка или иной привилегии с целью исполнения (воздержания от исполнения) каких-либо условий настоящего Договора, если указанные действия нарушают применимые законы или нормативные акты о противодействии взяточничеству и коррупции.

Статья 12. НОРМАТИВНЫЕ ДОКУМЕНТЫ

12.1. Стороны действуют на основании:

– Постановления Правительства Российской Федерации от 16 апреля 2012 г. № 313 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);

- Федерального закона Российской Федерации от 06.04.2011 № 63-ФЗ "Об электронной подписи";
- Приказа ФАПСИ РФ от 13.06.2001 № 152 «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»;
- Приказа Госкорпорации «Росатом» от 25.10.2011 № 1/910-П «Об организации Корпоративного удостоверяющего центра Госкорпорации «Росатом».
- Приказа Госкорпорации «Росатом» от 09.01.2019 №1/4-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию ограниченного распространения (с пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации «Росатом» и ее организациях».

Статья 13. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ К ДОГОВОРУ

Приложение №1. Форма заявления о присоединении к Договору на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств.

Приложение №2. Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом».

Приложение №3. Порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Приложение №4. Форма Акта сдачи-приемки оказанных Услуг.

Приложение №5. Перечень и стоимость услуг Исполнителя.

Приложение №6. Порядок контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем

Приложение №7. Порядок организации и обслуживания защищённой сети комплекса «ViPNet-Гринатом».

Приложение №8. Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с использованием информационной системы Органа криптографической защиты».

Приложение №9. Порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну с использованием информационной системы Органа криптографической защиты.
Приложение №10. Соглашение о применении простой и усиленной неквалифицированной электронных подписей в информационной системе органа криптографической защиты АО «Гринатом».

Приложение №11. Лист исполнения.

Приложение №12. Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом».

Приложение №13. Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом».

Приложение №14. Порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну с использованием Платформы доверенных сервисов Госкорпорации «Росатом».

Приложение №15. Соглашение об использовании усиленной квалифицированной электронной подписи.

Приложение №16. Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом»).

Приложение №17. Порядок применения усиленной квалифицированной электронной подписи.

Приложение №18. Порядок применения усиленной неквалифицированной электронной подписи.

Статья 14. ЮРИДИЧЕСКИЙ АДРЕС И БАНКОВСКИЕ РЕКВИЗИТЫ ИСПОЛНИТЕЛЯ

Полное наименование: Акционерное общество «Гринатом»

Место нахождения: 119017, Россия, г. Москва, ул. Большая Ордынка, дом 24

Почтовый адрес: 115114, Россия, г. Москва, 1-й Нагатинский проезд, дом 10, стр. 1

ОГРН: 1097746819720

ИНН: 7706729736

КПП: 770601001

Расчетный счет: 40702810038110013312

Банк: Московский банк Сбербанка России ПАО

Корреспондентский счет: 30101810400000000225 в ОПЕРУ Московского ГТУ Банка России

БИК: 044525225

ОКПО: 64509942

ОКАТО: 45286596000

ОКТМО: 45384000

Телефон: +7 (499) 949-49-19

Адрес электронной почты: dogovor@greenatom.ru

От Исполнителя:

Директор по информационным технологиям

АО «Гринатом»

_____А.Н. Киселёв

М.П.

Приложение № 1
к Договору присоединения № 22/2143-Д от 06 июля 2012 г.

Заявление о присоединении к Договору на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств

_____

_____

(наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

Действующего на основании _____

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяется к Договору на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, условия которого определены АО «Гринатом» и опубликованы на сайте по адресу https://crypto.rosatom.ru

С Договором на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Уполномоченное должностное лицо

_____ _____ / _____ /

М.П. (подпись) (ФИО)

Реквизиты организации:

Полное наименование:
Место нахождения:
Почтовый адрес:
ОГРН:
ИНН:
КПП:
Расчетный счет:
Банк:
Кор. счет:
БИК:
ОКПО:
ОКТМО:
ОКАТО:
Телефон/факс:
e-mail:

Данное Заявление о присоединении к Договору на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств зарегистрировано в реестре АО «Гринатом»

Заявление о присоединении к Договору подается Исполнителю в двух экземплярах. После регистрации Заявления у Исполнителя один экземпляр предоставляется заявителю.

Регистрационный № _____ от «____» _____ 20___ г.

Директор по информационным технологиям _____ А.Н. Киселёв

М.П.

Приложение № 2 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю

Директор по информационным технологиям

АО «Гринатом»

_____ / А.Н. Киселёв /

М.П.

ПОРЯДОК

предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

Москва 2020 г.

Содержание

1. Назначение и область применения

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

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

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

Руководитель предприятия/организации;

Пользователь КУЦ;

Доверенное лицо КУЦ;

Оператор КУЦ;

Администратор КУЦ;

Комиссия КУЦ;

Руководитель КУЦ.

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

Порядок 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 №0014254 Рег.№15686 Н от 19.01.2017 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических)	Действует	Лицензия	Волков С.П.

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

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	Волков С.П.
Приказ Министерства связи и массовых коммуникаций РФ от 23 ноября 2011 г. № 320 “Об аккредитации удостоверяющих центров”	Действует	Приказ	Волков С.П.
Порядок организации и обеспечения 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	Порядок	Волков С.П.
Инструкция оператора КУЦ	Действует	Порядок	Волков С.П.
Порядок подтверждения подлинности электронной подписи в электронном документе	Действует	Порядок	Волков С.П.

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 OCSP запроса
		Предоставление TSP запроса
		Предоставление официальной информации для принятия решения КУЦ

2.	Создание сертификата	
3.	Аннулирование сертификата	
4.	Подтверждение получения сертификата	
5.	Подтверждение подлинности ЭП в ЭД	
6.	Предоставление сервиса OCSP	
7.	Предоставление сервиса TSP	
8.	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 удостоверяющего центра	признание уполномоченным федеральным 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
СОС	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;
- 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 подтверждение подлинности электронной подписи в электронном документе	Руководитель предприятия	Корпорация
4.	Копия сертификата ключа проверки электронной подписи на бумажном носителе	Пользователь КУЦ	Корпорация
5.	Скан-копия сертификата ключа проверки электронной подписи на бумажном носителе	Пользователь КУЦ	Корпорация
6.	OCSP запрос	Пользователь КУЦ	Корпорация
7.	TSP запрос	Пользователь КУЦ	Корпорация
8.	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	Пользователь КУЦ	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления
	сертификатом, Конверт с пин-кодом и парольной фразой и руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.		
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, 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;
- 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 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;
- 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 подтверждения подлинности ЭП в ЭД Пользователь КУЦ подготавливает и отправляет в адрес КУЦ Заявление на подтверждение подлинности электронной подписи в электронном документе (Приложение №9).

Для подтверждения факта получения сертификата Пользователь КУЦ отправляет подписанную копию сертификата ключа проверки электронной подписи (Приложение №10).

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;
- 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 подтверждения подлинности ЭП в ЭД Пользователь КУЦ подготавливает и отправляет в адрес КУЦ «Заявление на подтверждение подлинности электронной подписи в электронном документе» (Приложение №9).

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 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.

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 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».

Электронные адреса обращения к Службе актуальных статусов сертификатов КУЦ:

http://ocsp1.rosatom.ru/ocsp/ocsp.srf	http://ocsp1.rosatom.ru/ocsp2/ocsp.srf	http://ocsp1.rosatom.ru/ocsp3/ocsp.srf
http://ocsp2.rosatom.ru/ocsp/ocsp.srf	http://ocsp2.rosatom.ru/ocsp2/ocsp.srf	http://ocsp2.rosatom.ru/ocsp3/ocsp.srf
http://ocsp1.rosatom.local/ocsp/ocsp.srf	http://ocsp1.rosatom.local/ocsp2/ocsp.srf	http://ocsp1.rosatom.local/ocsp3/ocsp.srf
http://ocsp2.rosatom.local/ocsp/ocsp.srf	http://ocsp2.rosatom.local/ocsp2/ocsp.srf	http://ocsp2.rosatom.local/ocsp3/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».

3.5.1.6 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)».

Электронные адреса обращения к Службе штампов времени КУЦ:

http://tsp1.rosatom.ru/tsp/tsp.srf	http://tsp1.rosatom.ru/tsp2/tsp.srf	http://tsp1.rosatom.ru/tsp3/tsp.srf
http://tsp2.rosatom.ru/tsp/tsp.srf	http://tsp2.rosatom.ru/tsp2/tsp.srf	http://tsp2.rosatom.ru/tsp3/tsp.srf
http://tsp1.rosatom.local/tsp/tsp.srf	http://tsp1.rosatom.local/tsp2/tsp.srf	http://tsp1.rosatom.local/tsp3/tsp.srf
http://tsp2.rosatom.local/tsp/tsp.srf	http://tsp2.rosatom.local/tsp2/tsp.srf	http://tsp2.rosatom.local/tsp3/tsp.srf

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

3.5.1.7 Процедура «Предоставление официальной информации для принятия решения КУЦ»

Руководитель КУЦ при получении информации о том, что сертификат содержит недостоверную информацию, принимает решение об 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 аннулировать сертификат 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 аннулирования сертификата Оператор КУЦ сообщает Пользователю КУЦ о наступлении события, повлекшего аннулирование сертификата.

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 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;
- 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 «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.

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.

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.

3.5.5 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.

3.5.6 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».

3.5.7 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»

3.5.8 Подпроцесс «Получение информации из КУЦ»

Данный подпроцесс регламентирует порядок получения информации из КУЦ после создания сертификата, аннулирования 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 подпроцесса «Аннулирование сертификата».

Входящая информация поступает из подпроцесса «Аннулирование сертификата».

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

Официальным уведомлением о факте аннулирования сертификата является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об отозванном сертификате, и изданного не ранее времени наступления произошедшего случая. Временем аннулирования 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», «Аннулирования 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 Порядок процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом».

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

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

6. Контроль и ответственность

6.1 Контроль выполнения требований Порядка

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 Порядка

За несоблюдение Порядка 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 №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.

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 решению КУЦ»		О		Инф	К	О
1.6. Процедура «Предоставление информации OCSP»					О	К
1.7. 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 «Получение информации доверенным лицом»		Инф	О	О	К	
2.4. Процедура «Получение информации		Инф		О	К	

Спецсвязью России»						
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 «Подтверждение подлинности ключа проверки электронной подписи»				О	О	К
7. Подпроцесс «Сервис OCSP»					О	К
8. Подпроцесс «Сервис TSP»					О	К

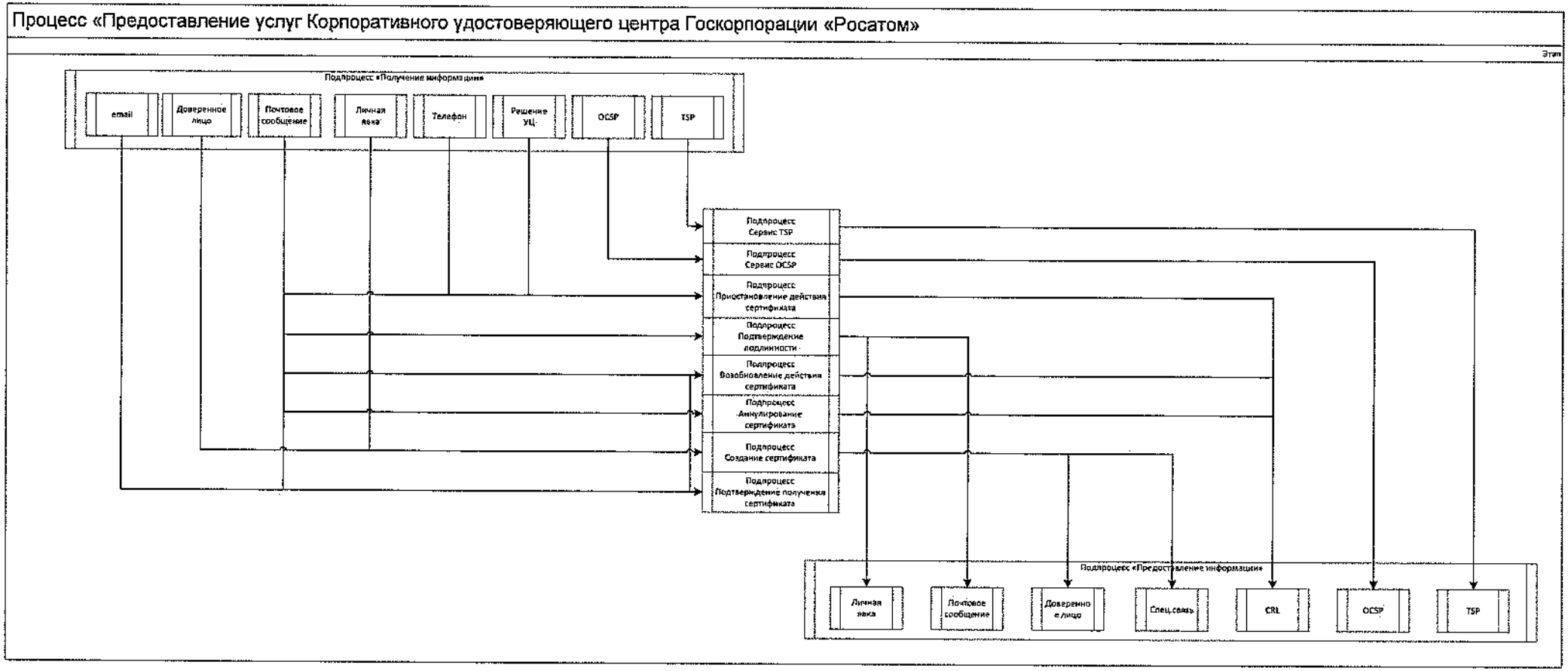
Название (включая сокращение названия) и определение ролей в матрице распределения ответственности и полномочий справочно приведено в таблице ниже:

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	Структурное подразделение

Сокра-щение	Название роли	Определение	Исполнитель Роли
		выполнения и достижения результатов подпроцесса/процедуры	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

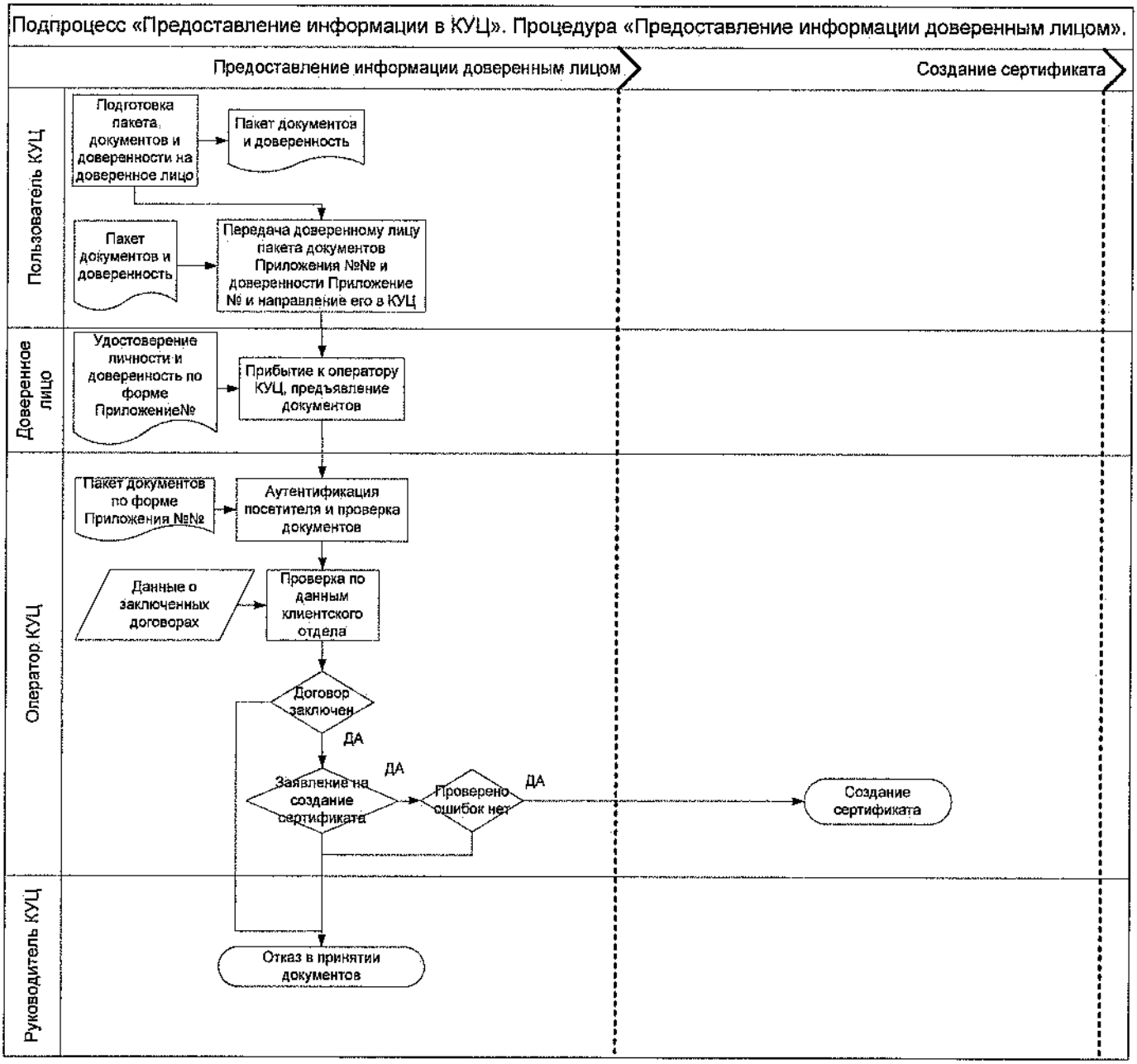
Приложение №2

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

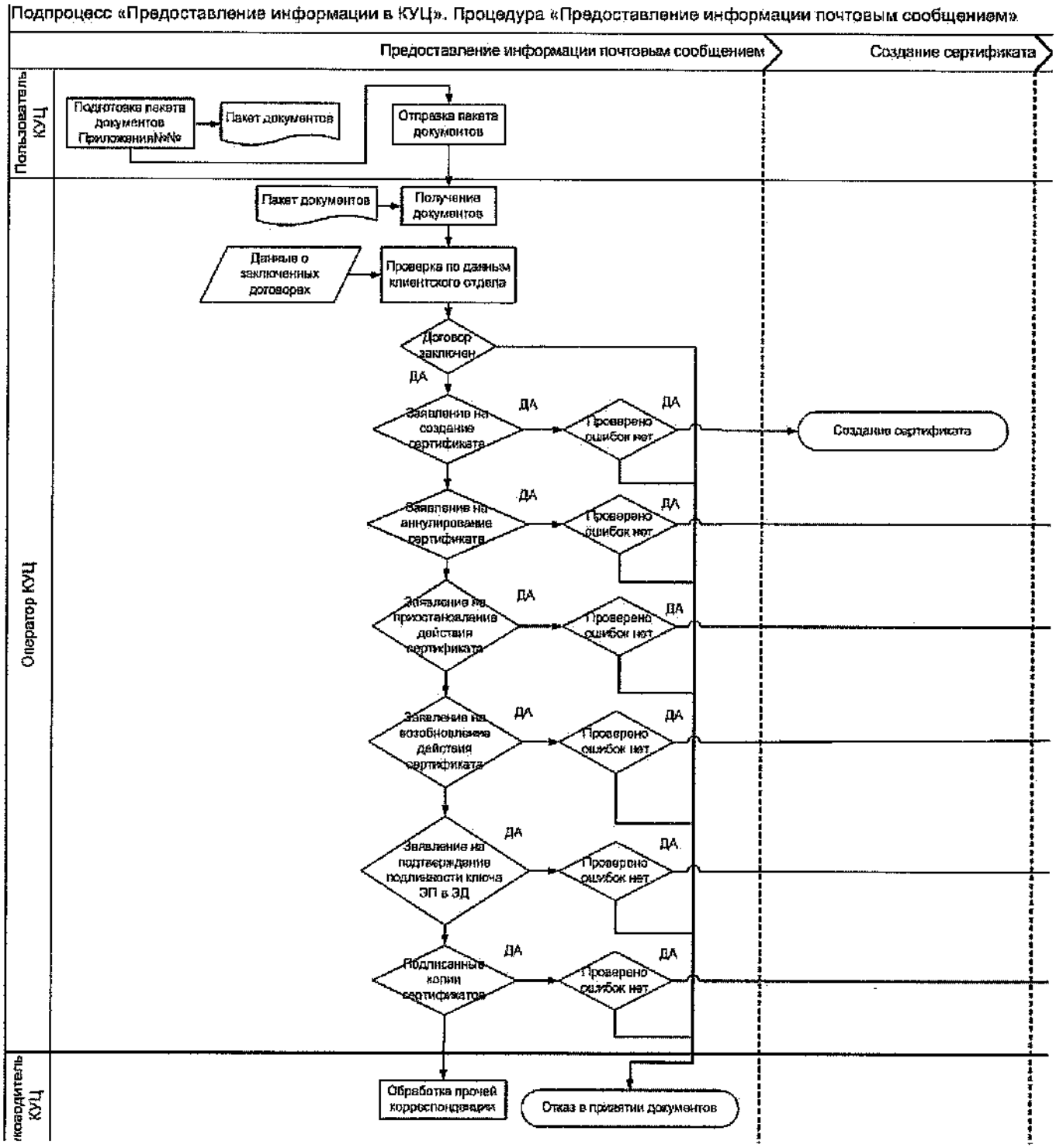


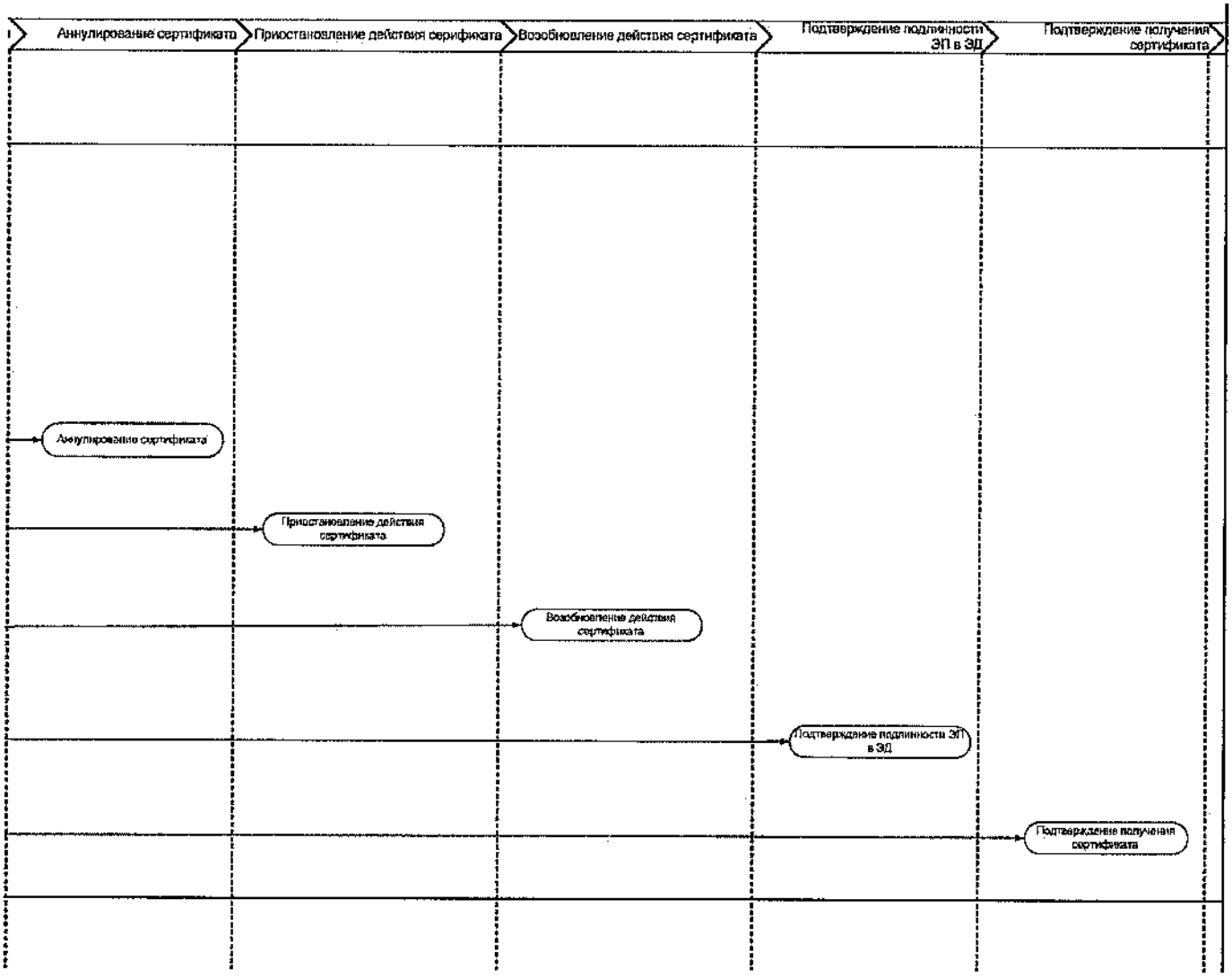
1. Подпроцесс «Предоставление информации в КУЦ»:

а) Схема процедуры «Предоставление информации доверенным лицом»:

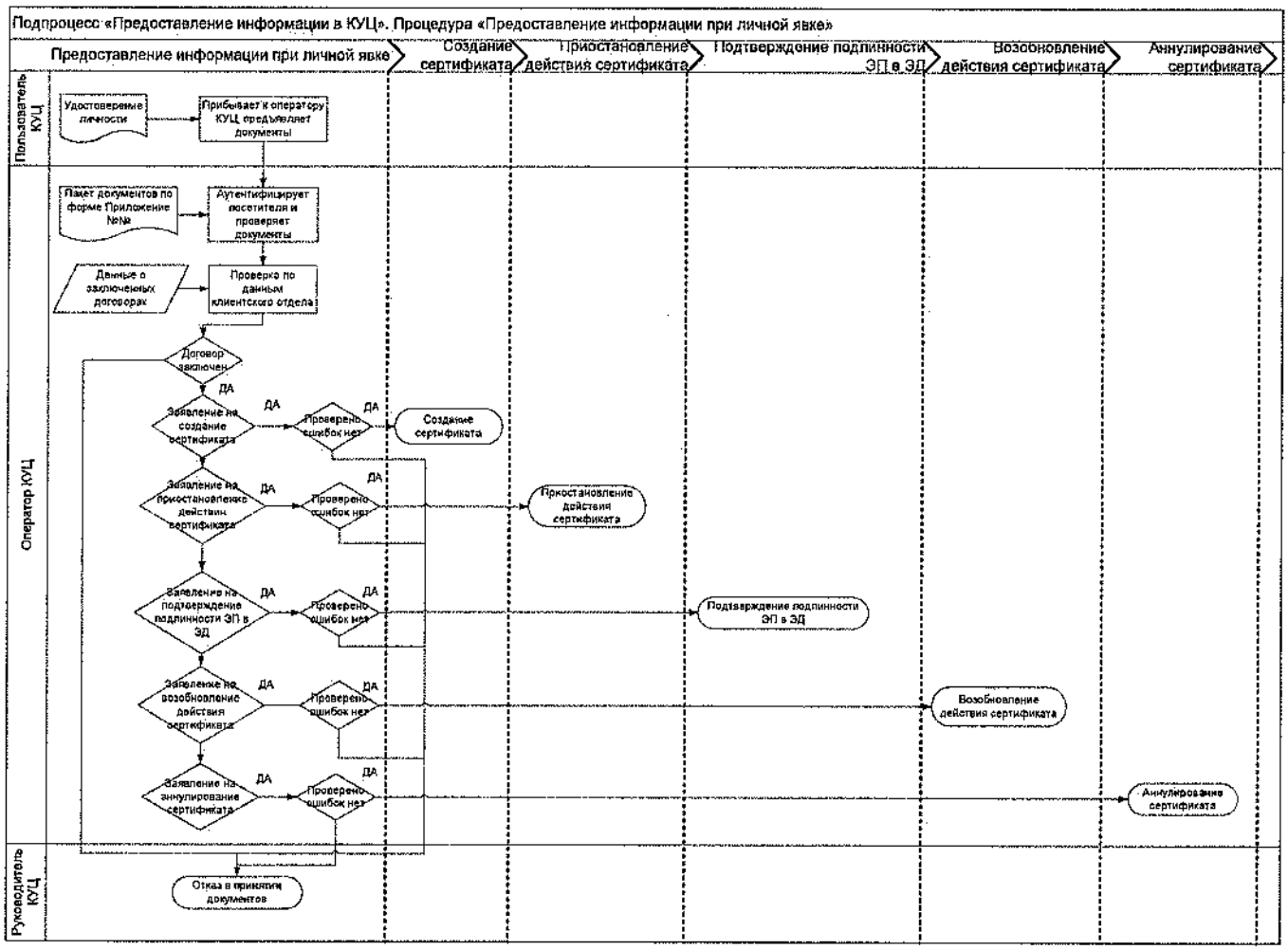


b) Схема процедуры «Предоставление информации почтовым сообщением»:

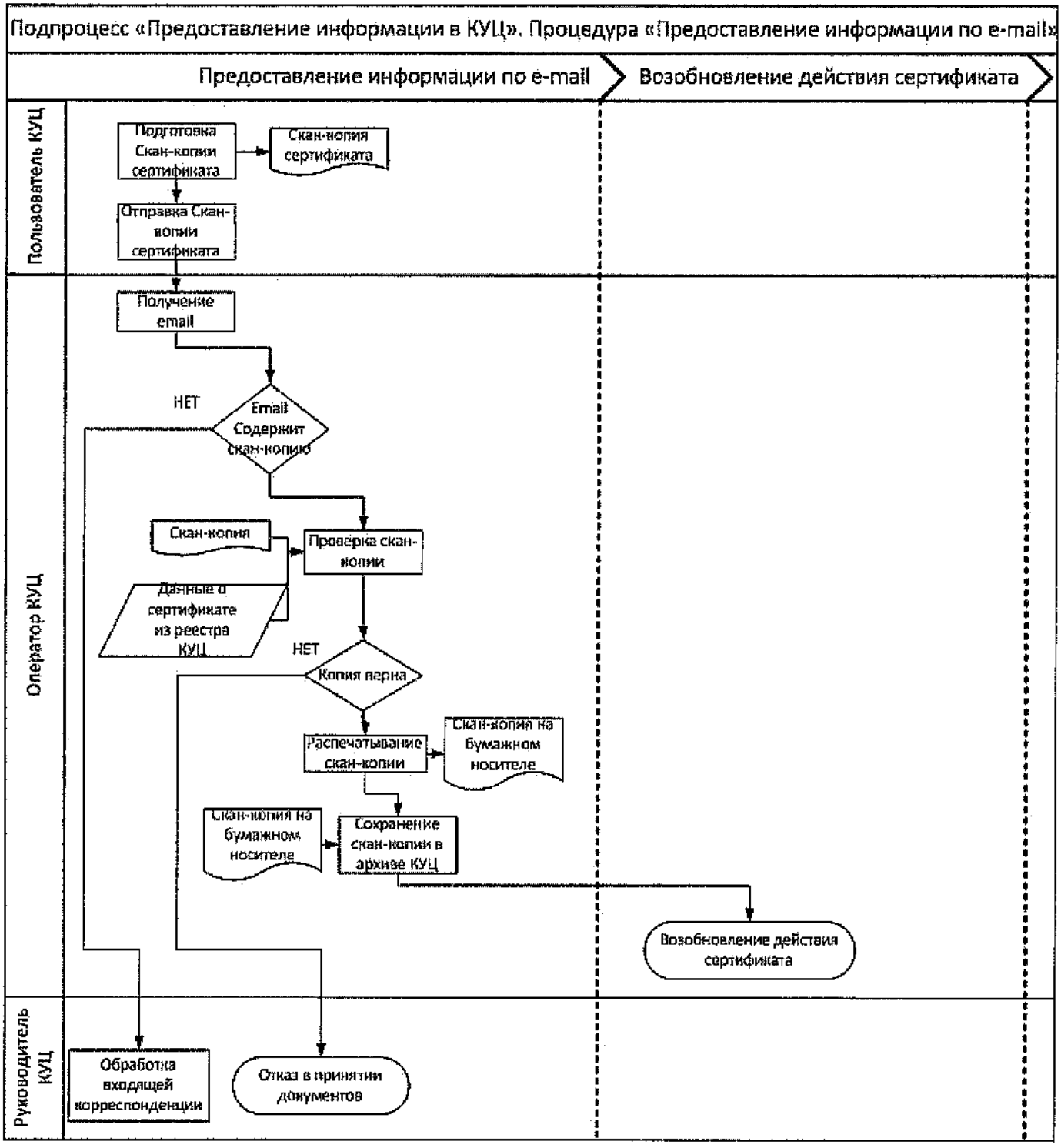



Аннулирование сертификата
Приостановление действия сертификата
Возобновление действия сертификата
Подтверждение подлинности ЭП в ЭД
Подтверждение получения сертификата
Аннулирование сертификата
Приостановление действия сертификата
Возобновление действия сертификата
Подтверждение подлинности ЭП в ЭД
Подтверждение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

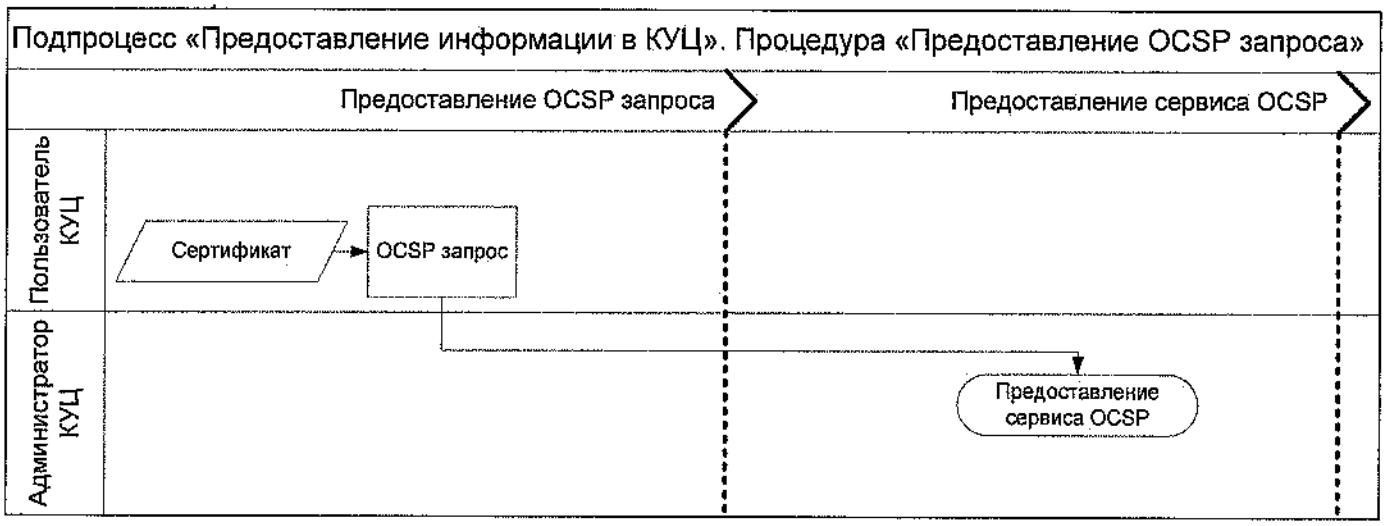
c) Схема процедуры «Предоставление информации при личной явке»:



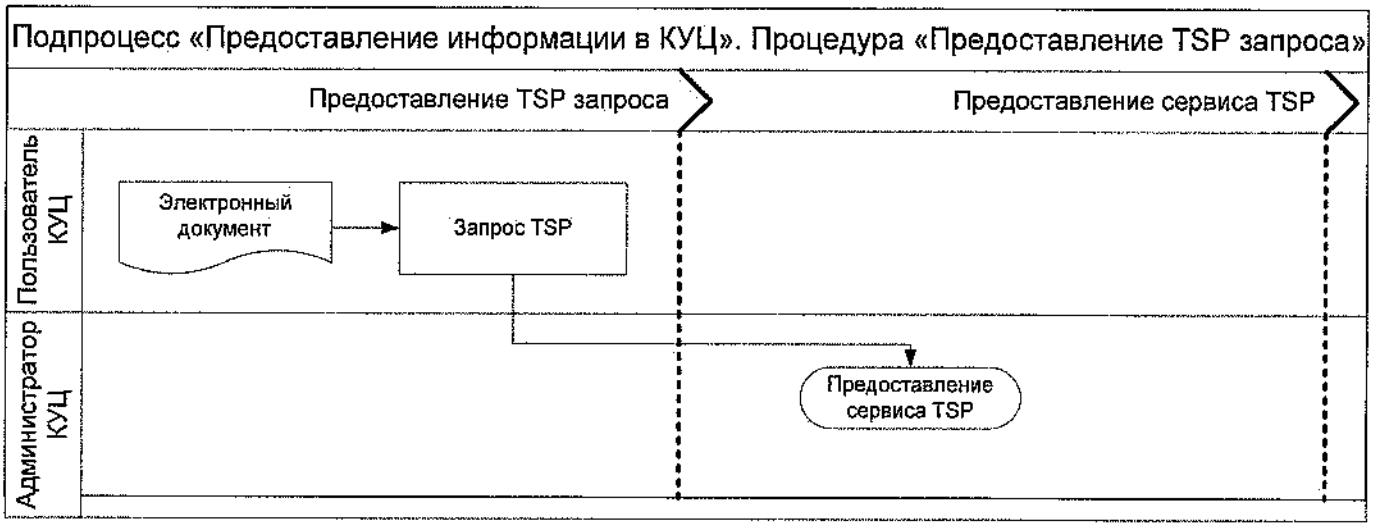
d) Схема процедуры « Предоставление информации по e-mail»:



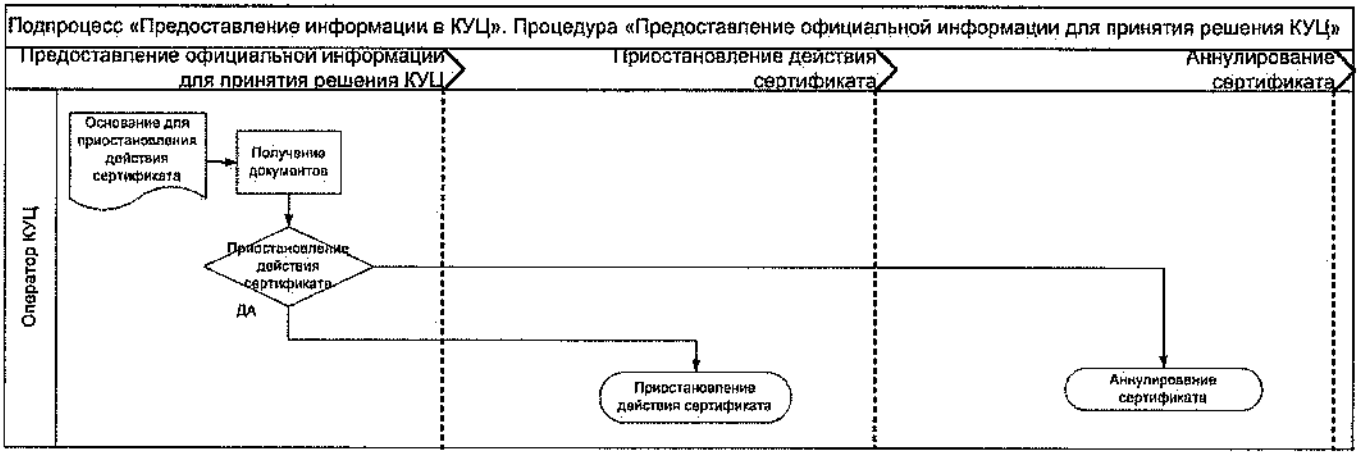
e) Схема процедуры «Предоставление OCSP запроса»:



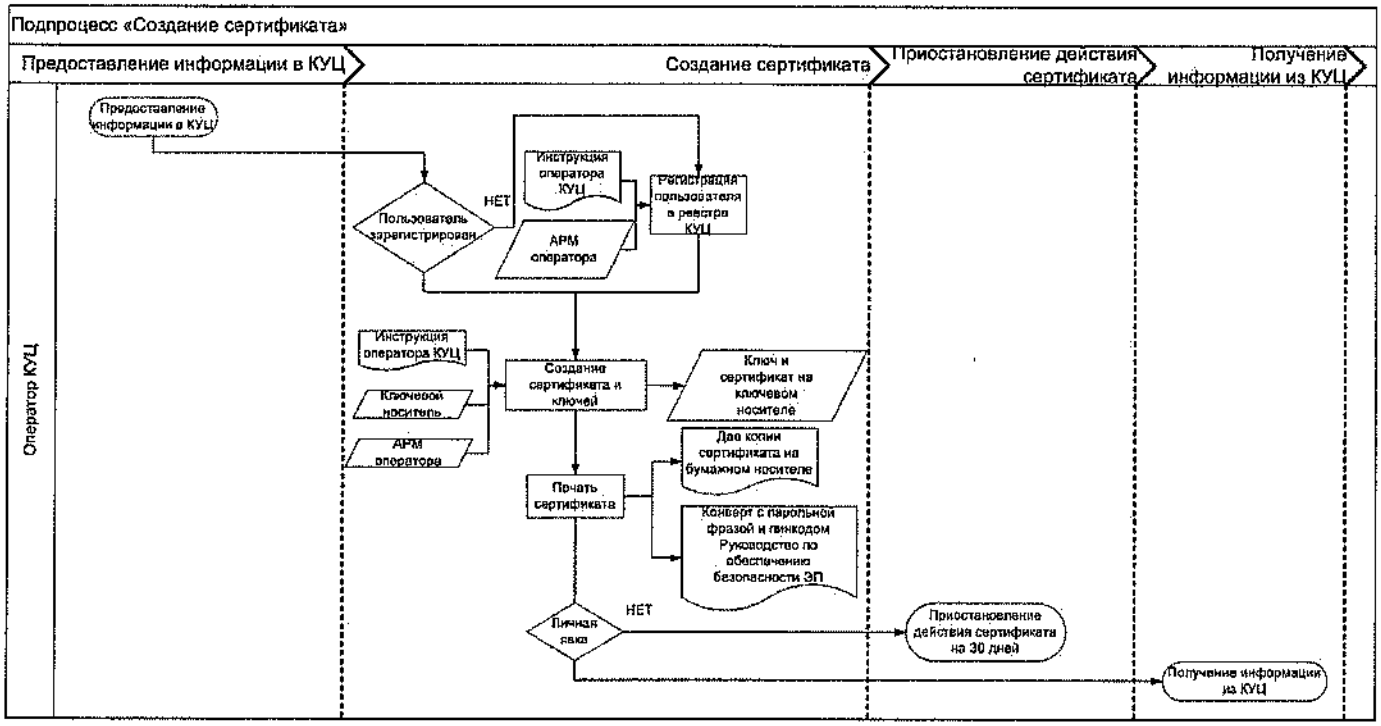
f) Схема процедуры «Предоставление TSP запроса»:



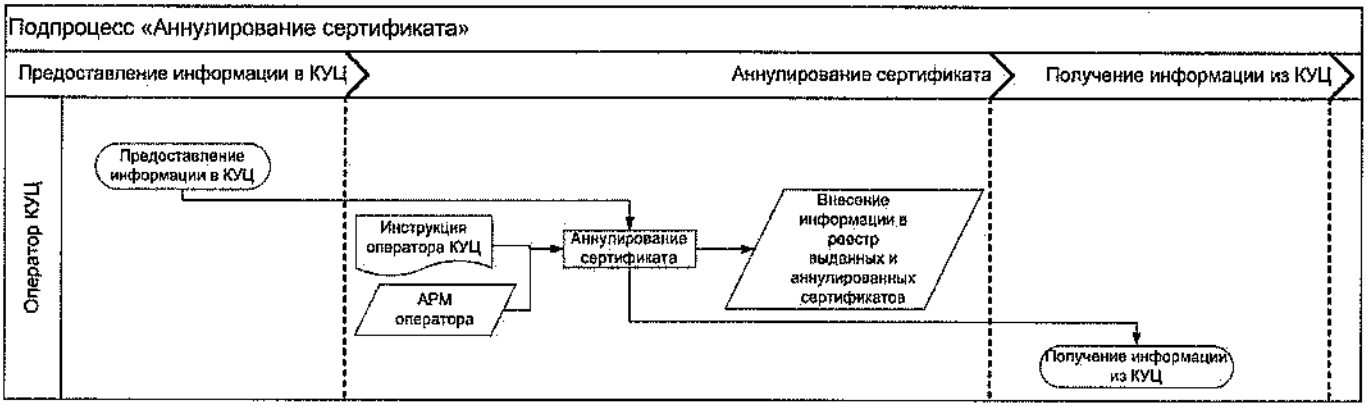
g) Схема процедуры «Предоставление официальной информации для принятия решения КУЦ»:



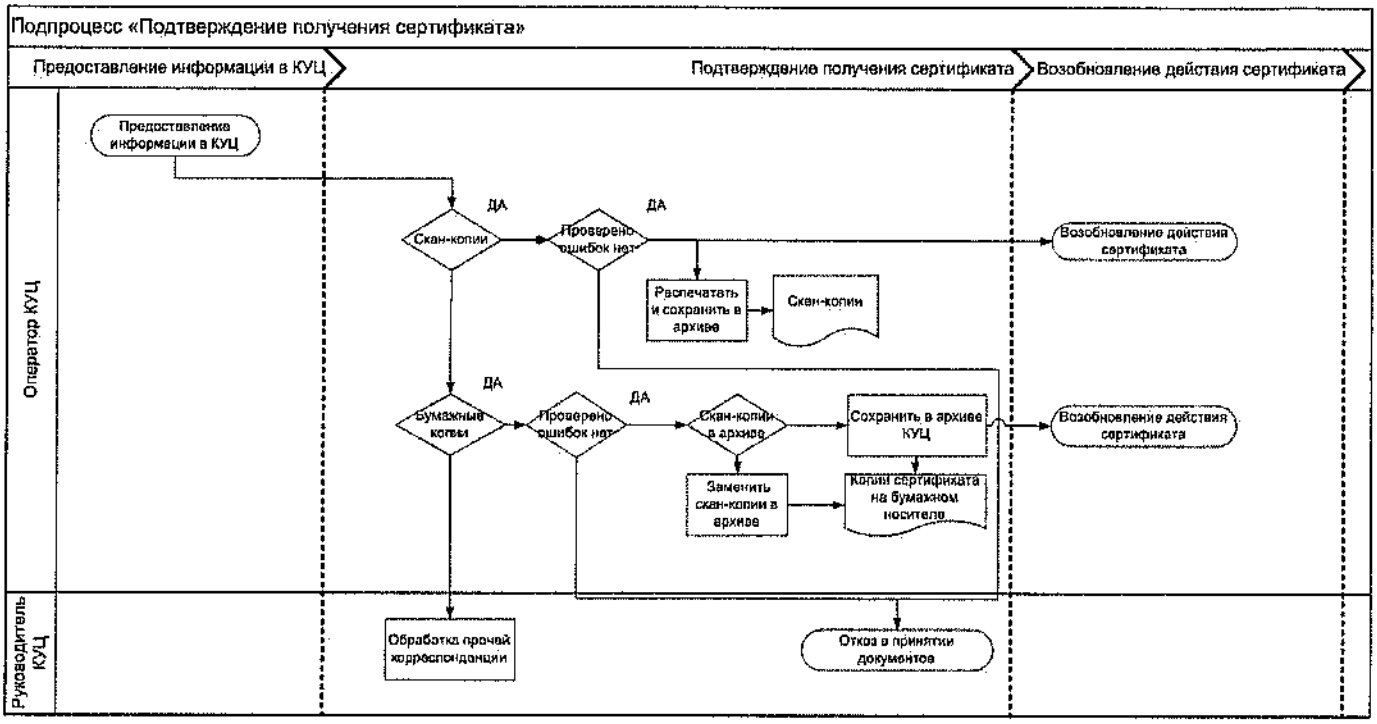
2. Схема подпроцесса «Создание сертификата»:



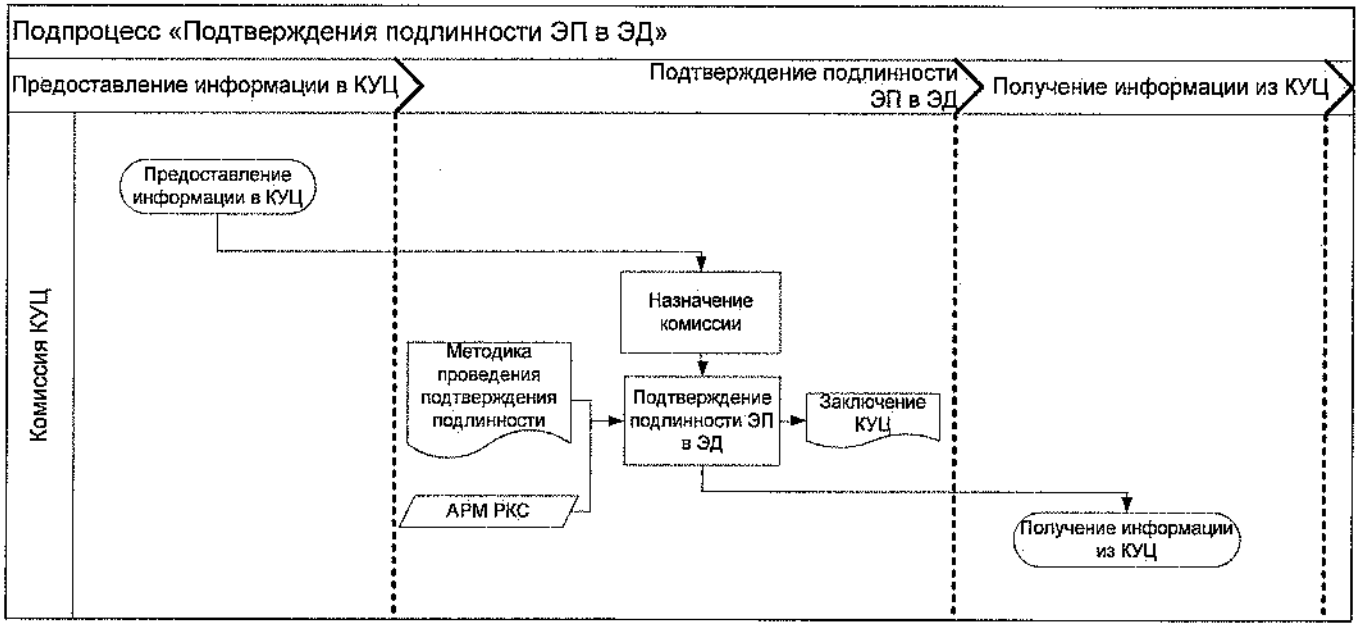
3. Схема подпроцесса «Аннулирование сертификата»:



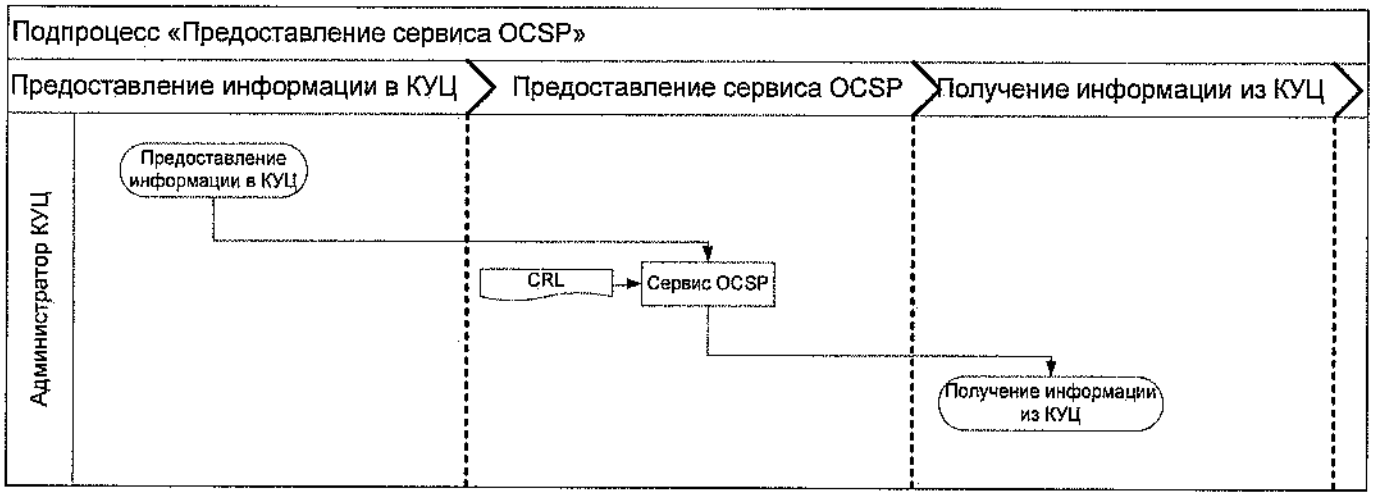
4. Схема подпроцесса «Подтверждение получения сертификата»:



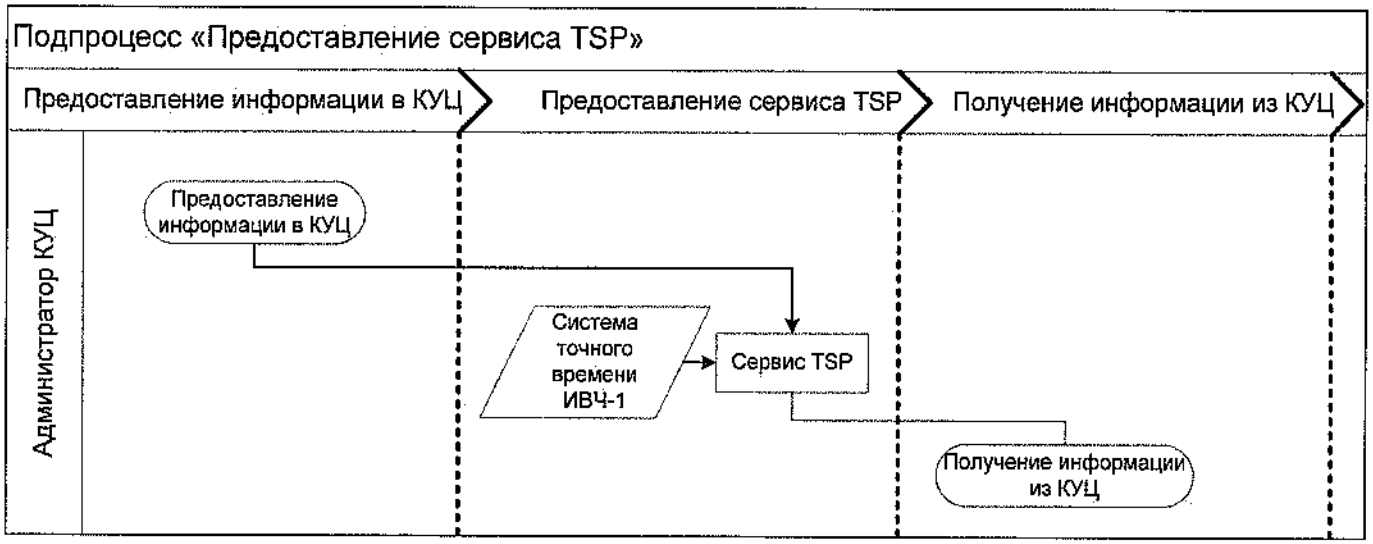
5. Схема подпроцесса «Подтверждение подлинности ЭП в ЭД»:



6. Схема подпроцесса «Предоставление сервиса OCSP»:

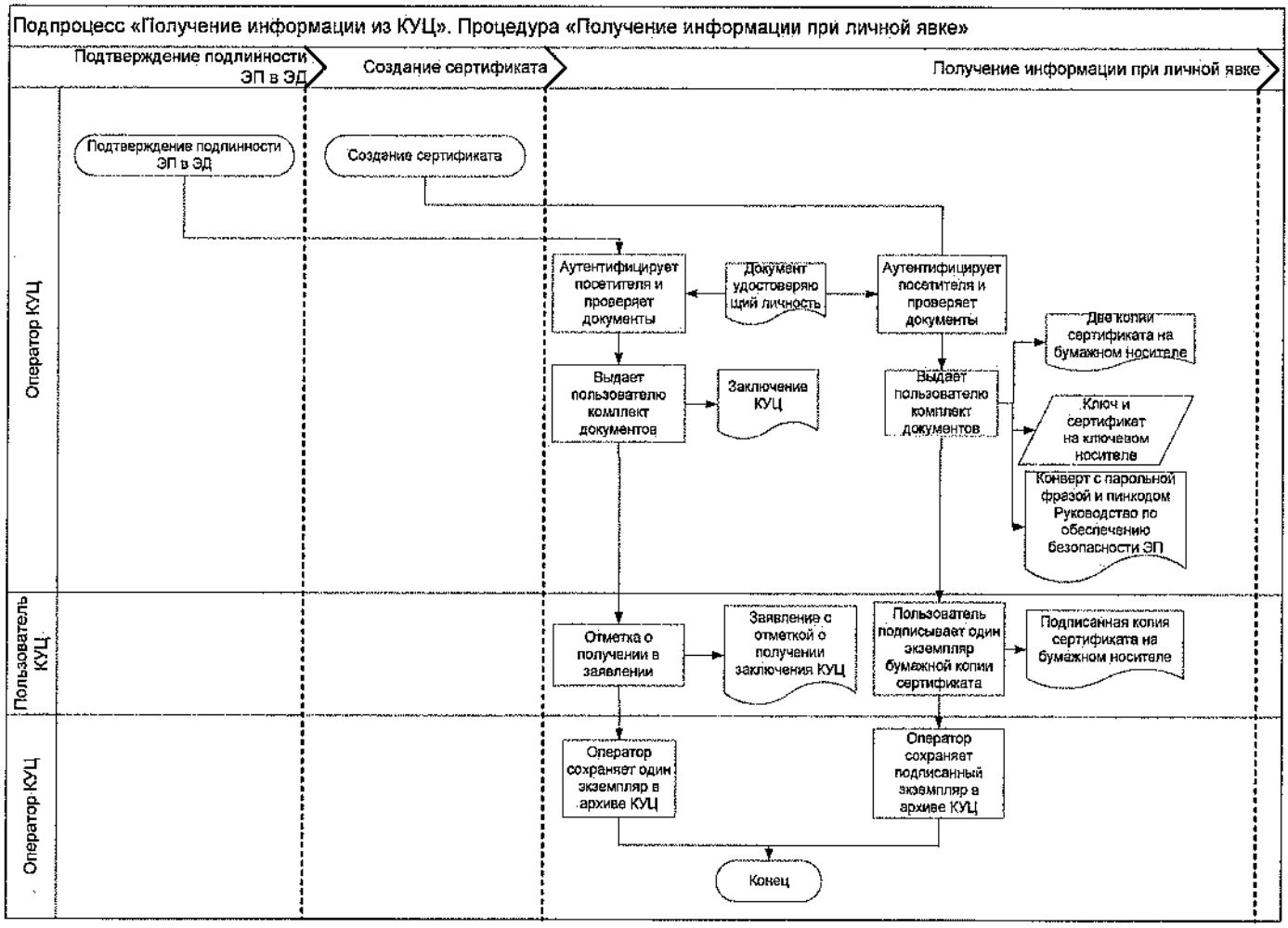


7. Схема подпроцесса «Предоставление сервиса TSP»:

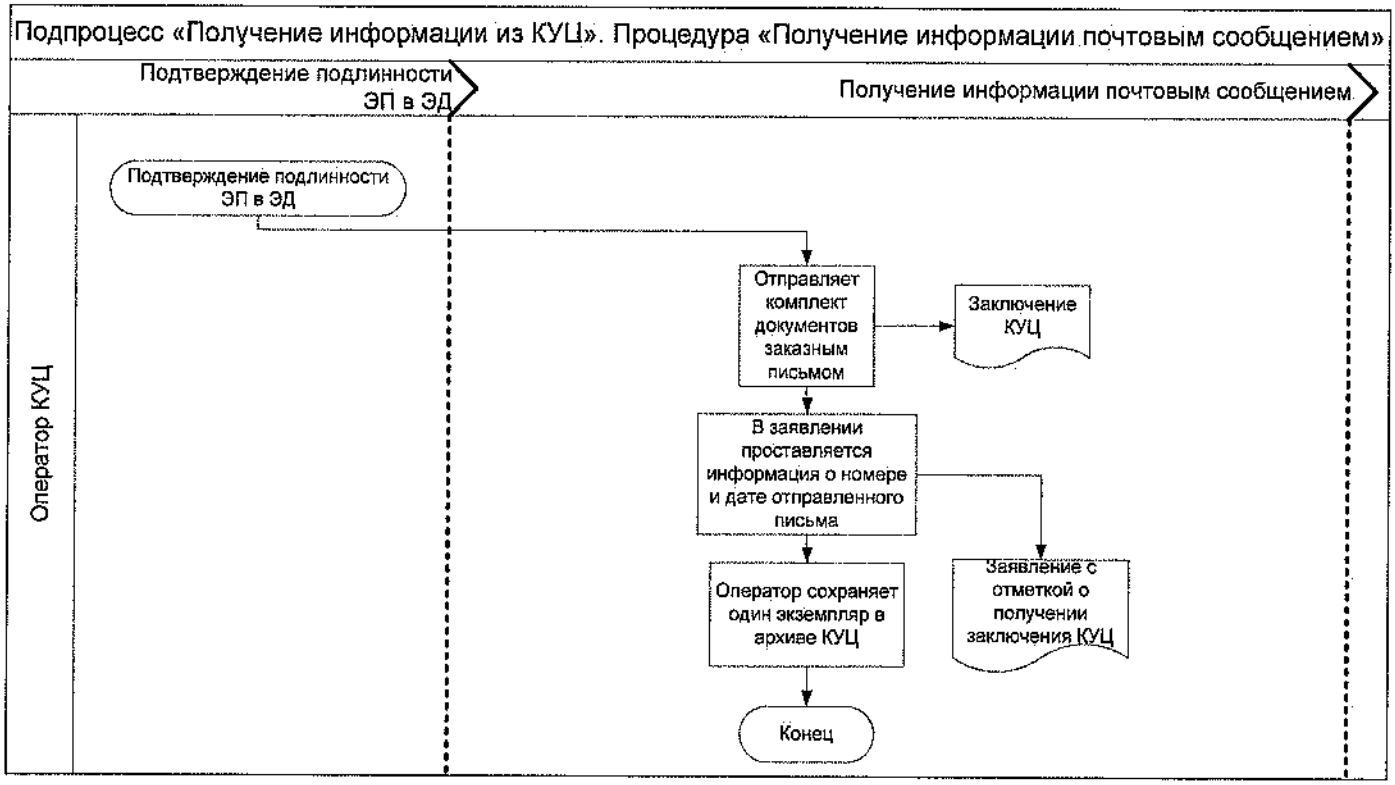


8. Подпроцесс «Получение информации из КУЦ»:

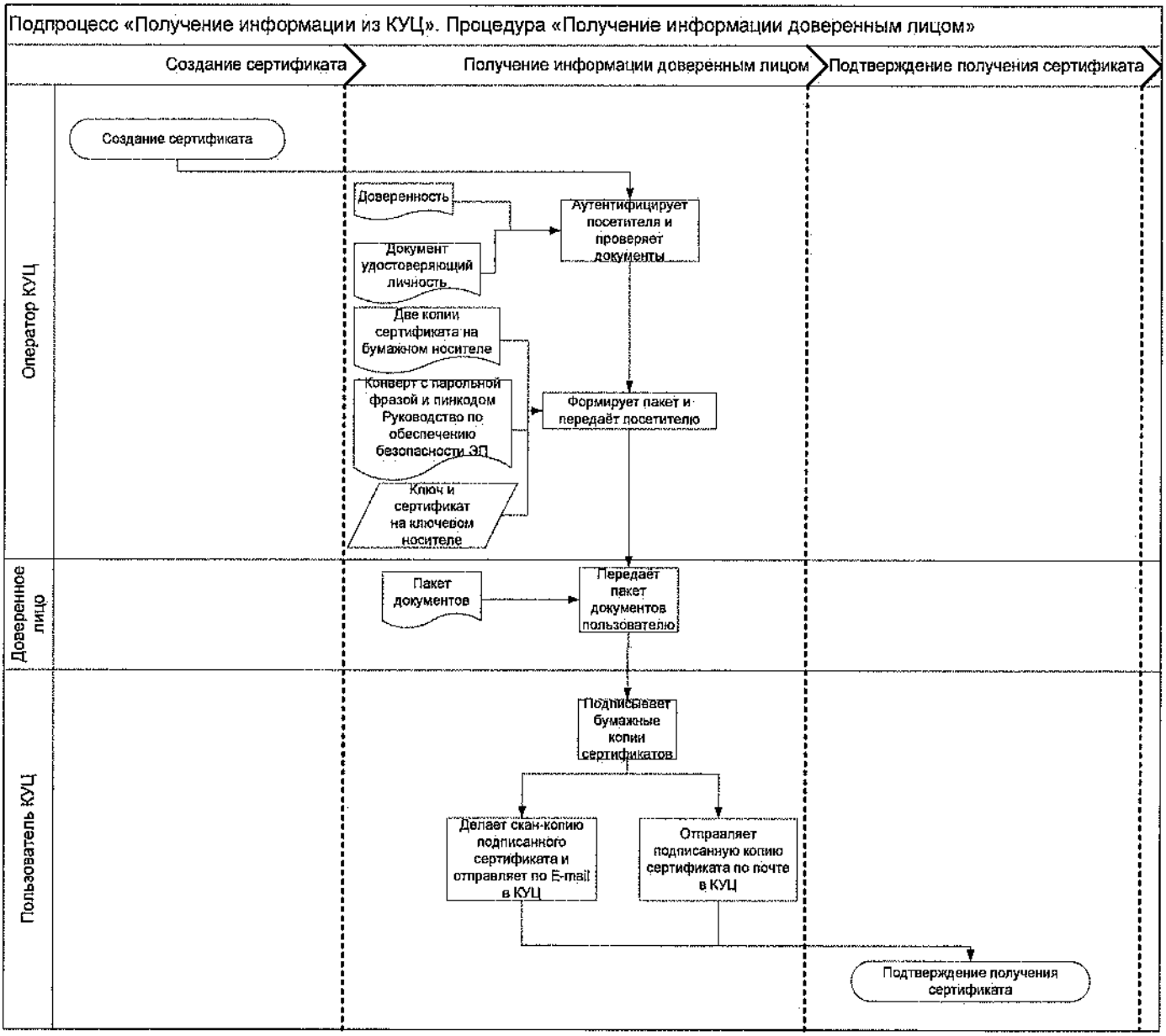
а) Схема процедуры «Получение информации при личной явке»:



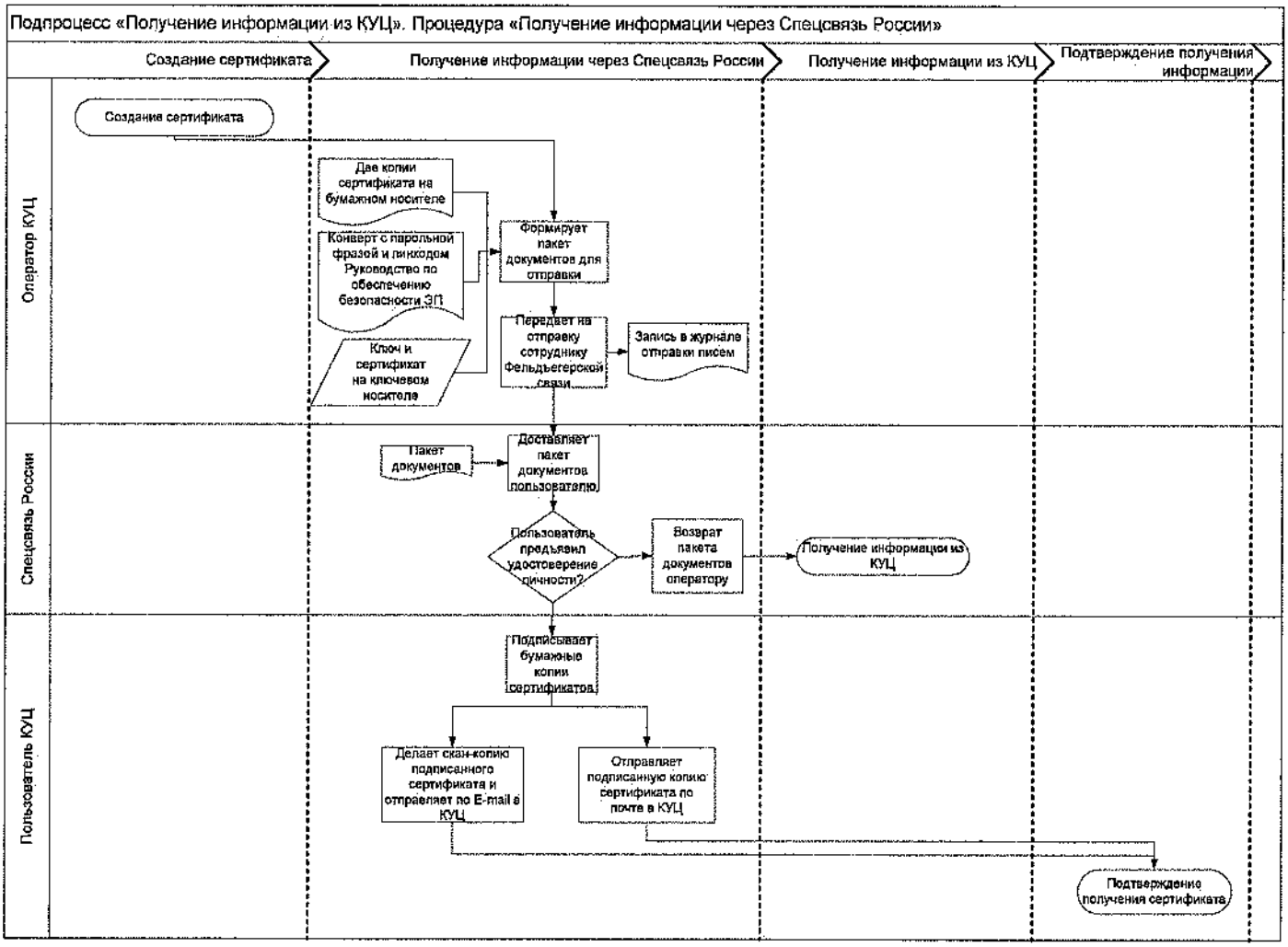
b) Схема процедуры «Получение информации почтовым сообщением»:



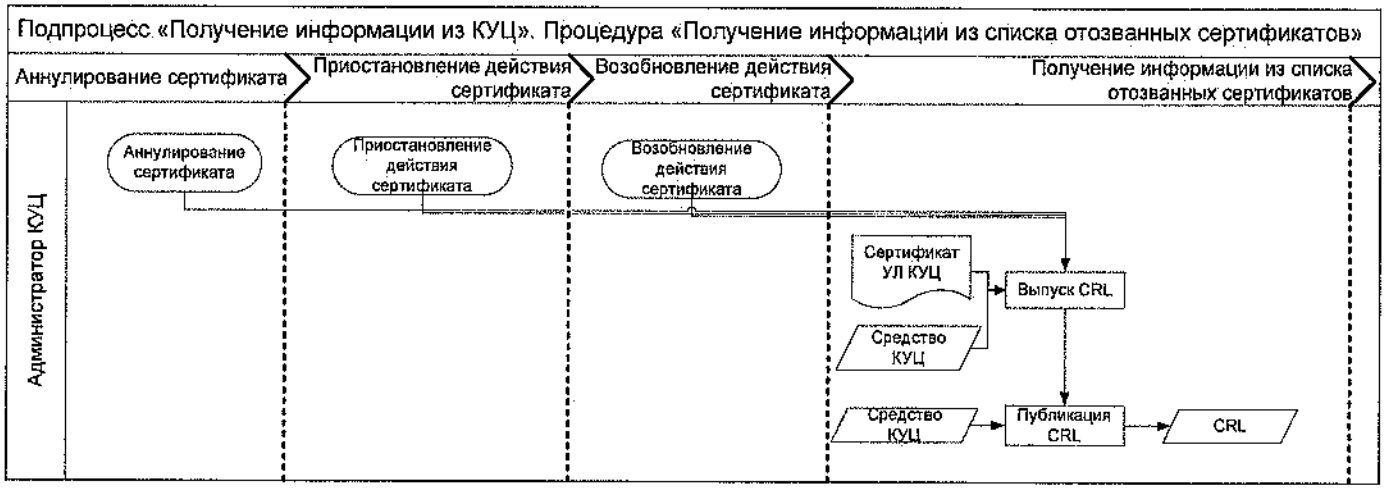
с) Схема процедуры «Получение информации доверенным лицом»:



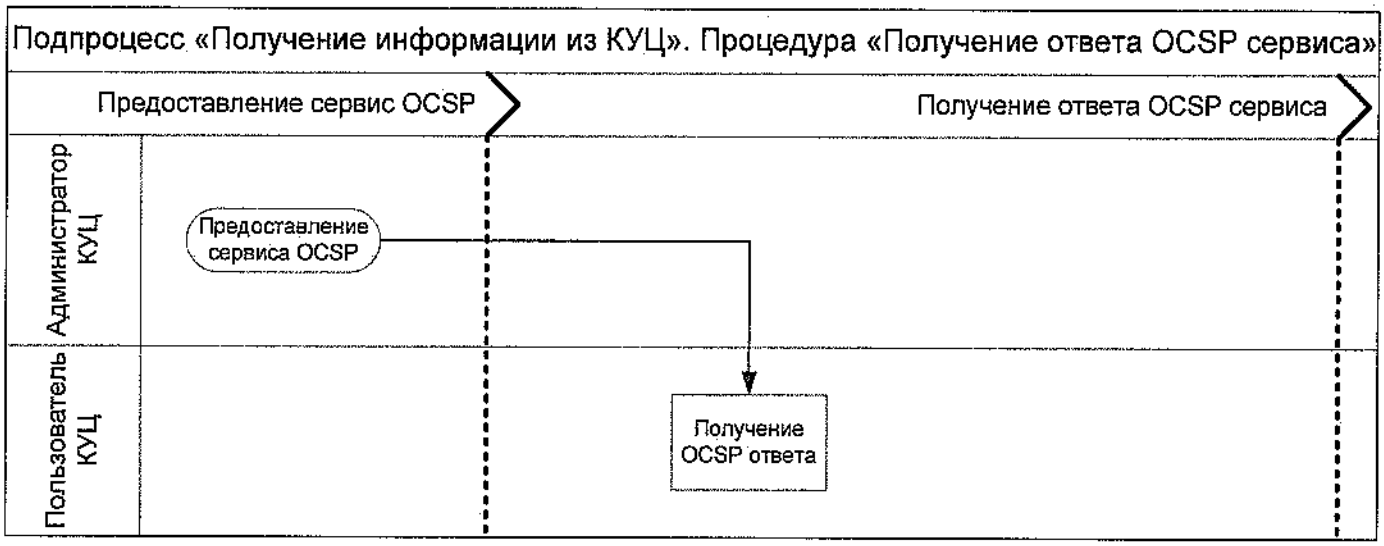
d) Схема процедуры «Получение информации через Спецсвязь России»:



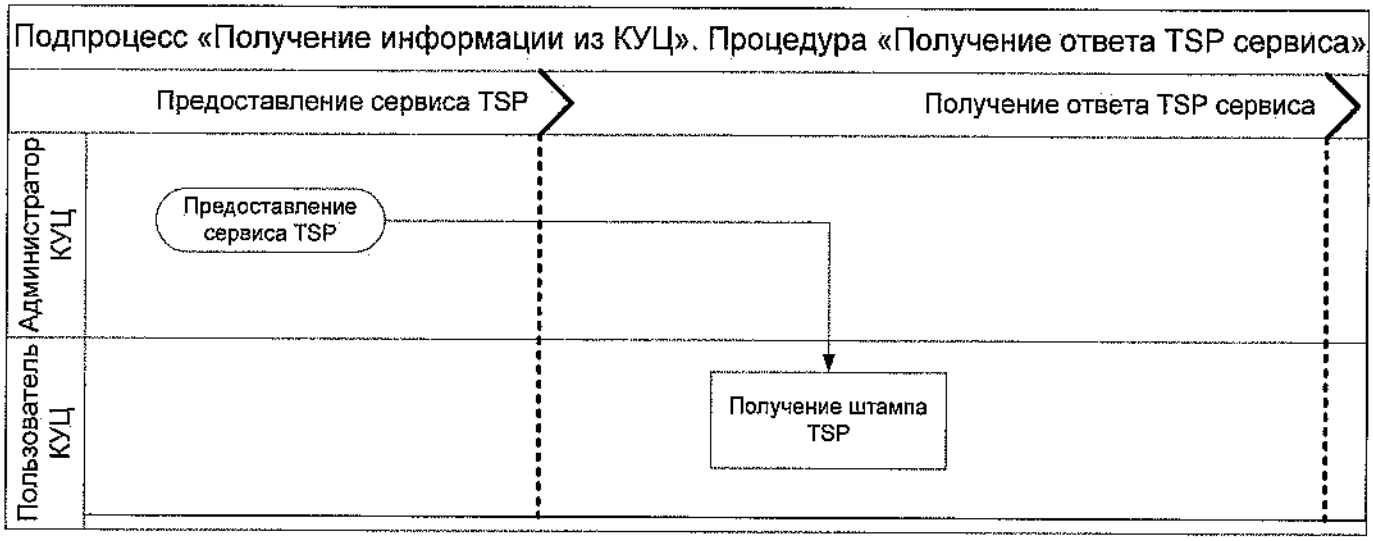
e) Схема процедуры «Получение информации из списков отозванных сертификатов»:



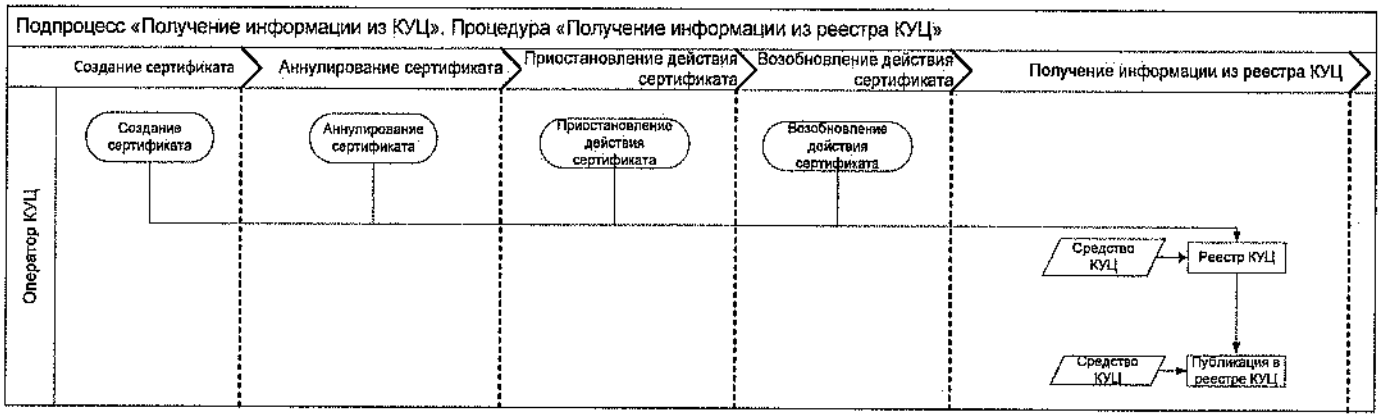
f) Схема процедуры «Получение ответа OCSP сервиса»:



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 С 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 «Т» 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 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 № 10

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 1c 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 № 11

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 № 12

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 № 13

Ограничения использования сертификатов ключей проверки электронной подписи

1. **Квалифицированный сертификат Госкорпорации «Росатом»**

Данные сертификаты ключа проверки электронной подписи предназначены для использования при участии в качестве заказчика на электронных торговых площадках, для использования в защищенной корпоративной почтовой системе Госкорпорации «Росатом», для аутентификации пользователей при доступе к корпоративным информационным системам ЦОД из сети Интернет.

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В сертификате указываются следующие ограничения:

- 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)
- 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. **Облачная подпись Госкорпорации «Росатом»**

Данные сертификаты ключа проверки электронной подписи предназначены для Формирования 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

3. **Квалифицированный сертификат для Росреестра (требуется доп. доверенность)**

Данные сертификаты ключа проверки электронной подписи предназначены для 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, для использования при участии в качестве заказчика на электронных торговых площадках, для использования в защищенной корпоративной почтовой системе Госкорпорации «Росатом», для аутентификации пользователей при доступе к корпоративным информационным системам ЦОД из сети Интернет.

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)
- Шифрующая файловая система (EFS) (1.3.6.1.4.1.311.10.3.4)
- Вход со смарт-картой (1.3.6.1.4.1.311.20.2.2)
- 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

4. Аутентификация сервера

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

- Аутентификация веб-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

5. 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 ЗАО «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

6. 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

7. 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 № 14

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

У Т В Е Р Ж Д А Ю
Директор по информационным технологиям
АО «Гринатом»

_____ / А.Н. Киселёв /

М.П.

ПОРЯДОК

организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

Москва 2021 г.

Содержание

1. Назначение и область применения

Настоящий порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее – Порядок), разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты (далее – ОКЗ).

Настоящий Порядок определяет условия предоставления и правила пользования услугами ОКЗ, основные организационно-технические мероприятия, направленные на обеспечение работы ОКЗ. Порядок имеет статус локального.

Требования настоящего Порядка распространяются на организации-обладатели конфиденциальной информации (далее - ООКИ), использующие автоматизированные и/или информационные системы, в которых хранится, обрабатывается и/или передается по каналам связи с использованием средств криптографической защиты информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну и обязательны для выполнения сотрудниками, исполняющими следующие функциональные роли:

1. Руководитель ООКИ;
2. Аналитик ОКЗ АО «Гринатом»;
3. Администратор безопасности ОКЗ АО «Гринатом»;
4. Руководитель АО «Гринатом»;
5. Начальник Управления информационной безопасности АО «Гринатом»;
6. Руководитель Органа криптографической защиты АО «Гринатом»;
7. Проверяющий.

Настоящий Порядок использует ссылки на следующие документы, необходимые для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

Документ	Статус	Тип документа	Ответственный
Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686 Н 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	Действует	Лицензия	Волков С.П.

(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 06.04.11 г. № 63-ФЗ "Об электронной подписи"	Действует	Федеральный закон	Волков С.П.
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	Волков С.П.
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	Волков С.П.
Приказ ФСБ России от 10.07.2014 г. N 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности»	Действует	Приказ	Волков С.П.

Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» (с пометкой «Для служебного пользования»)	Действует	Требование	Волков С.П.

и является основой для регламентации следующих подпроцессов и процедур:

Подпроцессы:
Подпроцесс «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
Подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации»
Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ в ОКЗ»
Подпроцесс «Отправка и получение СКЗИ»
Подпроцесс «Учет СКЗИ в ООКИ»
Подпроцесс «Установка и настройка СКЗИ»
Подпроцесс «Генерация ключевой информации»
Подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ»
Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»
Подпроцесс «Обеспечение функционирования, безопасности и контроля за применением СКЗИ»
Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»
Подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ»
Подпроцесс «Проверка выполнения требований Порядка»

2. Термины, определения и сокращения

Термин	Определение
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока
Книга лицевых счетов	Книга регистрации применяющихся Пользователями средств криптографической защиты информации, эксплуатационной и технической документации

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
Средства криптографической защиты информации (СКЗИ)	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
АБ	Администратор безопасности ОКЗ АО «Гринатом»

ООКИ	Организация-обладатель конфиденциальной информации
КУЦ	Корпоративный Удостоверяющий центр Госкорпорации «Росатом»
ОКЗ	Орган криптографической защиты АО «Гринатом»
Руководитель ООКИ	Руководитель организации-обладателя конфиденциальной информации
СКЗИ	Средство криптографической защиты информации
ЭП	Электронная подпись

3. Описание процесса

3.1. Цель процесса

Предоставление услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

3.2. Задачи процесса

- Разработка и утверждение схемы организации криптографической защиты информации;
- Формирование комплекта поставки СКЗИ и учет СКЗИ;
- Отправка и получение СКЗИ;
- Учет СКЗИ в ООКИ;
- Установка и настройка СКЗИ;
- Генерация ключевой информации;
- Обучение и допуск Пользователей к самостоятельному использованию СКЗИ;
- Принятие решения о возможности эксплуатации СКЗИ;
- Обеспечение функционирования, безопасности и контроля за применением СКЗИ;
- Расследование фактов нарушений условий использования СКЗИ;
- Вывод из эксплуатации и уничтожение СКЗИ;
- Проверка выполнения требований Порядка.

3.3. Участники группы процессов и их роли

№ п.п.	Участники	Основные роли
1	Руководитель ООКИ	• Принимает решение о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации; • Принимает решение о допуске пользователей к самостоятельной работе с СКЗИ; • Согласовывает документы, необходимые для получения услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Принимает решение о прекращении получения услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Ознакамливается и подписывает документы по результатам проверки и устранению недостатков выполнения требований Порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Принимает решение о проведении расследований по фактам нарушения условий использования СКЗИ; • Ознакамливается и подписывает Заключения по результатам расследований фактов нарушения условий использования СКЗИ.

2	Аналитик ОКЗ АО «Гринатом» (далее – Аналитик)	• Разрабатывает и поддерживает в актуальном состоянии схему криптографической защиты информации; • Определяет требования к защищенности различных информационных систем в соответствии с действующей нормативно-методической документацией; • Составляет заключение о возможности эксплуатации СКЗИ; • Формирует комплект поставки СКЗИ; • Учитывает СКЗИ в ОКЗ; • Отправляет СКЗИ в ООКИ.
3	Администратор безопасности ОКЗ АО «Гринатом»	• Подготавливает и согласовывает документы, необходимые для получения услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Получает и учитывает СКЗИ в ООКИ; • Устанавливает, настраивает, проверяет готовность к работе СКЗИ на рабочих местах Пользователей СКЗИ; • Обучает Пользователей СКЗИ. и принимает зачеты; • Осуществляет контроль за правильностью эксплуатации СКЗИ; • Проводит регламентные работы; • Уничтожает выведенные из действия СКЗИ.
4	Руководитель АО «Гринатом»	• Согласовывает Приказ о проведении проверки требований Порядка; • Согласовывает Приказ о проведении расследования условий использования СКЗИ.

5	Начальник Управления информационной безопасности АО «Гринатом»	• Согласовывает документы, необходимые для предоставления услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Ознакамливается и подписывает Заключения по результатам расследований фактов нарушения условий использования СКЗИ.
6	Руководитель Органа криптографической защиты АО «Гринатом»	• Согласовывает документы, необходимые для предоставления услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Утверждает Заключение комиссии Органа криптографической защиты АО «Гринатом» по результатам расследования фактов нарушения условий использования СКЗИ.
7	Проверяющий	• Подготавливает документы для проведения проверок выполнения требований Порядка; • Осуществляет проверки выполнения требований Порядка; • Отслеживает устранение ООКИ выявленных по результатам проверок недостатков.

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	Приказ о назначении администраторов безопасности и лиц, их замещающих	Предприятие, АО «Гринатом»	Организация
2	Заявление на услугу Администратора безопасности	Предприятие, АО «Гринатом»	Организация
3	Перечень лиц, допускаемых к самостоятельной работе с СКЗИ	Предприятие, АО «Гринатом»	Организация
4	Приказ о назначении прав подписей Пользователей СКЗИ	Предприятие, АО «Гринатом»	Организация
5	Заявление на организацию 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» (с передачей СКЗИ на предприятие)	Предприятие, АО «Гринатом»	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация,/ Дивизион/ Организация)
6	Заявление на организацию 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» (без передачи СКЗИ на предприятие)	Предприятие, АО «Гринатом»	Организация
7	Схема организации криптографической защиты информации	АО «Гринатом»	Организация
8	Утвержденная схема организации криптографической защиты информации	АО «Гринатом»	Организация
9	СКЗИ	Предприятие	Организация
10	Книга лицевых счетов	АО «Гринатом»	Организация
11	Доверенность на получение АБ СКЗИ из банка	Предприятие	Организация
12	СКЗИ из банка	Предприятие	Организация
13	Акт повреждения упаковки	АО «Гринатом»	Организация
14	Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов	Предприятие, АО «Гринатом»	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация,/ Дивизион/ Организация)
	(для обладателя конфиденциальной информации)		
15	Технический (аппаратный) журнал	Предприятие, АО «Гринатом»	Организация
16	Акт готовности СКЗИ к эксплуатации	Предприятие, АО «Гринатом»	Организация
17	Учтенные ключевые носители	Предприятие	Организация
18	Ключевой носитель с ключевой информацией	Предприятие	Организация
19	Сертификаты	Предприятие	Организация
20	Зарегистрированные сертификаты	Предприятие	Организация
21	Заключение о сдаче зачетов	Предприятие, АО «Гринатом»	Организация
22	Заключение о возможности эксплуатации СКЗИ	Предприятие, АО «Гринатом»	Организация
23	Журнал учета выполнения регламентных работ	Предприятие, АО «Гринатом»	Организация
24	План устранения недостатков с отметками о выполнении	Предприятие, АО «Гринатом»	Организация
25	Акт об уничтожении СКЗИ	Предприятие, АО «Гринатом»	Организация
26	Приказ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с	Предприятие, АО «Гринатом»	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация,/ Дивизион/ Организация)
	ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ		
27	План-график проведения проверок	Предприятие, АО «Гринатом»	Организация
28	Письмо о проведении проверки работ по договору присоединения на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств	Предприятие	Организация
29	Сводная таблица по объекту проверки	АО «Гринатом»	Организация
30	Акт проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ	Предприятие, АО «Гринатом»	Организация

3.5. Основные входы процесса

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
1	Единые отраслевые методические указания по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях	ГК «Росатом»	Корпорация
2	Заявление на организацию 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» (с передачей СКЗИ на предприятие)	Предприятие	Организация
3	Заявление на организацию 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» (без передачи СКЗИ на предприятие)	Предприятие	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
4	Скан-копия Приказа о назначении администраторов безопасности и лиц их замещающих	Предприятие	Организация
5	Заявление на услугу Администратора безопасности	Предприятие	Организация
6	Скан-копия Перечня лиц, допускаемых к самостоятельной работе с СКЗИ	Предприятие	Организация
7	Скан-копия Приказа о назначении прав подписей Пользователей СКЗИ	Предприятие	Организация
8	Скан-копия Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)	Предприятие	Организация
9	Скан-копия Заключения о сдаче зачетов	Предприятие	Организация
10	Скан-копия Акта готовности СКЗИ к эксплуатации	Предприятие	Организация
11	Скан-копия Технического (аппаратного) журнала (если он ведется)	Предприятие	Организация
12	Акт об уничтожении СКЗИ	Предприятие	Организация
13	Акт повреждения упаковки	Предприятие	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
14	Схема организации криптографической защиты конфиденциальной информации	АО «Гринатом»	Организация
15	Утвержденная схема организации криптографической защиты конфиденциальной информации	АО «Гринатом»	Организация
16	СКЗИ	АО «Гринатом»	Организация
17	Сопроводительное письмо к СКЗИ	АО «Гринатом»	Организация
18	Акт приема-передачи банковского СКЗИ	Банк	Организация
19	Доверенность на получение АБ ООКИ СКЗИ из банка	Предприятие	Организация
20	Инструкция по установке СКЗИ	АО «Гринатом»	Организация
21	Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ	АО «Гринатом»	Организация
22	Учтенные ключевые носители	Предприятие	Организация
23	Сертификаты	Банк	Организация
24	Учебные материалы	АО «Гринатом»	Организация
25	Анкеты для опроса пользователей СКЗИ	АО «Гринатом»	Организация
26	Скан-копия Заключения о сдаче зачетов	Предприятие	Организация
27	Заключение о возможности эксплуатации СКЗИ	Предприятие	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
28	Эксплуатационная и техническая документация к СКЗИ	АО «Гринатом»	Организация
29	План реализации рекомендаций по результатам проверки лицензиата ФСБ России АО «Гринатом» в ООКИ	Предприятие	Организация
30	Скан-копия Журнала учета выполнения регламентных работ	Предприятие	Организация
31	Акт уничтожения СКЗИ	Предприятие	Организация
32	Приказ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ	АО «Гринатом»	Организация
33	Выписка из схемы криптографической защиты конфиденциальной информации	АО «Гринатом»	Организация
34	Выписка из Центра Регистрации Удостоверяющего центра Госкорпорации «Росатом»	АО «Гринатом»	Организация
35	Письмо о проведении проверки в ООКИ	АО «Гринатом»	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
36	Сводная таблица по объекту проверки	АО «Гринатом»	Организация
37	Программа проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ	АО «Гринатом»	Организация
38	Акт проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ	АО «Гринатом»	Организация

3.6. Описание подпроцессов

3.6.1. Подпроцесс «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе

СКЗИ из эксплуатации»

Руководитель ООКИ:

- Принимает решение о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в соответствии с Едиными отраслевыми методическими указаниями по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях

В случае если принимается решение об обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

- Назначает Приказом АБ и лиц их замещающих (Приложение №4) или использует АБ в рамках связанной услуги GEN.23 «Услуга Администратора безопасности АО «Гринатом» (Приложение №5).
  В рамках услуги GEN.23 АО «Гринатом» предоставляет Администратора безопасности на предприятие, который проводит комплекс работ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну;
- Утверждает Перечень лиц, допускаемых к самостоятельной работе с СКЗИ (Приложение №6);
- Назначает Приказом лиц, имеющих права подписи в системе(ах) (Приложение №7) (в случае если такие права предоставляются);
- Направляет в адрес ОКЗ АО «Гринатом» следующий комплект документов:
  - Заявление на организацию 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 (далее - Заявление на СКЗИ с передачей СКЗИ на предприятие) (Приложение №8.1), в случае если АО «Гринатом», передает СКЗИ на предприятие или Заявление на организацию 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 (далее - Заявление на СКЗИ без передачи СКЗИ на предприятие) (Приложение №8.2), в случае если АО «Гринатом» не передает СКЗИ на предприятие;
  - Скан-копию Приказа о назначении АБ и лиц их замещающих или Заявление на услугу Администратора безопасности;

- Скан-копию Перечня лиц, допускаемых к самостоятельной работе с СКЗИ;
- Скан-копию Приказа о предоставлении прав подписей в системе(ах).

Исходящая информация поступает в подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации».

В случае если принимается решение о выводе СКЗИ из эксплуатации:

- Принимает решение о выводе СКЗИ из эксплуатации.

Исходящая информация поступает в подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ».

3.6.2. Подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации»

Входящая информация поступает из подпроцесса «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации» или из подпроцесса «Вывод из эксплуатации и уничтожение СКЗИ».

Аналитик:

- Разрабатывает «Схему организации криптографической защиты конфиденциальной информации» (далее – Схема) (Приложение №9) на основании данных, указанных в Заявлении на СКЗИ (с передачей СКЗИ на предприятие), Заявления на СКЗИ (без передачи СКЗИ на предприятие), скан-копии Приказа о назначении АБ и лиц их замещающих или Заявления на услугу Администратора безопасности, скан-копии Перечня лиц, допускаемых к самостоятельной работе с СКЗИ, скан-копии Приказа о предоставлении прав подписей Пользователей СКЗИ, скан-копии Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации), скан-копии Заключения о сдаче зачетов, скан-копии Технического (аппаратного) журнала, скан-копии Акта готовности СКЗИ к эксплуатации, Акта об уничтожении СКЗИ, Акта повреждения упаковки.

Начальник управления информационной безопасности АО «Гринатом»:

- Утверждает Схему.

Если Аналитику пришла информация из подпроцесса «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации», то исходящая информация поступает в подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ в ОКЗ».

Если Аналитику пришла информация из подпроцесса «Вывод из эксплуатации и уничтожение СКЗИ», то процесс взаимодействия ОКЗ и ООКИ завершается.

Исходящая информация поступает в подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ» или в конец процесса.

3.6.3. Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ»

Входящая информация поступает из подпроцесса «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации».

Аналитик:

- Формирует комплект поставки СКЗИ;
- Учитывает СКЗИ в Книге лицевых счетов ОКЗ АО «Гринатом» (Приложение №10).

Если СКЗИ получаются из банка, то комплект поставки не формируется Аналитиком.

Исходящая информация поступает в подпроцесс «Отправка и получение СКЗИ».

3.6.4. Подпроцесс «Отправка и получение СКЗИ»

Входящая информация поступает из подпроцесса «Формирование комплекта поставки СКЗИ и учет СКЗИ».

Способы доставки СКЗИ:

- фельдъегерской (в том числе ведомственной) связью;
- доверенным лицом (необходима доверенность по форме Приложения №11);
- АБ.

Доставка осуществляется при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ во время доставки.

Пересылка эксплуатационной и технической документации СКЗИ организуется и производится Аналитиком заказным или ценным почтовым отправлением.

Аналитик:

- Помещает СКЗИ в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия.
  На упаковках указывает АБ, для которых эти упаковки предназначены. Упаковки опечатывает таким образом, чтобы исключить возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.
  Помещает во внешнюю упаковку при предъявлении фельдсвязью дополнительных требований;
- Подготавливает сопроводительное письмо (Приложение №12), в котором указывает, что посылается и в каком количестве, учетные номера изделий и/или документов, а также, при необходимости, назначение и порядок

использования высылаемого отправления. Сопроводительное письмо вкладывает в одну из упаковок.

АБ:

- Получает упаковку с СКЗИ;
- Составляет и направляет в адрес ОКЗ АО «Гринатом» акт повреждения упаковки (Приложение №13) (*в случае, если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому*), после чего ожидает указаний от ОКЗ АО «Гринатом» о дальнейшем применении СКЗИ (*в случае составления акта повреждения упаковки*).

АБ (в случае если СКЗИ получаются из банка, а также других УЦ, данные работы входят в состав услуги GEN.43):

- Запрашивает и заполняет актуальные шаблоны доверенностей;
- Запрашивает и заполняет актуальные шаблоны документов на получение первичной ключевой информации;
- Согласовывает документы на первичную ключевую информацию с поддержкой банка, УЦ или ИС, а также ответственными со стороны ООКИ;
- Выезжает в УЦ для получения ключа ЭП;
- Подписывает при получении СКЗИ или ЭП акт приема-передачи, по форме установленной банком, УЦ или другой организацией.

Исходящая информация поступает в подпроцесс «Учет СКЗИ в ООКИ» или в подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации» (*в случае, если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому).*

3.6.5. Подпроцесс «Учет СКЗИ в ООКИ»

Входящая информация поступает из подпроцесса «Отправка и получение СКЗИ».

АБ:

- Учитывает СКЗИ в «Журнале поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)» (далее – Журнал учета (для обладателя конфиденциальной информации) (Приложение №14);
- Отправляет подтверждение о получении СКЗИ в ОКЗ АО «Гринатом» в соответствии с порядком, указанным в сопроводительном письме.

Все полученные АБ экземпляры СКЗИ, эксплуатационная и техническая документация к ним должны быть выданы под расписку в Журнале учета (для

обладателя конфиденциальной информации) Пользователям СКЗИ, несущим персональную ответственность за их сохранность.

В случае если СКЗИ получаются из банка, подтверждение в получении СКЗИ в ОКЗ АО «Гринатом» не отправляется.

Исходящая информация поступает в подпроцесс «Установка и настройка СКЗИ».

3.6.6. Подпроцесс «Установка и настройка СКЗИ»

Входящая информация поступает из подпроцесса «Учет СКЗИ в ООКИ».

АБ:

- Устанавливает и настраивает СКЗИ в соответствии с Инструкцией по установке СКЗИ (поставляется в комплекте к СКЗИ);
- Учитывает факт установки и настройки СКЗИ в Журнале учета (для обладателя конфиденциальной информации);
- Проверяет готовность АРМ с установленным СКЗИ на соответствие «Единым отраслевым методическим указаниям по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» и «Порядку разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ» (Приложение №15), делает запись об опечатывании технических средств СКЗИ в Техническом (аппаратном) журнале (Приложение №16).
  Технический (аппаратный) журнал ведется в случае ввода ключевой информации на весь срок эксплуатации.
- Составляет Акт готовности СКЗИ к эксплуатации (Приложение №17).

Исходящая информация поступает в подпроцесс «Генерация ключевой информации».

3.6.7. Подпроцесс «Генерация ключевой информации»

Входящая информация поступает из подпроцесса «Установка и настройка СКЗИ».

При получении СКЗИ от ОКЗ АО «Гринатом» генерация ключевой информации не производится.

АБ (в случае если СКЗИ получаются из банка, а также других УЦ, данные работы входят в состав услуги GEN.43):

- Ставит на учет носители информации в качестве ключевых;
- Подписывает запрос на генерацию ключевых документов у пользователя СКЗИ и руководителя ООКИ;

- Передает запрос на генерацию ключа на бумажном носителе в бухгалтерию ООКИ для проставления оттиска печати (в случае необходимости);
- Отправляет в ИС запрос на генерацию ключевой информации подписанта;
- Принимает ключ на АРМ пользователя СКЗИ;
- Производит генерацию технологического ключа (в случае необходимости);
- Учитывает факт генерации и передачи Пользователям в Журнале поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации);
- Отправляет сертификаты в ИС;
- Делает отметку в Журнале учета (для обладателя конфиденциальной информации) о сроках действия сертификата;
- Передает данные о ключевых документах в ОКЗ.

Исходящая информация поступает в подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ».

3.6.8. Подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ»

Входящая информация поступает из подпроцесса «Генерация ключевой информации».

Непосредственно к работе с СКЗИ Пользователи допускаются только после соответствующего обучения.

АБ:

- Осуществляет обучение Пользователей СКЗИ, применяя учебные материалы (Приложение №18);
- Проводит опрос Пользователей СКЗИ по окончании обучения, используя Анкеты для опроса пользователей СКЗИ (Приложение №19) и заполняет Заключение о сдаче зачетов (Приложение №20);
- Направляет в адрес ОКЗ АО «Гринатом» следующий комплект документов:
  - скан-копию Журнала учета (для обладателя конфиденциальной информации);
  - скан-копию Технического (аппаратного) журнала (*в случае если он ведется*);
  - скан-копию Заключения о сдаче зачетов;
  - скан-копию Акта готовности СКЗИ к эксплуатации.

Исходящая информация поступает в подпроцесс «Принятие решения о возможности эксплуатации СКЗИ».

3.6.9. Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»

Входящая информация поступает из подпроцесса «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ».

Аналитик:

- Составляет Заключение о возможности эксплуатации СКЗИ (Приложение №21) на основании следующих полученных от ООКИ документов:
  - Заявления на СКЗИ (с передачей СКЗИ на предприятие);
  - Заявления на СКЗИ (без передачи СКЗИ на предприятие);
  - Скан-копии Приказа о назначении администраторов безопасности и лиц их замещающих или Заявления на услугу Администратора безопасности;
  - Скан-копии Перечня лиц, допускаемых к самостоятельной работе с СКЗИ;
  - Скан-копии Приказа о назначении прав подписей пользователей СКЗИ;
  - Скан-копии Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации);
  - Скан-копии Технического (аппаратного) журнала *(если он ведется)*;
  - Скан-копии Заключения о сдаче зачетов;
  - Скан-копии Акта готовности СКЗИ к эксплуатации.
- Отправляет Заключение о возможности эксплуатации СКЗИ в ООКИ.

Исходящая информация поступает в подпроцесс «Обеспечение функционирования и безопасности и контроля за применением СКЗИ».

3.6.10. Подпроцесс «Обеспечение функционирования и безопасности и контроля за применением СКЗИ»

Входящая информация поступает из подпроцесса «Принятие решения о возможности эксплуатации СКЗИ» или из подпроцесса «Проверка выполнения требований Порядка».

Функционирование и безопасность применения СКЗИ обеспечивается в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам.

Оригиналы выданных сертификатов соответствия требованиям безопасности находятся в ОКЗ АО «Гринатом», копии находятся в ООКИ.

АБ (если проводятся регламентные работы):

- Дополнительно к проверке порядка использования СКЗИ проводит регламентные работы с СКЗИ не реже одного раза в 6 месяцев, о чем

делает отметки в Журнале учета выполнения регламентных работ (Приложение №22). Перечни регламентных работ указаны в формулярах на СКЗИ.

АБ (если СКЗИ получены из банка, работы входят в состав услуги GEN.43):

- Дополнительно к проверке порядка использования СКЗИ отслеживает сроки действия ключевой информации Пользователей с помощью Журнала учета (для обладателя конфиденциальной информации). В случае если срок действия ключевой информации истекает, проводит процедуру генерации новой ключевой информации Пользователей;
- Отслеживает сроки действия доверенностей;
- Ведет реестр ключей, доверенностей и АРМ;
- Предоставляет информацию о сроках действия ключей и доверенностей на подписантов по запросам пользователей;
- Предоставляет информацию для паспорта рабочего места.

АБ (если входящая информация поступает из подпроцесса «Принятие решения о возможности эксплуатации СКЗИ»):

- Осуществляет проверку порядка использования СКЗИ в соответствии с эксплуатационной и технической документацией с периодичностью не реже 1-го раза в год. В состав проверки входит как минимум:
  - соответствие номеров СКЗИ данным в книгах и журналах учета СКЗИ;
  - наличие носителей ключевой информации и их соответствие данным, указанным в книгах и журналах учета СКЗИ;
  - соответствие настроек системного ПО, СКЗИ и мер физической защиты СКЗИ требованиям документации к СКЗИ;
  - наличие носителей ключевой информации и их соответствие данным, указанным в книгах и журналах учета СКЗИ.
- Проставляет отметки в Техническом (аппаратном) журнале *(в случае, если он ведется)*;
- Составляет Акт готовности СКЗИ к эксплуатации (Приложение №17);
- Направляет в ОКЗ АО «Гринатом»:
  - скан-копию Технического (аппаратного) журнала *(если он ведется)*;
  - скан-копию Акта готовности СКЗИ к эксплуатации;
  - скан-копию Журнала учета выполнения регламентных работ *(если регламентные работы проводятся)*.

АБ (если входящая информация поступает из подпроцесса «Проверка выполнения требований Порядка»):

- Устраняет недостатки, выявленные в ходе проверки выполнения требований Порядка;

- Проставляет отметки об устранении недостатков в Плане устранения недостатков, выявленных в ходе проверки выполнения требований Порядка;
- Направляет в ОКЗ АО «Гринатом» План устранения недостатков, выявленных в ходе проверки выполнения требований Порядка, с отметками об устранении.

Аналитик/Проверяющий:

- Обрабатывают полученные документы от АБ.

В случае, если в результате обработки полученных документов выявятся факты нарушений условий использования СКЗИ, то может быть инициировано расследование.

Исходящая информация поступает в подпроцесс «Генерация ключевой информации», в подпроцесс «Расследование фактов нарушений условий использования СКЗИ» или в начало подпроцесса «Обеспечение функционирования, безопасности и контроля за применением СКЗИ».

3.6.11. Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»

Входящая информация поступает из подпроцесса «Обеспечение функционирования, безопасности и контроля за применением СКЗИ».

Подпроцесс «Расследование фактов нарушений условий использования СКЗИ» описан в документе «Порядок проведения расследований фактов нарушения условий использования средств криптографической защиты информации в организациях Госкорпорации «Росатом» (Приложение №23).

Расследование фактов нарушения условий использования СКЗИ может быть инициировано со стороны ООКИ, со стороны АО «Гринатом» или ФСБ России.

Исходящая информация поступает в подпроцесс «Обеспечение функционирования и безопасности и контроля за применением СКЗИ».

3.6.12. Подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ»

Входящая информация поступает из подпроцесса «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации».

Руководитель ООКИ:

- Принимает решение о выводе СКЗИ из эксплуатации;

АБ:

- Изымает СКЗИ из аппаратных средств, с которыми они функционировали. При этом СКЗИ считается изъятым из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и он полностью отсоединен от аппаратных средств;
- Уничтожает СКЗИ на месте.

  В случае если ООКИ отказывается от услуги CLB.18, то уничтожение СКЗИ производится по акту (уничтожение производится комиссионно в составе не менее двух АБ, Приложение № 24). В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых СКЗИ, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. При этом в Журнале учета (для обладателя конфиденциальной информации) в графах об изъятии и уничтожении СКЗИ указываются реквизиты Акта уничтожения.

  Уничтожение путем физического уничтожения или путем стирания (разрушения), исключающего возможность их использования, а также восстановления. Непосредственные действия по уничтожению конкретного типа СКЗИ регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями ОКЗ АО «Гринатом».

  Бумажные и прочие сгораемые материалы, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью шредеров.

  СКЗИ должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации. Если срок уничтожения эксплуатационной и технической документацией не установлен, то СКЗИ должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия).
- В случае если ООКИ не отказываются от услуги CLB.18, то уничтожение СКЗИ сопровождается отметками в Журнале учета (для обладателя конфиденциальной информации) об изъятии и уничтожении СКЗИ, при этом Акт уничтожения не составляется;
- Направляет в адрес ОКЗ АО «Гринатом» следующие документы:
  - скан-копию Журнала учета (для обладателя конфиденциальной информации);
  - Акт об уничтожении СКЗИ.

Не реже одного раза в год АБ должны направлять в ОКЗ АО «Гринатом» письменные отчеты об уничтоженных СКЗИ. ОКЗ АО «Гринатом» вправе устанавливать периодичность представления указанных отчетов чаще одного раза в год.

Исходящая информация поступает в подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации».

3.6.13.Подпроцесс «Проверка выполнения требований Порядка».

Руководитель АО «Гринатом»:

- Утверждает Приказ о проведении проверок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ (Приложение №25) и План-график проведения проверок (Приложение №26).

Проверяющий:

- Подготавливает и отправляет письмо Руководителю ООКИ о проведении проверки работ по договору присоединения на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств (далее – Информационное письмо о проведении проверки, Приложение №27);
- Изучает материалы по объекту проверки:
  - выписку из Схемы организации криптографической защиты конфиденциальной информации (перечень СКЗИ, выданных ОКЗ на предприятие);
  - выписку из Центра Регистрации Удостоверяющего центра Госкорпорации «Росатом» (перечень сертификатов ключей проверки электронной подписи, выданных на предприятие).
- Заполняет Сводную таблицу по объекту проверки (Приложение №28);
- Проводит проверку организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ в соответствии с Программой проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ (далее – Программа проверки, Приложение №29) и Сводной таблицей по объекту проверки;
- Подготавливает, подписывает и отправляет в адрес Руководителя ООКИ 2 экземпляра Акта проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ (далее – Акт проверки, Приложение №30).

Руководитель Органа криптографической защиты АО «Гринатом»:

- Согласовывает Информационное письмо о проведении проверки;
- Согласовывает Программу проверки;
- Утверждает Акт проверки.

Начальник Управления информационной безопасности АО «Гринатом»:

- Согласовывает Программу проверки;
- Ознакамливается под роспись с Актом проверки.

Руководитель ООКИ:

- Ознакамливается под расписку с Актом проверки;
- Составляет и направляет в адрес Руководителя ОКЗ АО «Гринатом»:
  - План реализации рекомендаций по результатам проверки лицензиата ФСБ России АО «Гринатом» в ООКИ (далее – План устранения недостатков, Приложение №31);
  - Один экземпляр подписанного Акта проверки.

В случае если условия использования СКЗИ не нарушены, то Руководитель ООКИ возвращает только один экземпляр подписанного Акта проверки, План устранения недостатков не составляется.

Исходящая информация поступает в подпроцесс «Обеспечение функционирования и безопасности и контроля за применением СКЗИ».

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)»;
- Приказ ФСБ России от 10.07.2014 г. N 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения

установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности»;

- 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.№15686 Н 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);
- Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» (с пометкой «Для служебного пользования»);
- 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).

5. Порядок внесения изменений

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

6. Контроль и ответственность

6.1 Порядок обязаны соблюдать все следующие участники процесса:

Руководитель ООКИ;
Аналитик ОКЗ АО «Гринатом»;
Администратор безопасности ОКЗ АО «Гринатом»;
Руководитель АО «Гринатом»;
Начальник Управления информационной безопасности АО «Гринатом»;
Начальник Отдела криптографической защиты АО «Гринатом»;
Проверяющий.

6.2. Ответственность работников за несоблюдение требований Порядка.

За несоблюдение Порядка 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.	Форма приказа о назначении Администраторов безопасности и лиц их замещающих
Приложение №5.	Форма Заявления на услугу Администратора безопасности
Приложение №5.1.	Форма Заявления на услугу по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя
Приложение №6.	Перечень лиц, допускаемых к самостоятельной работе с СКЗИ
Приложение №7.	Форма Приказа о предоставлении прав подписей
Приложение №8.1.	Заявление на СКЗИ (с передачей СКЗИ)
Приложение №8.2.	Заявление на СКЗИ (без передачи СКЗИ)
Приложение №9.	Схема организации криптографической защиты конфиденциальной информации (шаблон)
Приложение №10.	Книга лицевых счетов
Приложение №11.	Доверенность доверенного лица на получение СКЗИ в ОКЗ
Приложение №12.	Сопроводительное письмо к СКЗИ
Приложение №13.	Акт повреждения упаковки
Приложение №14.	Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Приложение №15.	Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ

Приложение №16.	Технический (аппаратный) журнал
Приложение №17.	Акт готовности СКЗИ к эксплуатации
Приложение №18.	Учебные материалы
Приложение №19.	Анкета для опроса Пользователей
Приложение №20.	Заключение о сдаче зачетов
Приложение №21.	Заключение о возможности эксплуатации СКЗИ
Приложение №22.	Журнал выполнения регламентных работ
Приложение №23.	Порядок проведения расследований фактов нарушения условий использования средств криптографической защиты информации в организациях Госкорпорации «Росатом»
Приложение №24.	Акт уничтожения СКЗИ
Приложение №25.	Приказ о проведении проверки
Приложение №26.	План-график проведения проверок
Приложение №27.	Информационное письмо о проведении проверки
Приложение №28.	Сводная таблица по объекту проверки
Приложение №29.	Программа проверки
Приложение №30.	Акт проверки
Приложение №31.	План устранения недостатков

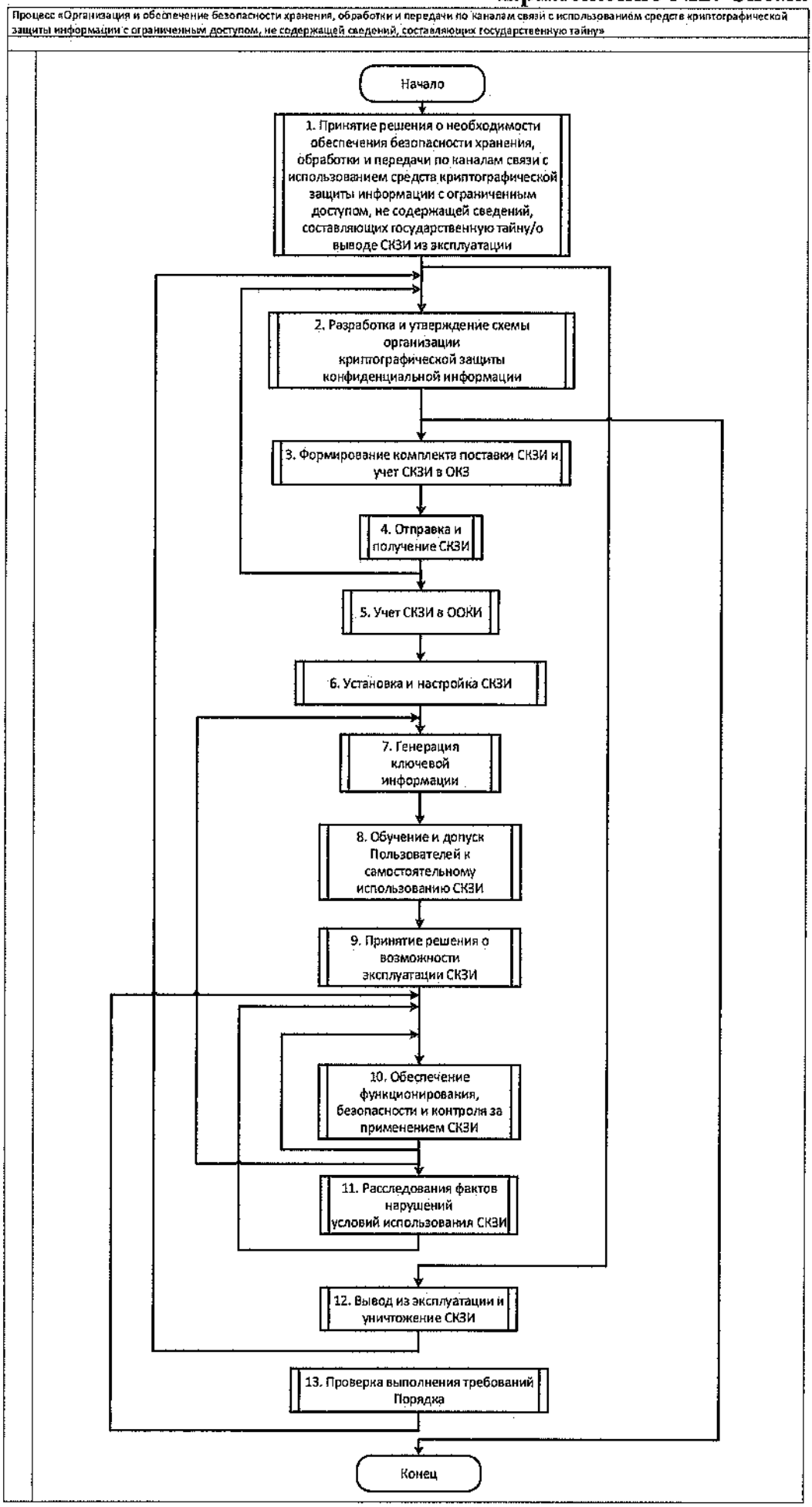
Приложение №1. Матрица ответственности

Подпроцессы в составе процесса	Участники процесса						
	Руководитель ООКИ	Аналитик»	АБ	Начальник Управления информационной безопасности АО «Гринатом»	Руководитель Органа криптографической защиты АО «Гринатом»	Руководитель АО «Гринатом»	Проверяющий
Подпроцесс «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»	Утв.						
Подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации»		О		Утв.			
Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ»		О					
Подпроцесс «Отправка и получение СКЗИ»		О	О				
Подпроцесс «Учет СКЗИ в ООКИ»		Инф.	О				
Подпроцесс «Установка и настройка СКЗИ»		Инф.	О				
Подпроцесс «Генерация ключевой информации»		Инф.	О				
Подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ»		Инф.	О				
Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»		О	Инф.				
Подпроцесс «Обеспечение функционирования и безопасности и контроля за применением СКЗИ»		Инф.	О				
Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»	Инф.			Инф.	О		О
Подпроцесс «Вывод из эксплуатации и уничтожения СКЗИ»	Утв.	Инф.	О				
Подпроцесс «Проверка выполнения требований Порядка»	О		О	О	О	Утв.	О

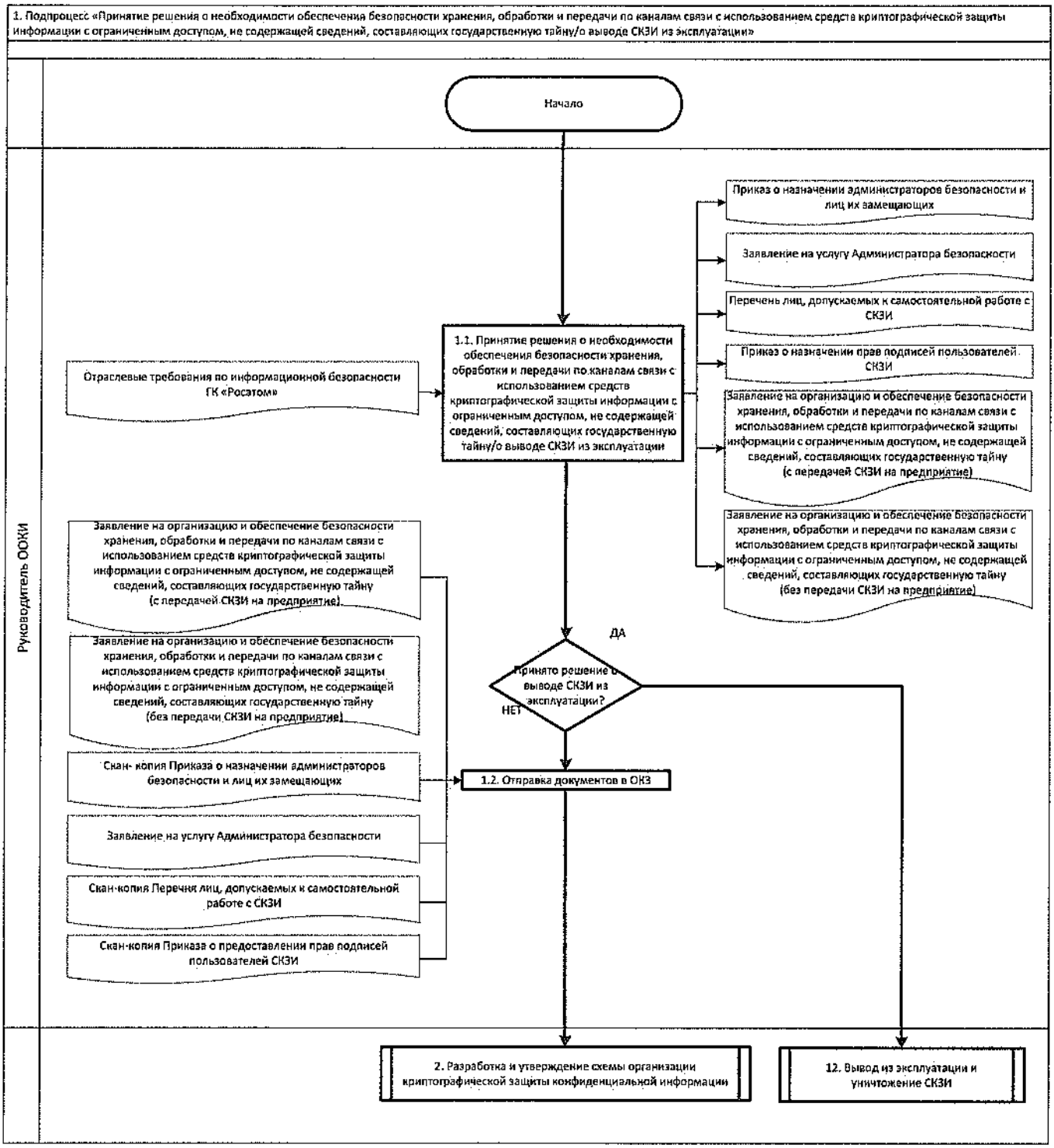
Сокращение	Название роли	Определение	Исполнитель Роли

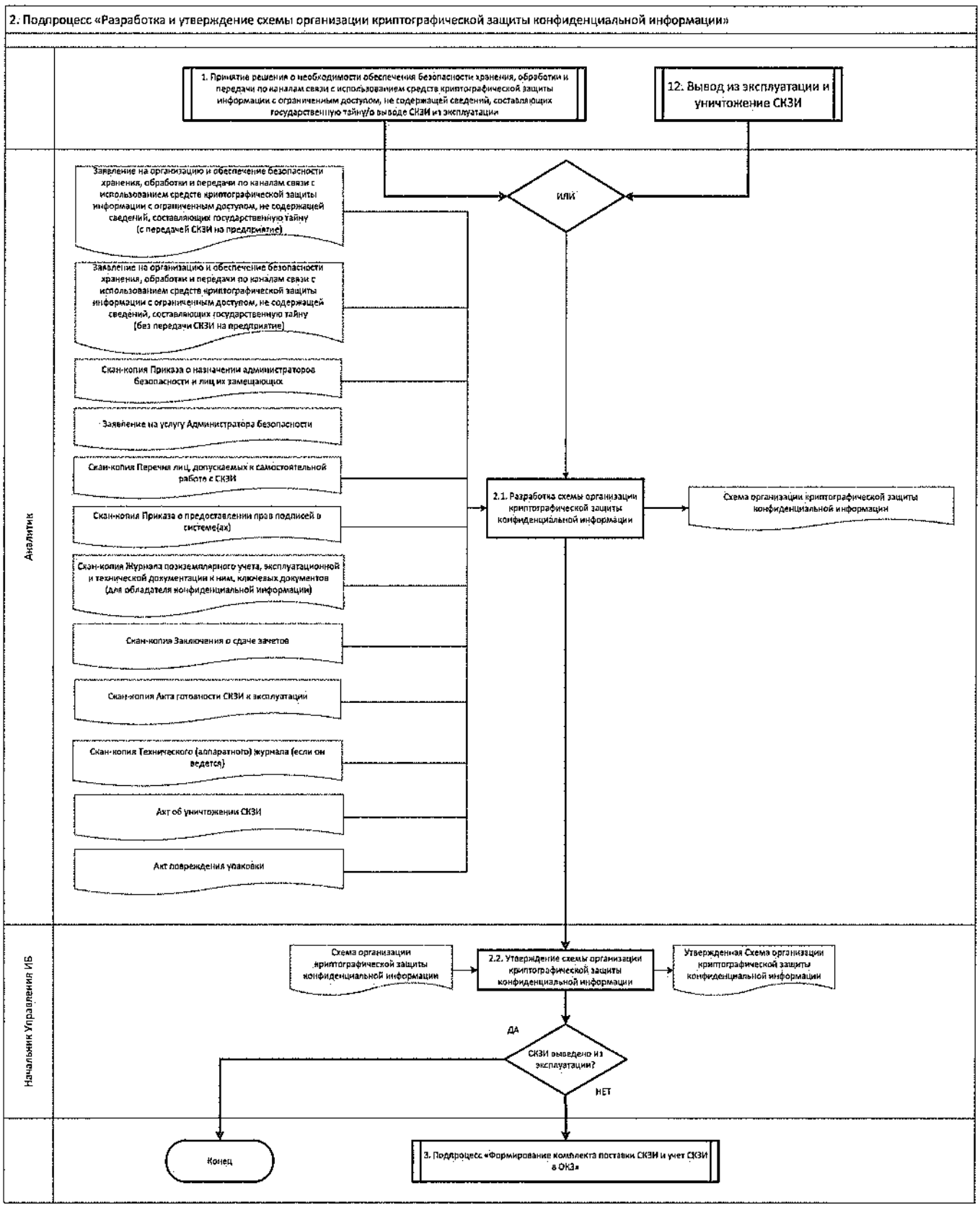
М	Методолог	Формирует требования к организации деятельности в рамках подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации
И	Интегратор	Интегрирует результаты подпроцесса/процедуры и отвечает за организацию подпроцесса/процедуры, включая взаимодействие участников	Структурное 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

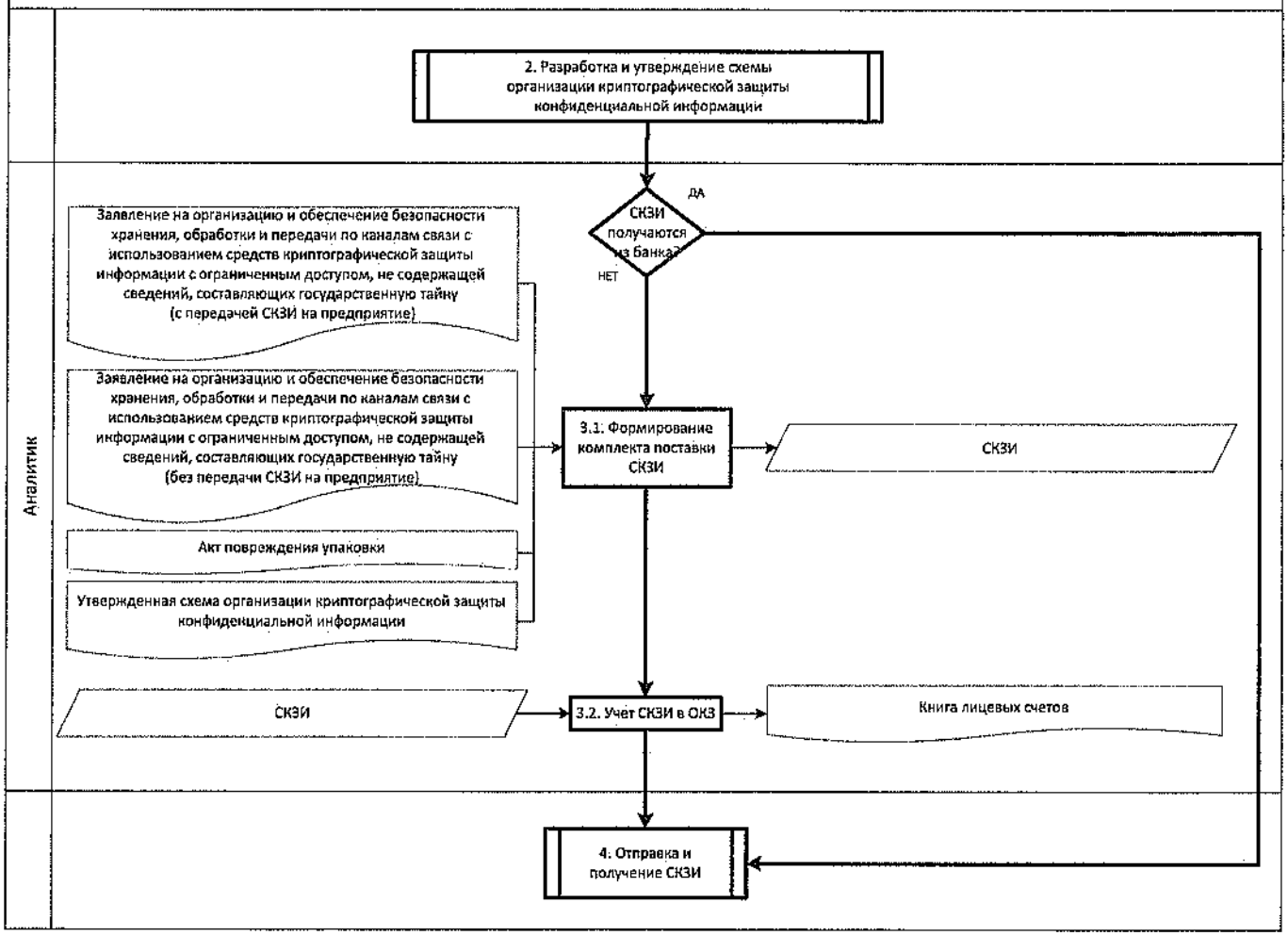


1. Подпроцесс «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации»

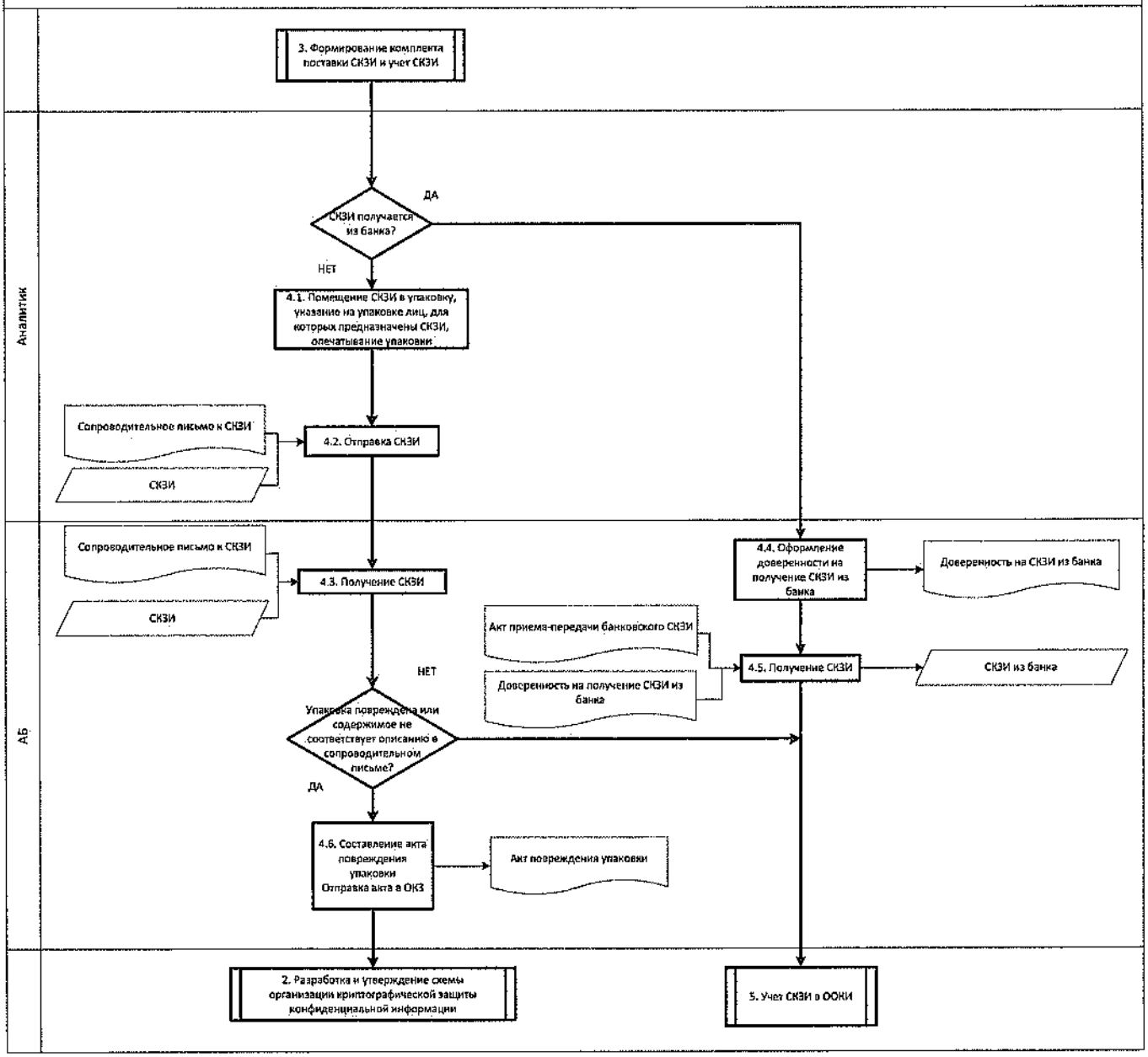



2. Подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации»
Аналитик
Начальник Управления ИБ
1. Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации
12. Вывод из эксплуатации и уничтожение СКЗИ
ИЛИ
Заявление на организацию 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 (с передачей СКЗИ на предприятие)
Заявление на организацию 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 (без передачи СКЗИ на предприятие)
Скан-копия Приказа о назначении администраторов безопасности и лиц их замещающих
Заявление на услугу Администратора безопасности
Скан-копия Перечня лиц, допускаемых к самостоятельной работе с СКЗИ
Скан-копия Приказа о предоставлении прав подписей в системе(ах)
Скан-копия Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Скан-копия Заключения о сдаче зачетов
Скан-копия Акта готовности СКЗИ к эксплуатации
Скан-копия Технического (аппаратного) журнала (если он ведется)
Акт об уничтожении СКЗИ
Акт повреждения упаковки
2.1. Разработка схемы организации криптографической защиты конфиденциальной информации
Схема организации криптографической защиты конфиденциальной информации
Схема организации криптографической защиты конфиденциальной информации
2.2. Утверждение схемы организации криптографической защиты конфиденциальной информации
Утвержденная Схема организации криптографической защиты конфиденциальной информации
ДА
СКЗИ выведено из эксплуатации?
НЕТ
Конец
3. Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ в ОКЗ»

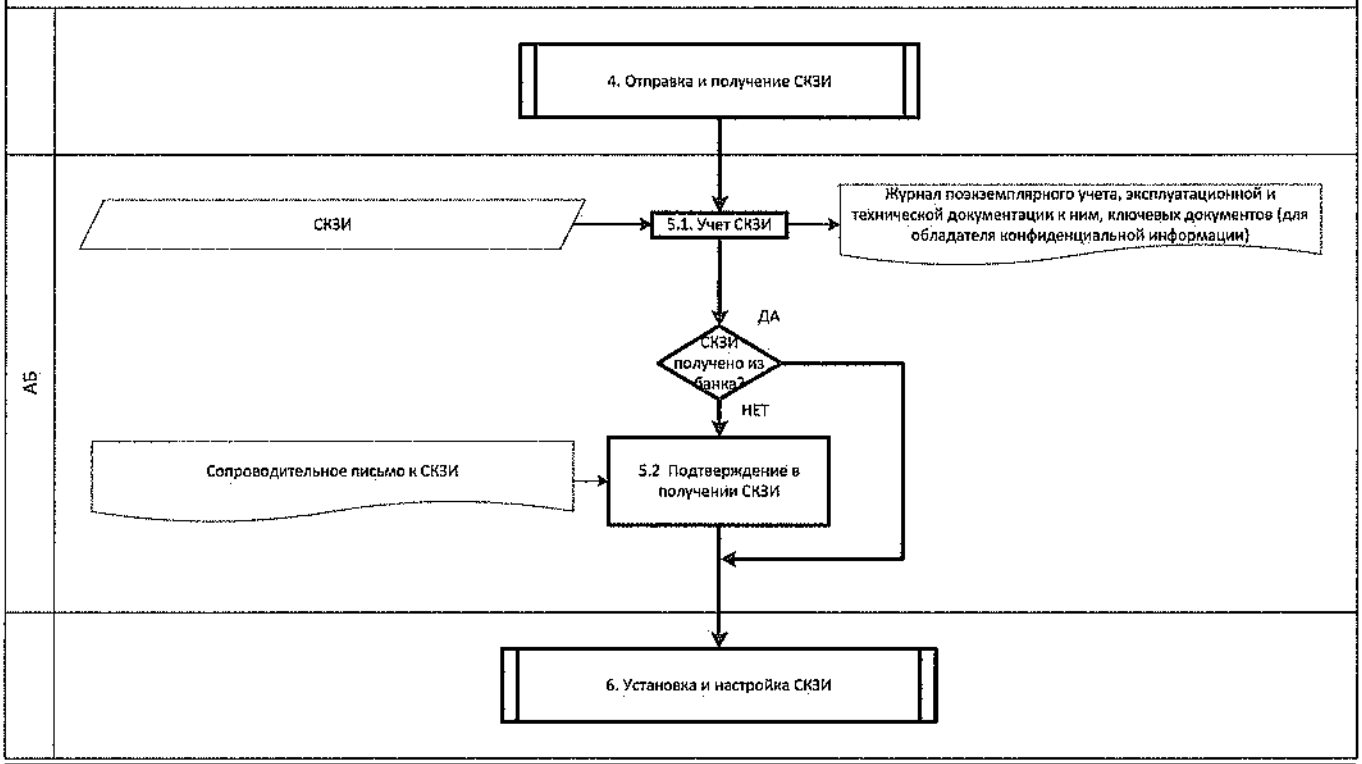
3. Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ в ОКЗ»



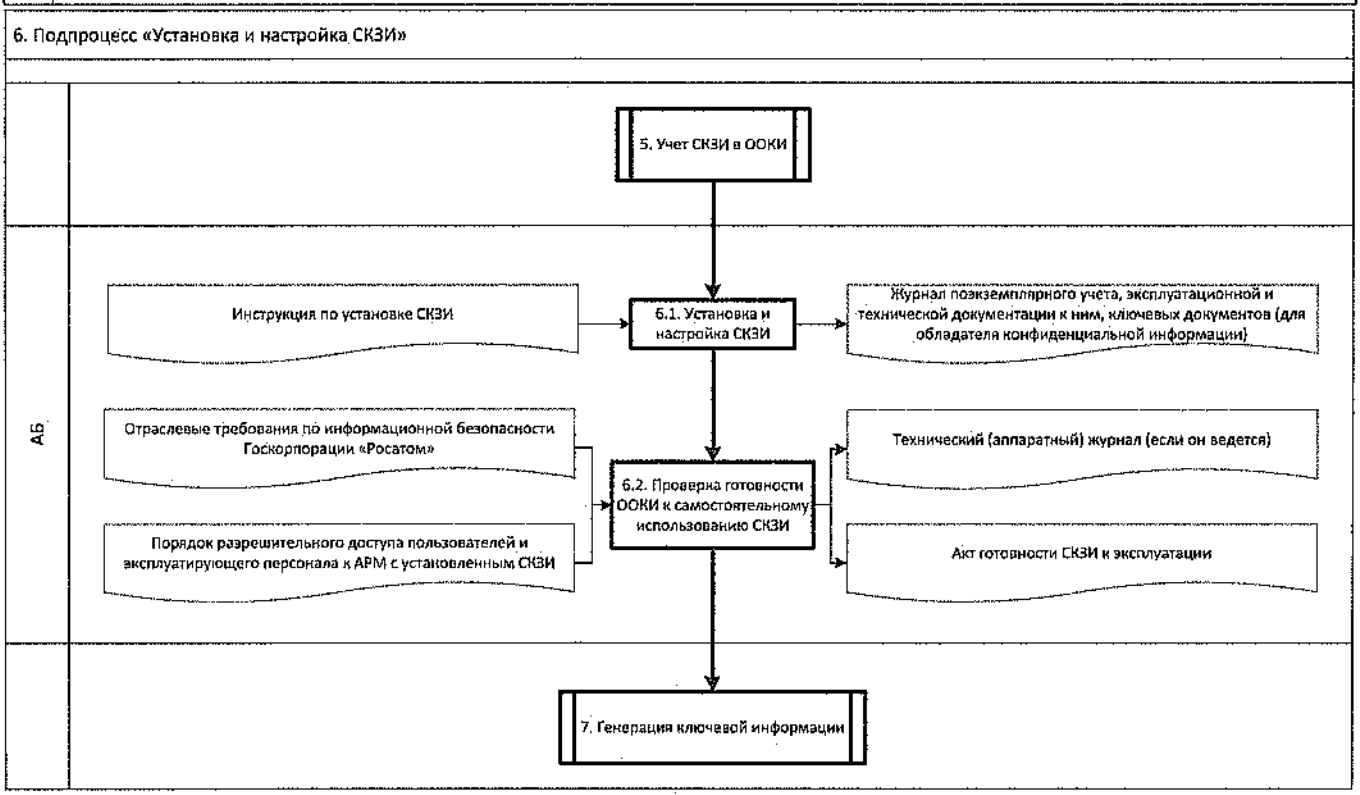
4. Подпроцесс «Отправка и получение СКЗИ»

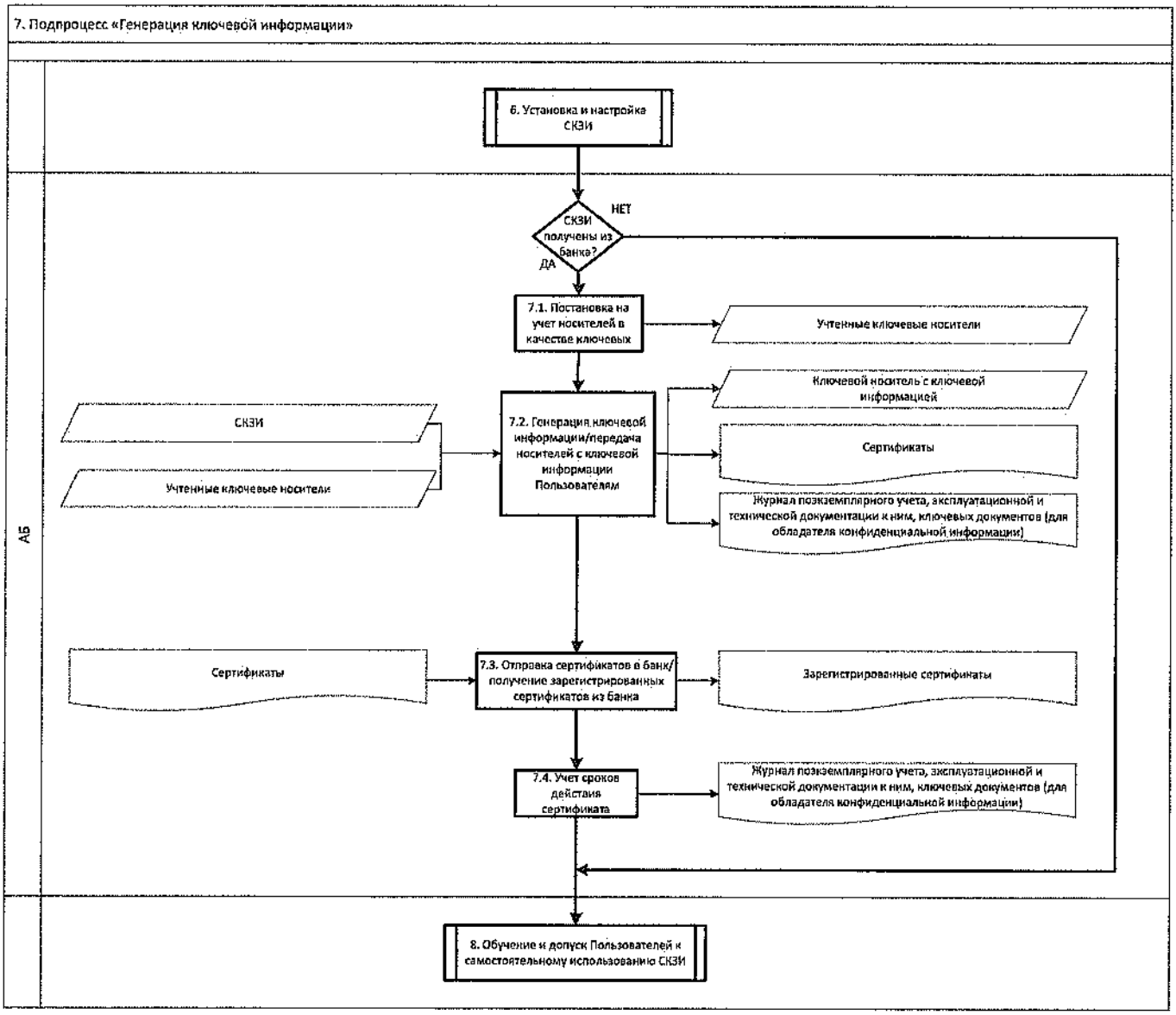


5. Подпроцесс «Учет СКЗИ в ООКИ»

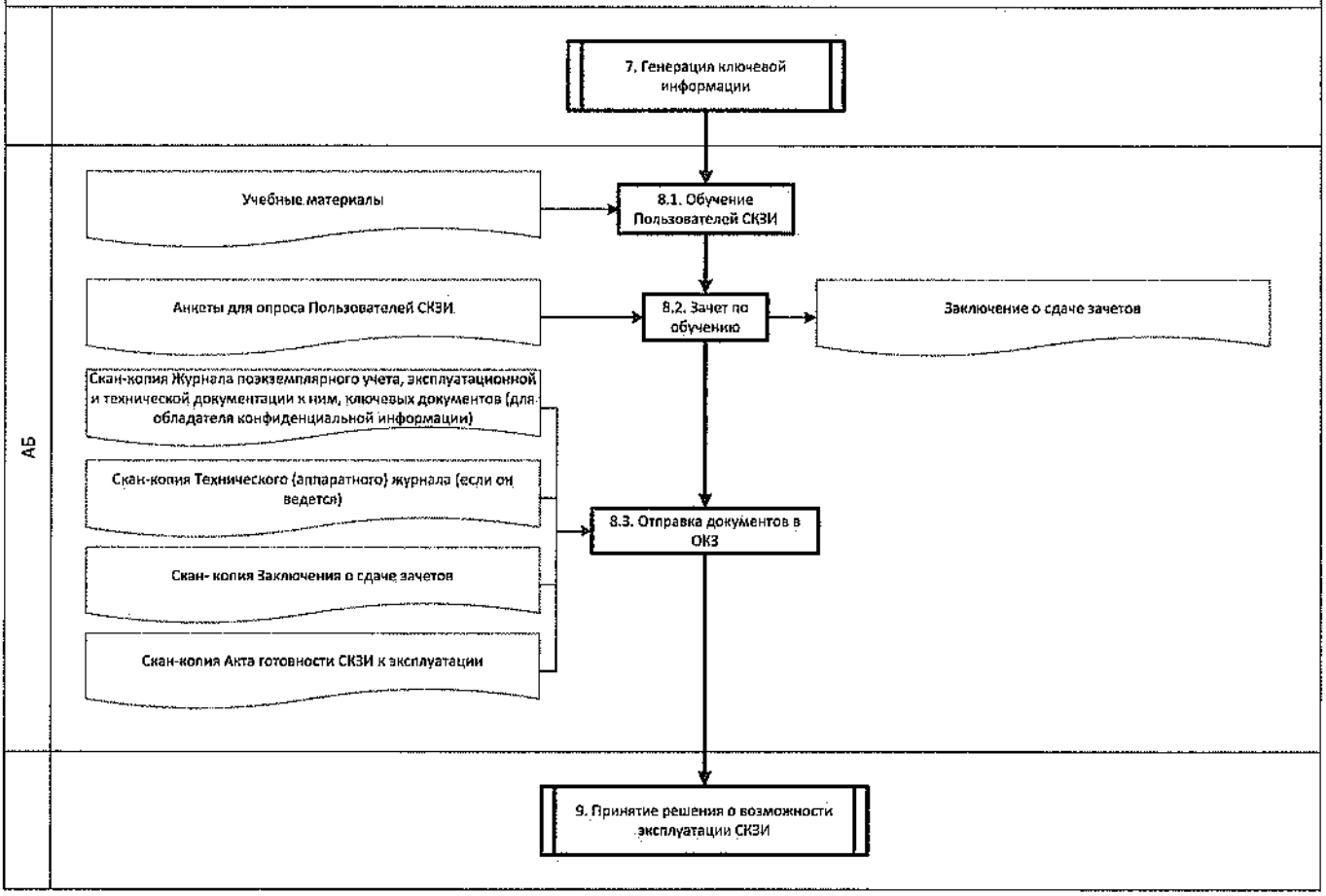


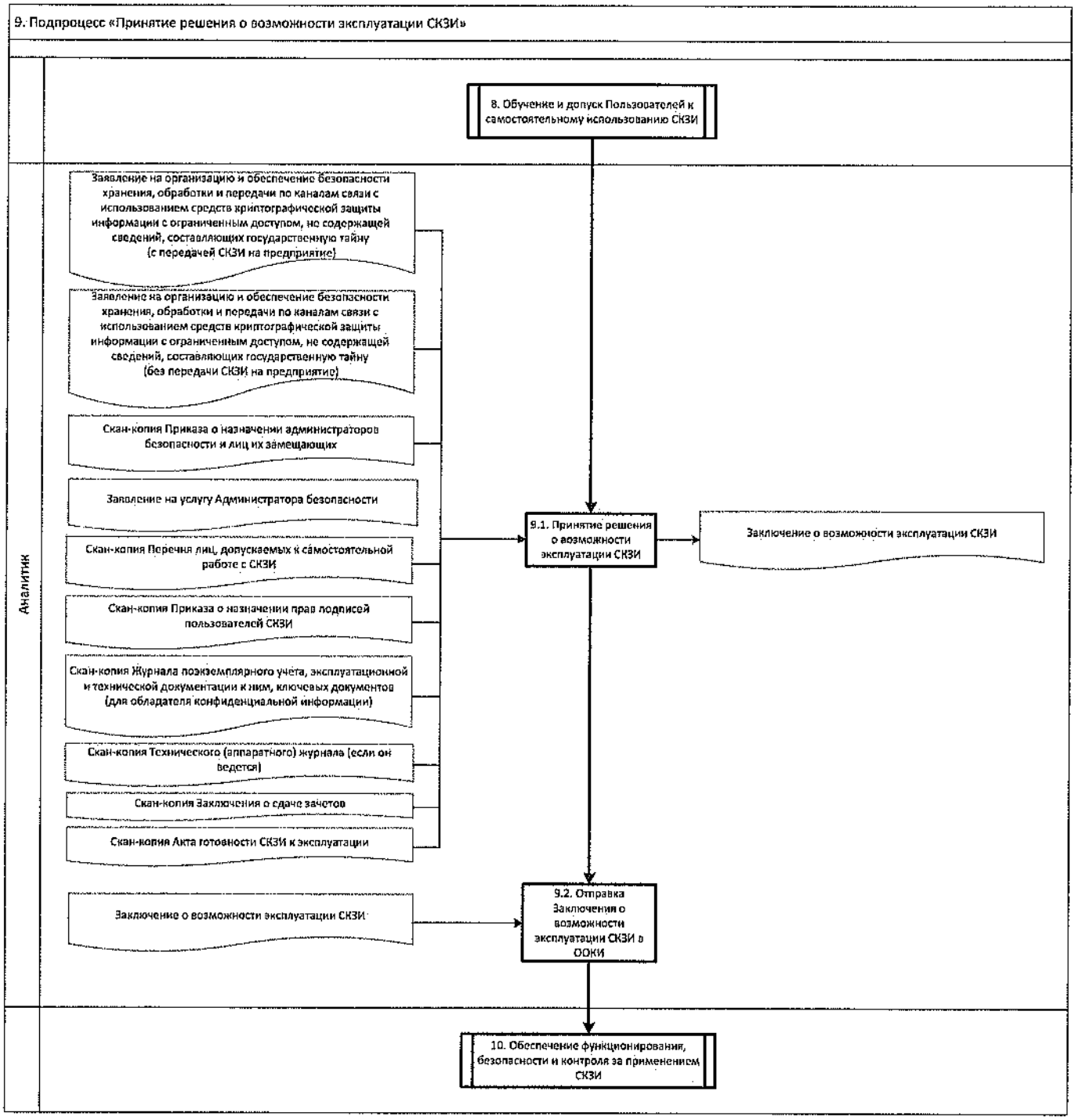
6. Подпроцесс «Установка и настройка СКЗИ»

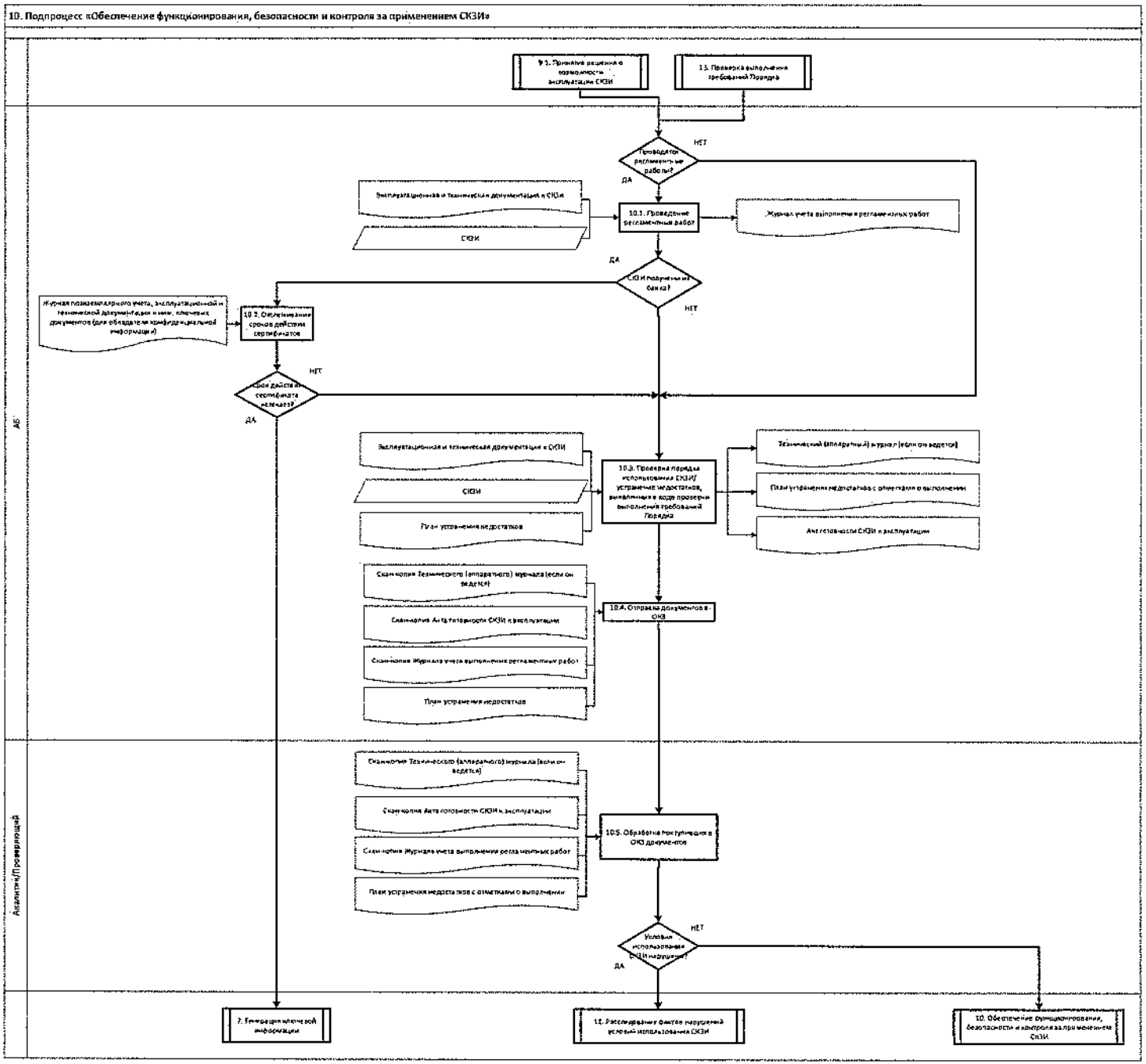


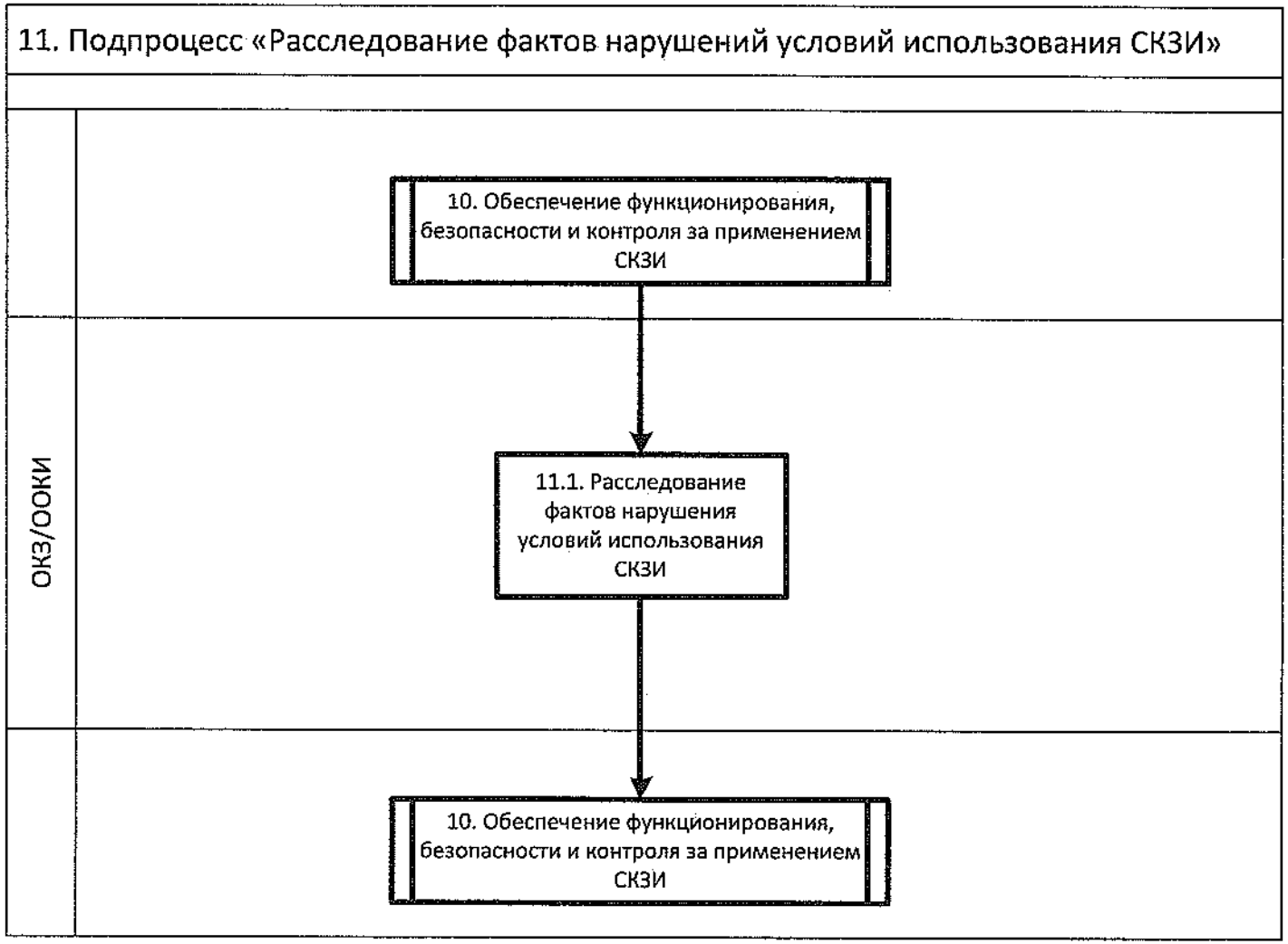

7. Подпроцесс «Генерация ключевой информации»
АБ
6. Установка и настройка СКЗИ
СКЗИ получены из Банка?
НЕТ
ДА
7.1. Постановка на учет носителей в качестве ключевых
Учтенные ключевые носители
СКЗИ
Учтенные ключевые носители
7.2. Генерация ключевой информации/передача носителей с ключевой информации Пользователям
Ключевой носитель с ключевой информацией
Сертификаты
Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Сертификаты
7.3. Отправка сертификатов в банк/ получение зарегистрированных сертификатов из банка
Зарегистрированные сертификаты
7.4. Учет сроков действия сертификата
Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
8. Обучение и допуск Пользователей к самостоятельному использованию СКЗИ

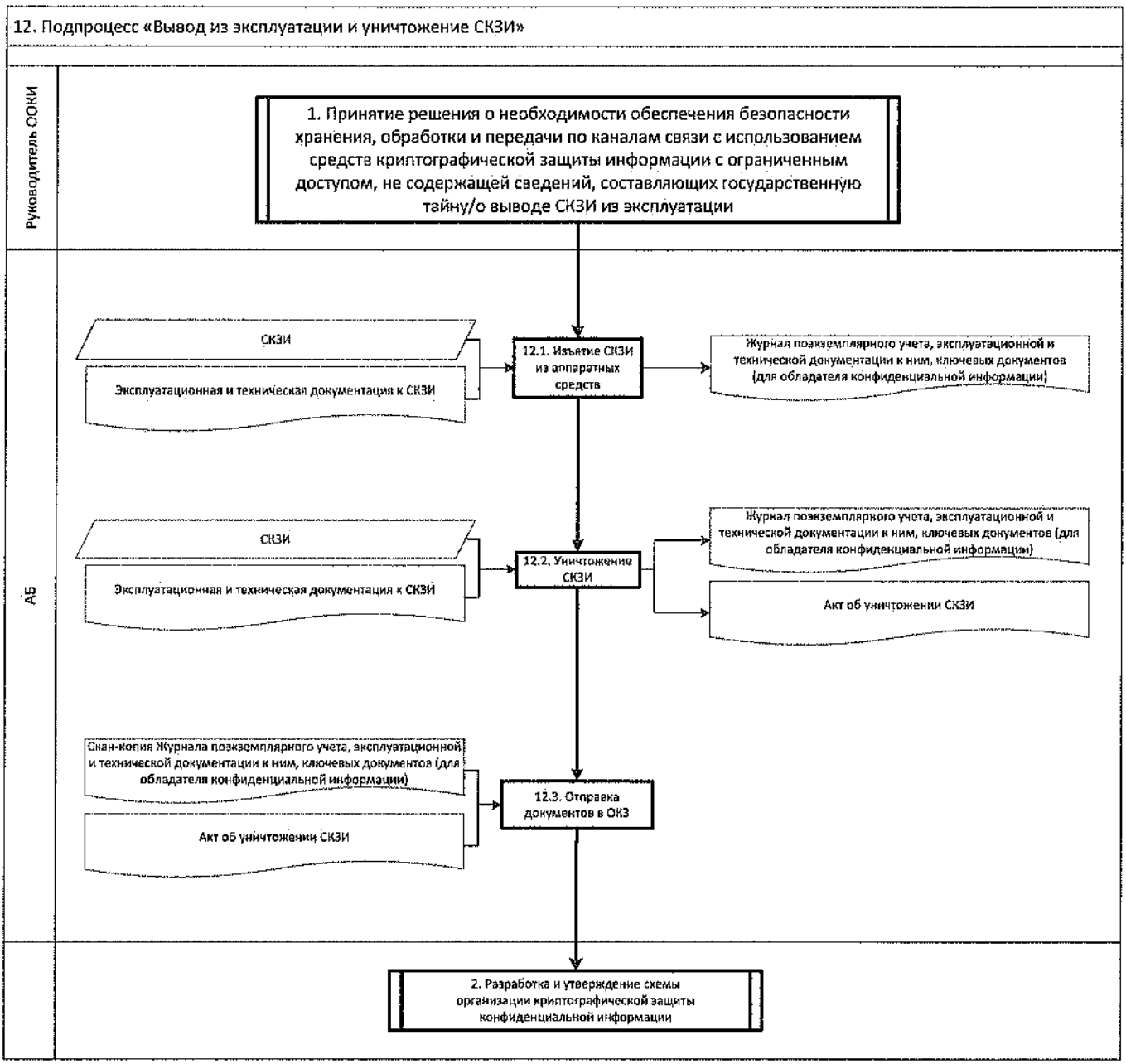
8. Подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ»

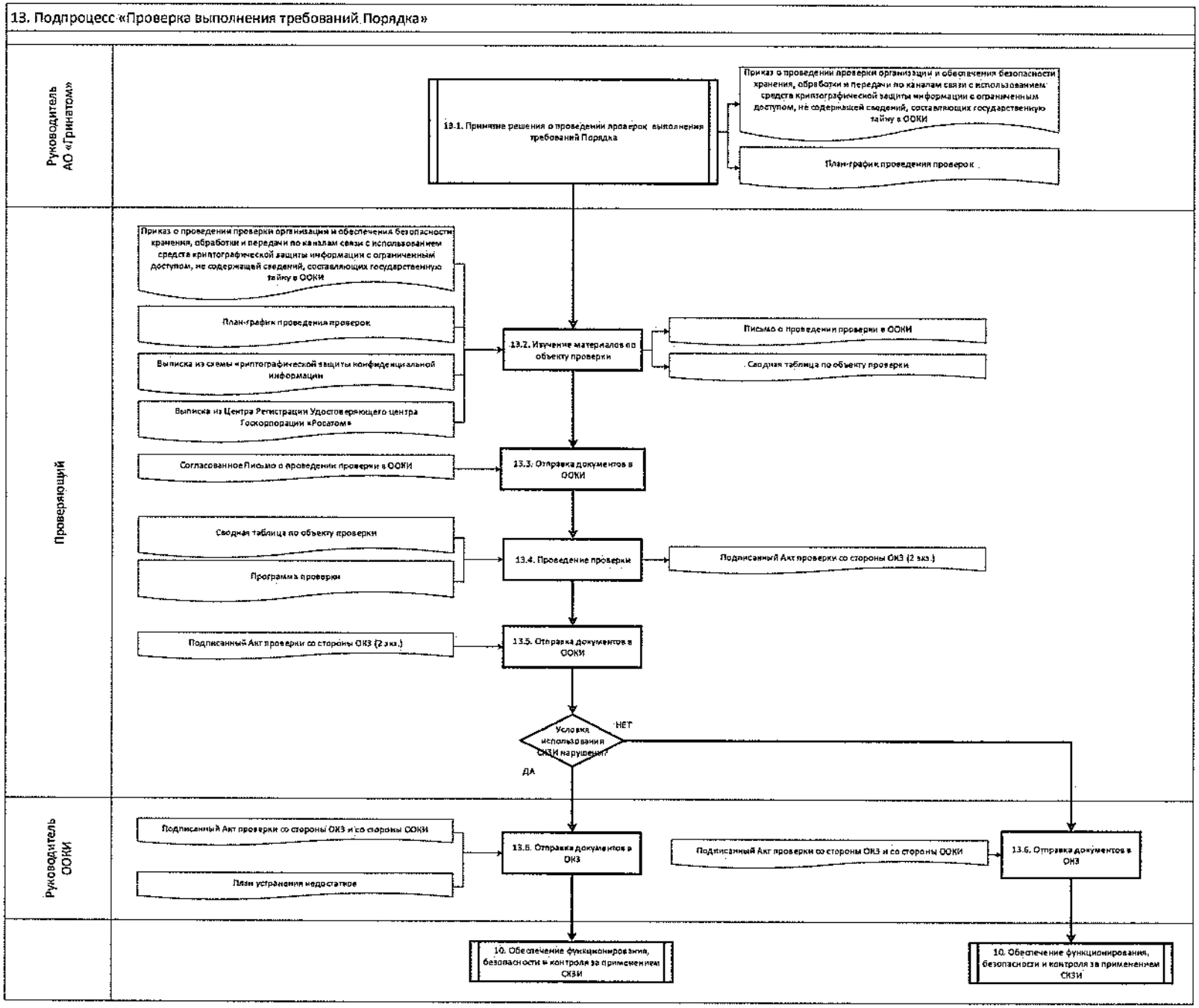



9. Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»
Аналитик
8. Обучение и допуск Пользователей к самостоятельному использованию СКЗИ
Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (с передачей СКЗИ на предприятие)
Заявление на организацию 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 (без передачи СКЗИ на предприятие)
Скан-копия Приказа о назначении администраторов безопасности и лиц их замещающих
Заявление на услугу Администратора безопасности
Скан-копия Перечня лиц, допускаемых к самостоятельной работе с СКЗИ
Скан-копия Приказа о назначении прав подписей пользователей СКЗИ
Скан-копия Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Скан-копия Технического (аппаратного) журнала (если он ведется)
Скан-копия Заключения о сдаче зачетов
Скан-копия Акта готовности СКЗИ к эксплуатации
9.1. Принятие решения о возможности эксплуатации СКЗИ
Заключение о возможности эксплуатации СКЗИ
Заключение о возможности эксплуатации СКЗИ
9.2. Отправка Заключения о возможности эксплуатации СКЗИ в ООКИ
10. Обеспечение функционирования, безопасности и контроля за применением СКЗИ


10. Подпроцесс «Обеспечение функционирования, безопасности и контроля за применением СКЗИ»
9.1. Принятие решения о возможности эксплуатации СКЗИ
13. Проверка выполнения требований Порядка
Администратор безопасности
Аналитик/Программист
НЕТ
Проводятся регламентные работы?
ДА
Эксплуатационная и техническая документация к СКЗИ
СКЗИ
10.1. Проведение регламентных работ
Журнал учета выполнения регламентных работ
ДА
СКЗИ и ключевые документы выведены из эксплуатации?
НЕТ
Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
10.2. Отслеживание сроков действия сертификатов
НЕТ
Срок действия сертификата истекает?
ДА
Эксплуатационная и техническая документация к СКЗИ
СКЗИ
План устранения недостатков
10.3. Проверка порядка использования СКЗИ/ устранение недостатков, выявленных в ходе проверки выполнения требований Порядка
Технический (аппаратный) журнал (если он ведется)
План устранения недостатков с отметками о выполнении
Акт готовности СКЗИ к эксплуатации
Скан-копия Технического (аппаратного) журнала (если он ведется)
Скан-копия Акта готовности СКЗИ к эксплуатации
Скан-копия Журнала учета выполнения регламентных работ
План устранения недостатков
10.4. Отправка документов в ОКЗ
Скан-копия Технического (аппаратного) журнала (если он ведется)
Скан-копия Акта готовности СКЗИ к эксплуатации
Скан-копия Журнала учета выполнения регламентных работ
План устранения недостатков с отметками о выполнении
10.5. Обработка поступивших в ОКЗ документов
Условия использования СКЗИ нарушены?
НЕТ
ДА
7. Генерация ключевой информации
12. Расследование фактов нарушений условий использования СКЗИ
10. Обеспечение функционирования, безопасности и контроля за применением СКЗИ


11. Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»
ОКЗ/ООКИ
10. Обеспечение функционирования, безопасности и контроля за применением СКЗИ
11.1. Расследование фактов нарушения условий использования СКЗИ
10. Обеспечение функционирования, безопасности и контроля за применением СКЗИ


12. Подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ»
Руководитель ООКИ
АБ
1. Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации
СКЗИ
Эксплуатационная и техническая документация к СКЗИ
12.1. Изъятие СКЗИ из аппаратных средств
Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
СКЗИ
Эксплуатационная и техническая документация к СКЗИ
12.2. Уничтожение СКЗИ
Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Акт об уничтожении СКЗИ
Скан-копия Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Акт об уничтожении СКЗИ
12.3. Отправка документов в ОКЗ
2. Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации


13. Подпроцесс «Проверка выполнения требований Порядка»
Руководитель АО «Гринатом»
Проверяющий
Руководитель ООКИ
13.1. Принятие решения о проведении проверок выполнения требований Порядка
Приказ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ
План-график проведения проверок
Приказ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ
План-график проведения проверок
Выписка из схемы криптографической защиты конфиденциальной информации
Выписка из Центра Регистрации Удостоверяющего центра Госкорпорации «Росатом»
13.2. Изучение материалов по объекту проверки
Письмо о проведении проверки в ООКИ
Сводная таблица по объекту проверки
Согласованное Письмо о проведении проверки в ООКИ
13.3. Отправка документов в ООКИ
Сводная таблица по объекту проверки
Программа проверки
13.4. Проведение проверки
Подписанный Акт проверки со стороны ОКЗ (2 экз.)
Подписанный Акт проверки со стороны ОКЗ (2 экз.)
13.5. Отправка документов в ООКИ
Условия использования СКЗИ нарушены?
НЕТ
ДА
Подписанный Акт проверки со стороны ОКЗ и со стороны ООКИ
План устранения недостатков
13.6. Отправка документов в ОКЗ
Подписанный Акт проверки со стороны ОКЗ и со стороны ООКИ
13.6. Отправка документов в ОКЗ
10. Обеспечение функционирования, безопасности и контроля за применением СКЗИ
10. Обеспечение функционирования, безопасности и контроля за применением СКЗИ

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. Форма приказа о назначении Администраторов безопасности и лиц их замещающих

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

ПРИКАЗ

«__» _____ 20__ г. № _____
(дата)

О назначении администраторов безопасности и лиц их замещающих

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

ПРИКАЗЫВАЮ:

1. Назначить администраторами безопасности и возложить функции органа криптографической защиты по организации работ с СКЗИ, выработки соответствующих инструкций для пользователей, контроля за соблюдением требований безопасности, а также функции доверенного лица удостоверяющего центра по приему заявлений на выдачу сертификатов ключей проверки электронной подписи и по вручению сертификатов ключей проверки электронных подписей от имени удостоверяющего центра на следующих сотрудников:

   ФИО (полностью) _____
   Должность, подразделение _____
   Контактный телефон _____
   E-mail _____

   ФИО (полностью) _____
   Должность, подразделение _____
   Контактный телефон _____
   E-mail _____
2. Администраторам безопасности провести инструктаж и обучение Пользователей СКЗИ и ознакомить под расписку с правилами эксплуатации СКЗИ.
3. Контроль исполнения настоящего Приказа оставляю за собой.

_____ _____ _____
(должность руководителя) (подпись руководителя) (Ф.И.О. руководителя)

Приложение №5. Форма Заявления на услугу Администратора безопасности

Заявление
на услугу Администратора безопасности

ПОДКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ
(нужное подчеркнуть)

« _____ » _____ 20 _____ г.

_____

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____

в рамках оказания услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств запрашивает предоставление услуги Администратора безопасности (код услуги GEN.23), для обслуживания защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем согласно перечню

№ п/п	Пользователь СКЗИ (должность, Ф.И.О.)	Установленное СКЗИ	Автоматизированная/ информационная система	Учетный номер АРМ, на котором установлено СКЗИ	Адрес месторасположения АРМ

<УПОЛНОМОЧЕННОЕ ДОЛЖНОСТНОЕ ЛИЦО> _____ / _____
(подпись) (ФИО)

М.П.

Приложение №5.1 Форма Заявления на услугу по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя

Заявление
на услугу по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя

ПОДКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ «_____» _____ 20 _____ г.
(нужное подчеркнуть)

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____

в рамках оказания услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств запрашивает предоставление услуги по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя (код услуги GEN.43), согласно перечню:

№ п/п	Владелец ключа (Ф.И.О., полностью)	Тип ключа	Сроки действия ключа	Автоматизированная/ информационная система	Учетный номер АРМ, на котором установлено СКЗИ	Адрес месторасположения АРМ

Уполномоченное должностное лицо

_____ _____ _____
(подпись) (ФИО)

М.П.

Приложение №6. Перечень лиц, допускаемых к самостоятельной работе с СКЗИ

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

ПРИКАЗ

«____» _____ 20 ____ г. № _____

(дата)

О назначении лиц, допускаемых к самостоятельной работе с СКЗИ

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

ПРИКАЗЫВАЮ:

1. К работе с СКЗИ допустить следующих работников:

№	ФИО пользователя	Структурное подразделение	Должность

2. Контроль исполнения настоящего Приказа оставляю за собой.

_____ _____ _____

(должность руководителя) (подпись руководителя) (Ф.И.О. руководителя)

Приложение №7. Форма Приказа о предоставлении прав подписей в системе(ах)

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

ПРИКАЗ

«____» _____ 20___ г. № _____

(дата)

О предоставлении прав подписей в системе(ах) <НАИМЕНОВАНИЕ СИСТЕМЫ>

В соответствии с пунктами 7.5-7.6 Инструкции Банка России от 30.05.2014 №153-И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов» для осуществления платежей с использованием системы <НАИМЕНОВАНИЕ СИСТЕМЫ>

ПРИКАЗЫВАЮ:

1. Предоставить право первой подписи в системе <НАИМЕНОВАНИЕ СИСТЕМЫ>:

_____
(Ф.И.О., должность)

_____
(Ф.И.О., должность)

2. Предоставить право второй подписи в системе <НАИМЕНОВАНИЕ СИСТЕМЫ>:

_____
(Ф.И.О., должность)

_____
(Ф.И.О., должность)

3. Предоставить право запроса выписки в системе <НАИМЕНОВАНИЕ СИСТЕМЫ>:

_____
(Ф.И.О., должность)

_____
(Ф.И.О., должность)

2. Контроль исполнения настоящего Приказа оставляю за собой.

_____	_____	_____
(должность руководителя)	(подпись руководителя)	(Ф.И.О. руководителя)

Приложение №8.1 Заявление на СКЗИ (с передачей СКЗИ)

Заявление
на организацию 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
(с передачей СКЗИ)

« _____ » _____ 20 _____ г.

_____
(наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____

просит ОКЗ АО «Гринатом» организовать и обеспечить безопасность хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в рамках услуг лицензируемой деятельности для следующих автоматизированных рабочих мест (АРМ), указанных в таблице, для чего, в соответствии с «ЕОМУ по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» в организации, расположенной по адресу:

_____

функции ОКЗ возлагаются на администраторов безопасности, назначенных Приказом № _____ от _____ . Копия Приказа прилагается.

№ п/п	Пользователь СКЗИ (Ф.И.О. полностью)	Вид защищаемой информации	Автоматизированная/ информационная система	Тип СКЗИ	Учетный номер АРМ, на котором установлено СКЗИ	Подразделение (предприятие)	Адрес месторасположения АРМ	Общесистемное программное обеспечение, установленное на АРМ
1								

Администратор безопасности

_____/_____
(подпись) (ФИО)

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ДОЛЖНОСТНОГО ЛИЦА>

_____ _____/_____
(подпись) (ФИО)

М.П.

Приложение №8.2 Заявление на СКЗИ (без передачи СКЗИ)

Заявление
на организацию 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
(без передачи СКЗИ)

« _____ » _____ 20 _____ г.

_____
(наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
фамилия, имя, отчество

действующего на основании _____

просит ОКЗ АО «Гринатом» организовать и обеспечить безопасность хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в рамках услуг лицензируемой деятельности для следующих автоматизированных рабочих мест (АРМ), указанных в таблице, для чего, в соответствии с «ЕОМУ по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» в организации, расположенной по адресу:

_____

функции ОКЗ возлагаются на администраторов безопасности, назначенных Приказом № _____ от _____ . Копия Приказа прилагается.

№ п/п	Пользователь СКЗИ (Ф.И.О. полностью)	Вид защищаемой информации	Наименование СКЗИ, версия	Номер лицензии, код лицензии, код конечного пользователя	Автоматизированная/ информационная система	Учетный номер АРМ, на котором установлено СКЗИ	Подразделение	Адрес месторасположения АРМ	Общесистемное программное обеспечение, установленное на АРМ
1									

Администратор безопасности

_____/_____
(подпись) (ФИО)

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ДОЛЖНОСТНОГО ЛИЦА>

_____ _____/_____
(подпись) (ФИО)

М.П.

			№ п/п
			Краткое наименования предприятия
			Полное наименование предприятия
			Заявление о присоединении №
			Администратор безопасности (ФИО, Приказ/
			Пользователь СКЗИ (ФИО полностью)
			Тип используемого СКЗИ
			Серийный номер СКЗИ
			Автоматизированная/информационная система
			Учетный/серийный номер системного блока АРМ, на котором установлено СКЗИ
			Системный блок АРМ опечатан печатью №
			Адрес местоположения АРМ
			Программное обеспечение, установленное на АРМ
			Вид защищаемой информации
			Рег. номер заключения о сдаче зачетов
			Дата регистрации заключения о сдаче зачетов
			Рег. номер акта готовности
			Дата регистрации акта готовности
			Рег. номер лицевого счета / ЖПУ
			Дата регистрации лицевого счета / ЖПУ
			Рег. номер Приказа о лицах допускаемых к самостоятельной работе с СКЗИ
			Дата регистрации Приказа о лицах, допускаемых к самостоятельной работе с
			Рег. номер Приказа о предоставлении прав подписей в платежных системах
			Дата регистрации Приказа о предоставлении прав подписей в
			Заключение о возможности эксплуатации СКЗИ
			Примечание

Приложение №9. Схема организации криптографической защиты конфиденциальной информации (шаблон)

ГРИНАТОМ

Приложение №10. Книга лицевых счетов

**Приложение 1 к Инструкции,
утвержденной приказом Федерального агентства
правительственной связи и информации
при Президенте Российской Федерации
от 13.05.2001 г. № 152**

Книга лицевых счетов СКЗИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ

Начат «___» _____ 201___ г.
Окончен «___» _____ 201___ г.
На ____ листах

Опись лицевых счетов

1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		
34		
35		
36		
37		

41		
42		
43		
44		
45		
46		
47		
48		
49		
50		
51		
52		
53		
54		
55		
56		
57		
58		
59		
60		
61		
62		
63		
64		
65		
66		
67		
68		
69		
70		
71		
72		
73		
74		
75		
76		
77		

№ пп	Фамилия Инициалы	№ по картотеке	Расписка лица оформившего л/с	Отметки о местонахождении

Лицевой счет _____ тел. _____

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)			Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении	Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Приложение №11. Доверенность доверенного лица на получение СКЗИ в ОКЗ

ДОВЕРЕННОСТЬ

доверенного лица, наделенного правом получения средств криптографической защиты информации

г. _____ «____»_____20__г.

_____

_____

(наименование организации, включая организационно-правовую форму)

в лице_____,

(должность)

действующего на основании_____

уполномачивает_____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и когда выдан)

зарегистрированного по адресу: _____,

получать в Органе криптографической защиты АО «Гринатом» средства криптографической защиты информации.

Доверенное лицо наделяется правом подписи в соответствующих документах для исполнения поручений, определенных 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.

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ДОЛЖНОСТНОГО ЛИЦА>

_____ _____/_____

(подпись) (Ф.И.О.)

м.п.

Приложение №12. Сопроводительное письмо к СКЗИ

Акционерное общество «Гринатом»
(АО «Гринатом»)

1-й Нагатинский проезд, д. 10, стр. 1,
Москва, 115230
Телефон (499) 949-49-19, факс (499) 949-44-46
E-mail: info@greenatom.ru
ОКПО 64509942, ОГРН 1097746819720
ИНН 7706729736, КПП 770601001

«ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ЛИЦА»
«НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ»

«И.О.ФАМИЛИЯ»

_____ № _____

На № _____ от _____

О передаче СКЗИ

Уважаемый(ая) <ИМЯ, ОТЧЕСТВО>!

В ответ на Ваше «Заявление о присоединении к Договору на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств» и «Заявление на организацию 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» высылаем копии лицензий на право использования средств криптографической защиты информации.
Данный конверт необходимо передать в Орган криптографической защиты администратору безопасности.

Приложение: 1. Копии лицензий СКЗИ «КриптоПро CSP» – __ шт.

С уважением,

Начальник Отдела криптографической защиты — <И.О. ФАМИЛИЯ> (по дов.

Исполнитель

Приложение №13. Акт повреждения упаковки

АКТ №_____

г. Москва «___» _____ 201__ г.

Администратор безопасности _____
(ФИО)

составил настоящий акт в том, что полученная упаковка повреждена <УКАЗАТЬ СТЕПЕНЬ ПОВРЕЖДЕНИЯ>.

Вывод:

В выводе указывается возможность/невозможность дальнейшего использования ключевой информации/СКЗИ в зависимости от степени повреждения упаковки.

В случае образования свободного доступа к содержимому упаковки, использование ключевой информации/СКЗИ невозможно.

_____/_____
(подпись) (Ф.И.О)

Приложение №14. Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)

Приложение 2 к Инструкции,
утвержденной приказом Федерального агентства
правительственной связи и информации
при Президенте Российской Федерации
от 13.05.2001 г. № 152

ЖУРНАЛ
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)

Начат: «___» _____ 20__ г.
Окончен: «___» _____ 20__ г.

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудников органа криптографической защиты, пользователей СКЗИ, произведших подключение (установку)	Дата подключения (установки) подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение №15. Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ

Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ

Москва 2020 г.

Оглавление

1. Общие положения

Настоящий документ описывает порядок разрешительного доступа эксплуатирующего персонала и пользователей к автоматизированным рабочим местам (АРМ) с установленными средствами криптографической защиты (СКЗИ).

2. Требования к размещению технических средств установленными СКЗИ

При размещении технических средств с установленными СКЗИ необходимо выполнять следующие требования:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленными СКЗИ, 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 СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования к программному и аппаратному обеспечению

Технические средства с установленными СКЗИ должны отвечать следующим требованиям:

- На технических средствах, оснащенных СКЗИ должно использоваться только лицензионное программное обеспечение фирм-производителей, либо ПО, сертифицированное ФСБ. Указанное ПО не должно содержать средств разработки или отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование СКЗИ. В случае технологических потребностей организации, эксплуатирующей СКЗИ, в использовании иного программного обеспечения, его применения должно быть санкционировано администратором безопасности. В любом случае ПО не должно содержать в себе возможностей, позволяющих:
  - модифицировать содержимое произвольных областей памяти;
  - модифицировать собственный код и код других подпрограмм;
  - модифицировать память, выделенную для других подпрограмм;
  - передавать управление в область собственных данных и данных других подпрограмм;
  - несанкционированное модифицировать файлы, содержащие исполняемые кода при их хранении на жестком диске;

- использовать недокументированные фирмами-разработчиками функции.

- На ПЭВМ одновременно может быть установлена только одна разрешенная ОС;
- В BIOC ПЭВМ должны быть определены установки, исключающие возможность загрузки ОС, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС;
- Средствами BIOS должна быть отключена возможность отключения пользователями PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в PCI разъем;
- Вход в BIOS должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС;
- Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты;
- Программные модули СКЗИ (прикладного ПО со встроенным СКЗИ) должны быть доступны только по чтению/запуску (в атрибутах файлов запрещена запись и модификация);
- Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

4. Защита информации от НСД

При использовании СКЗИ необходимо принять следующие организационные меры:

- Предоставить права доступа к рабочим местам с установленным СКЗИ только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на СКЗИ;
- Запретить осуществление несанкционированного администратором безопасности копирования ключевых носителей;
- Запретить передачу передачу ключевых носителей лицам, к ним недопущенным;
- Запретить использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ;
- Запретить запись на ключевые носители посторонней информации;
- Запретить оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки;
- Хранить ключевые носители в опечатываемых пеналах, которые в свою очередь должны хранить в запираемых и опечатываемых сейфах.

Пользователь несет персональную ответственность за хранение личных ключевых носителей;

- Сдать ключевые носители в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей;
- Немедленно уведомлять Удостоверяющий центр о фактах утраты или недостачи ключевых носителей, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации;
- Запрещается разглашать содержимое носителей ключевой информации и передавать носители лицам к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п., иные средства отображения информации;
- Перед началом процесса установки ПО со встроенными модулями СКЗИ, либо автономных программных модулей СКЗИ должен осуществляться контроль целостности устанавливаемого ПО;
- При каждом запуске ПЭВМ с установленным СКЗИ должен осуществляться контроль целостности программного обеспечения, входящего в состав СКЗИ, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ;
- Администратор безопасности должен периодически (не реже 1 раза в год) менять пароль на вход в BIOS;
- В случае обнаружения «посторонних» (незарегистрированных) программ или нарушения целостности программного обеспечения работа должна быть прекращена;
- Пользователь должен запускать только те приложения, которые разрешены администратором;
- Администратор безопасности должен сконфигурировать ОС, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:
    - Не использовать нестандартные, измененные или отладочные ОС;
    - Исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;
    - Исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек;
    - Правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности;
    - ОС должна быть настроена только для работы с СКЗИ. Все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
    - Всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права;

- Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
  - Системный реестр;
  - Файлы и каталоги;
  - Временные файлы;
  - Журналы системы;
  - Файлы подкачки;
  - Кэшируемая информация (пароли и т.п.);
  - Отладочная информация.

  Кроме того, необходимо организовать затирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.
- Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;
- Необходимо регулярно устанавливать пакеты обновления безопасности ОС, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
- В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети;
- При использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых ОС, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты;
- Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита;
- Организовать и использовать комплекс антивирусной защиты;

- Исключить одновременную работу в ОС с работающим СКЗИ и загружаемой ключевой информацией нескольких пользователей.

Приложение №16. Технический (аппаратный) журнал

Технический (аппаратный) журнал

№ п.п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографческий номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	

Приложение №17. Акт готовности СКЗИ к эксплуатации

Акт готовности СКЗИ к эксплуатации №_____

г. _____ «_____»_____ 20 _____ г.

Администратор безопасности _____,
(ФИО полностью., e-mail)

составил настоящий акт в том, что произведена проверка готовности АРМ обладателя конфиденциальной информации

_____
(Наименование организации, фактический адрес)

к эксплуатации СКЗИ на соответствие «ЕОМУ по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» и требованиям «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», утвержденной Приказом ФАПСИ при Президенте РФ № 152 от 13.06.2001 г.

Произведена проверка выполнения «Порядка разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ» Приложение №15 к Порядку организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, операционная система настроена в соответствии с документацией на СКЗИ.

СКЗИ установлено:

№ п/п	ФИО пользователя СКЗИ полностью	№ помещения и раб.места	Уч.№ ПЭВМ	ПЭВМ опечатана печатью №	Наименование СКЗИ и версия	Версия ОС	Установлено сертифицированное	
							Антивирусное средство	СЗИ от НСД

Вывод:

Оборудование АРМ соответствует «ЕОМУ по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» и требованиям «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», утвержденной Приказом ФАПСИ при Президенте РФ № 152 от 13.06.2001 г., их функционирование проверено и готово к эксплуатации с установленным СКЗИ.

_____ / _____
(подпись) (ФИО адм.безопасности)

Управление информационной безопасности

Обучение пользователей правилам работы со средствами криптографической защиты информации

ГРИНАТОМ

Программа обучения пользователей правилами работы с СКЗИ

- ✓ Понятие безопасности информации
- ✓ Типичные причины нарушений пользователей
- ✓ Требования к эксплуатации СКЗИ
- ✓ Правила работы с СКЗИ
- ✓ Меры предосторожности при работе с паролями
- ✓ Ответственность за нарушение правил

Корпоративные ценности АО «Гринатом»

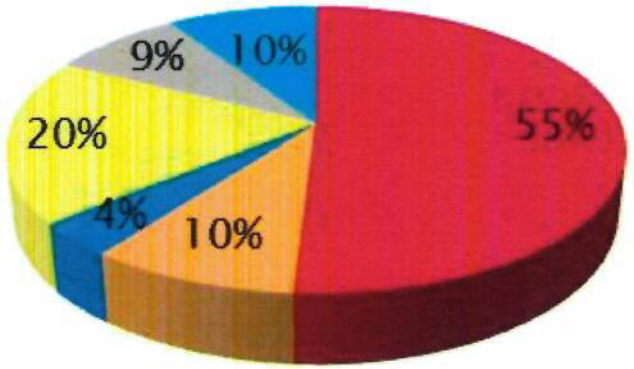
Корпоративные ценности компании - система принципов, на которых основывается ее деятельность, организация труда и стиль поведения сотрудников.
У компании «Гринатом» 6 ценностей:

- ✓ Ответственность за результат
- ✓ Эффективность
- ✓ Уважение
- ✓ Безопасность
- ✓ Единая команда
- ✓ На шаг впереди

Безопасность – наивысший приоритет. В нашей работе мы в первую очередь обеспечиваем полную безопасность людей и окружающей среды. В безопасности нет мелочей – мы знаем правила безопасности и выполняем их, пресекая нарушения. Особое внимание мы уделяем надежности/доступности сервисов и корпоративных информационных систем. Наши клиенты могут быть спокойны за сохранность их данных. Мы соблюдаем все внутренние регламенты и процедуры.

ГРИНАТОМ

Влияние осведомленности пользователей на уровень информационной безопасности



- Ошибки персонала
- Нечестные сотрудники
- Вирусы
- Проблемы электропитания
- Обиженные сотрудники
- Внешние нападения

Более 50 процентов от общего объема нарушений и преступлений составляют ошибки персонала

Обеспечение безопасности – задача всех работников организации

Пожарная безопасность обеспечивается не только пожарной дружиной, но и всеми сотрудниками, которые соблюдают установленные правила (не бросают окурки, не пользуются неисправленными электроприборами и т.п.).

Состояние безопасности предприятия (как информационной, так и пожарной) **зависит от каждого**

В состав системы обеспечения информационной безопасности входят все сотрудники, имеющие прямое или косвенное отношение к системе

ГРИНАТОМ

Типичные причины нарушений пользователей

- Использование ресурсов не по назначению

Действие:

использование предоставленных сотрудникам аппаратно-программных средств ГК «Росатом» в личных (иных, кроме служебных) целях

Последствия:

потери из-за непроизводительного использования ресурсов АС и рабочего времени, создание помех и дополнительных угроз основным технологическим процессам

Контрмеры:

запрет или введение существенных ограничений на использование аппаратно-программных средств не по назначению (в личных целях)

Пользователь не имеет право использовать предоставленные ему ресурсы ГК «Росатом» в личных целях

Типичные причины нарушений пользователей

- Непринятие мер по предотвращению порчи или утраты оборудования

Действие:

неумышленная порча или непринятие мер по предотвращению порчи или утраты (хищения) технических средств, носителей информации, повреждение линий связи...

Последствия:

прямой материальный ущерб. Частичный или полный отказ системы - потери из-за простоев и затраты на восстановление ресурсов и работоспособности (технопогических процессов)

Контрмеры:

повышение ответственности за сохранность и физическую целостность аппаратных средств (материальная компенсация в пользу ГК «Росатом»)

Если пользователь оказался свидетелем порчи имущества ГК «Росатом» он должен незамедлительно сообщить о произошедшем непосредственному руководителю

Типичные причины нарушений пользователей

- Несанкционированное изменение конфигурации устройств и программ

Действие:

самовольное изменение состава и конфигурации используемых аппаратных и программных средств, отключение или изменение режимов работы оборудования и программ

Последствия:

частичный или полный отказ системы.
Потери из-за простоев и затраты на восстановление ресурсов и работоспособности (технологических процессов), внедрение «жучков»

Контрмеры:

введение запретов и повышение ответственности за физическую целостность аппаратно-программных ресурсов

Пользователю запрещается: вскрытие системного блока ЭВМ (для протирания пыли), мыши, клавиатуры, добавление в аппаратную часть ЭВМ дополнительных плат для увеличения производительности, инсталляция сторонних программ, внесение изменений в настройки аппаратной части ЭВМ, программных продуктов, установленных на ЭВМ.

ГРИНАТОМ

Типичные причины нарушений пользователей

- Инсталляция и/или запуск сторонних программ на рабочих станциях

Действие:

несанкционированное внедрение и использование неразрешенных и сторонних программ, не имеющих отношения к производственной деятельности

Последствия:

необоснованный расход ресурсов системы (загрузка процессора, каналов связи, оперативной памяти и памяти на внешних носителях), возникновение конфликтов ПО, заражение компьютеров вирусами

Контрмеры:

запрет самостоятельной разработки, установки и использования неучтенных, не разрешенных программ (не относящихся к производственному процессу)

ГРИНАТОМ

Типичные причины нарушений пользователей

- Отключение или создание помех для работы штатных антивирусных программ

Действие:

отключение или создание препятствий для работы антивирусных программ, неправильные действия в случае обнаружения вирусов

Последствия:

потери из-за заражения компьютера вирусами и распространение эпидемии на другие сервера и рабочие станции (потеря данных, компрометация конфиденциальных сведений, простои системы, затраты на восстановление)

Контрмеры:

повышение ответственности пользователей, внедрение более совершенных антивирусных средств

При обнаружении вирусного заражения ЭВМ пользователь обязан прекратить обработку информации на компьютере и сообщить о произошедшем в подразделение информационной безопасности, эксплуатирующей систему

ГРИНАТОМ

Типичные причины нарушений пользователей

- Использование нелицензионного программного обеспечения

Действие:

использование непицензионного программного обеспечения на компьютерах предприятий отрасли (пиратских копий программ)

Последствия:

судебные иски правообладателей на компенсацию ущерба, возбуждение уголовного дела по ст. 146 УК РФ «Нарушение авторских и смежных прав» и связанные с этим риски, потеря репутации, выход из строя ряда АС

Контрмеры:

повышение ответственности конечных пользователей и обслуживающего персонала, усиление контроля, применение средств создания замкнутой программной среды

ГРИНАТОМ

Типичные причины нарушений пользователей

- Нарушение порядка формирования, использования, хранения и резервного копирования критичной информации

Действие:

непреднамеренное удаление или искажение программ и файлов с важной (не обязательно конфиденциальной) информацией, ввод ошибочных данных и т.п.

Последствия:

потери из-за простоев и затраты на восстановление ресурсов и работоспособности

Контрмеры:

упорядочение работы (наведение порядка), повышение ответственности исполнителей, внедрение процедур резервного копирования важных данных

Типичные причины нарушений пользователей

- Самовольное создание и использование разделяемых сетевых ресурсов

Действие:

самовольное создание совместно используемых сетевых ресурсов (папок общего пользования) на своих компьютерах, несанкционированное удаление или изменение прав доступа к ним

Последствия:

создание дополнительных угроз вирусного проникновения и НСД, связанных с потерей данных или компрометацией конфиденциальных сведений, затруднение резервного копирования и контроля обмена данными

Контрмеры:

повышение ответственности пользователей, использование настроек ОС (отключение служб, настройка сетевых фильтров и т.п.)

ГРИНАТОМ

Типичные причины нарушений пользователей

- Личная (непроизводственная) переписка по электронной почте

Действие:

злоупотребления при осуществлении личной переписки по электронной почте, претензии сотрудников на тайну личной переписки

Последствия:

непроизводительная трата ресурсов и рабочего времени (снижение продуктивности работы сотрудников), создание помех технологическим процессам, внутренние конфликты, подрыв репутации ГК «Росатом»

Контрмеры:

повышение ответственности сотрудников, подписание соглашений о контроле за перепиской

Типичные причины нарушений пользователей

- Пересылка конфиденциальных сведений ГК «Росатом» в открытом виде

Действие:

пересылка конфиденциальной корпоративной информации в открытом виде, отправка писем посторонним лицам по ошибочным адресам, использование дополнительных личных почтовых ящиков на внешних (сторонних) почтовых серверах и т.п.

Последствия:

утечка конфиденциальной информации (в том числе коммерческих секретов)

Контрмеры:

повышение ответственности, применение Защищенной корпоративной почтовой системы

Пересылка конфиденциальных сведений ГК «Росатом» осуществляется установленным порядком с помощью защищенных с использованием шифровальных (криптографических) средств систем

Типичные причины нарушений пользователей

- Использование доступа в Интернет в непроизводственных целях
- Посещение хакерских или взломанных хакерами сайтов

Действие:

посещение сторонних сайтов (информационных, развлекательных, электронных магазинов или каталогов и т.п.), загрузка различных файлов, посещение хакерских или взломанных хакерами (зараженных) и других подозрительных сайтов (содержащих повушки и вредоносные коды)

Последствия:

непроизводительные затраты ресурсов, создание помех основным технологическим процессам, вирусное заражение, загрузка троянских и других вредоносных программ, возможность обвинения во взломе данных сайтов, непреднамеренная пересылка конфиденциальной информации («фишинг»)

Контрмеры:

повышение ответственности пользователей, установка средств фильтрации трафика по адресам сайтов, безопасная настройка Web-клиентов

Приказ от 30.12.2019 №1/1517-П

РОСАТОМ

4. Права и обязанности пользователя

п. 4.1. Пользователь имеет право заявлять потребность на подключение к ИТ-ресурсу, необходимому ему для исполнения своих обязанностей.

п.4.3.2 Использовать средства вычислительной техники автоматизированной системы организации, предоставляемые ИТ-ресурсы только в целях исполнения своих обязанностей.

4.3.3 Принимать меры по предотвращению использования ИТ-ресурсов другими лицами от его имени, обеспечивать сохранность и конфиденциальность паролей, кодов доступа и иной ключевой информации, используемой для авторизованного доступа к ИТ-ресурсам.

ГРИНАТОМ

Типичные причины нарушений пользователей

- Нарушение правил использования средств криптографической защиты информации

Действие:

нарушение правил применения средств криптографической защиты информации

Последствия:

утрата криптографических ключей, требующая их замены в системе (выход из строя ключевого носителя). Компрометация секретных ключей, используемых для шифрования и ЭП файлов и защиты удаленного взаимодействия. Злоумышленник может получить доступ к зашифрованной конфиденциальной информации, доступ в корпоративную сеть с правами пользователя скомпрометированного ключа, а также в случае компрометации секретного ключа ЭП может подделывать подписи его владельца

Контрмеры:

обучение пользователей правилам работы со средствами криптографической защиты информации (СКЗИ), сдача зачетов по программе обучения

К самостоятельной работе к СКЗИ допускаются пользователи сдавшие зачеты по программе обучения правилам работы с СКЗИ. Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты (ОКЗ). Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего ОКЗ на основании принятых от этих лиц зачетов по программе обучения.

ГРИНАТОМ

Требования к эксплуатации СКЗИ

- Средствами СКЗИ НЕ ДОПУСКАЕТСЯ обрабатывать информацию, содержащую сведения, составляющие государственную тайну;
- Ключевая информация является конфиденциальной;
- Срок действия ключа проверки ЭП – не более 15 лет после окончания срока действия соответствующего ключа ЭП (определяется при сертификации СКЗИ);
- СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах;
- Инсталляция СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

Требование к размещению технических средств с установленными СКЗИ

- Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленными СКЗИ, 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 СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию
- Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, применяющего СКЗИ, с документацией на СКЗИ, а также с другими нормативными документами, созданными на её основе

ГРИНАТОМ

Требования к программному и аппаратному обеспечению

- На технических средствах, оснащенных СКЗИ должно использоваться только лицензионное программное обеспечение фирм-производителей, либо ПО, сертифицированное ФСБ. Указанное ПО не должно содержать средств разработки или отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование СКЗИ;
- На ПЭВМ одновременно может быть установлена только одна разрешенная ОС;
- В BIOC ПЭВМ должны быть определены установки, исключающие возможность загрузки ОС, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС;
- Средствами BIOS должна быть отключена возможность отключения пользователями PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в PCI разъем;
- Вход в BIOS должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС;
- Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты;
- Программные модули СКЗИ (прикладного ПО со встроенным СКЗИ) должны быть доступны только по чтению/запуску (в атрибутах файлов запрещена запись и модификация);
- Запрещается подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

ГРИНАТОМ

Правила использования и хранения ключевых носителей

ЗАПРЕЩАЕТСЯ:

- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации; при уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки;
- вносить какие-либо изменения в программное обеспечение СКЗИ; в случае исчезновения на компьютере системы использующей средства криптографической защиты – сообщить в службу информационной безопасности и прекратить работу с любой доступной на компьютере системой до выявления причины;
- 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;
- разглашать пароль другим лицам;
- записывать на ключевые носители постороннюю информацию;

Федеральный закон от 06.04.2011 №63 ФЗ «Об электронной подписи»

ст.10 п.1 При использовании усиленных электронных подписей участники электронного взаимодействия обязаны: обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия

При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Ключевые носители должны храниться в опечатываемых пеналах, которые в свою очередь необходимо помещать в опечатываемые сейфы. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

ГРИНАТОМ

Приказ от 09 февраля 2005 г. № 66

пп. 46 СКЗИ эксплуатируются в соответствии с правилами пользования ими...

пп. 51 Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

- обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;
- собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;
- ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

ГРИНАТОМ

Компрометация – это любая возможность (или совершившийся факт) попадания ключей посторонним (не допущенным) лицам. В случае утери действующего ключевого носителя с ЭП, а также обнаружения после потери – немедленно направить администратору безопасности сообщение о компрометации ключей ЭП

ГРИНАТОМ

Типичные причины нарушений пользователей

- Нарушение правил использования средств защиты от несанкционированного доступа

Действие:
использование простых для подбора паролей,
работа под чужими именами (с чужими паролями),
передача или утрата атрибутов разграничения доступа к ресурсам системы (паролей, идентификационных устройств, пропусков и т.п.)

Последствия:
любой возможный ущерб от несанкционированного доступа к ресурсам системы постороннего лица с правами владельца утраченных реквизитов разграничения доступа

Контрмеры:
повышение ответственности и контроля, внедрение многофакторной аутентификации

Ошибки при использовании паролей

- Пользователи очень любят записывать пароли
- Пользователи придумывают пароли которые легко угадать
- Пользователи обсуждают свои пароли вслух при посторонних

Пользователи часто оставляют компьютер включенным без присмотра

Приказ от 30.12.2019 №1/1517-П
Пользователю запрещается:
п. 4.4.4 Оставлять без присмотра во включенном состоянии АРМ, на котором пользователем производится обработка информации, не активизировав средства защиты информации от несанкционированного доступа

Заблокировать компьютер:

или
Ctrl–Alt–Del + Enter

ГРИНАТОМ

Меры предосторожности при работе с паролями

- Позаботьтесь, чтобы при вводе пароля за Вами не подглядывали (в том числе и с помощью камер видеонаблюдения);
- Когда вам оказывают техническую поддержку, всегда вводите свой пароль сами и никогда не выдавайте его;
- Не вводите свой пароль на чужих компьютерах;
- Не используйте один и тот же пароль для доступа к внутренним ресурсам ГК «Росатом» и для доступа к службам в сети Интернет;
- Периодически меняйте свой пароль. Следуйте правилам придумывания стойких и запоминающихся паролей;
- Если необходимо записать пароль, храните его в физически наиболее безопасном месте (в личном сейфе), либо используйте утвержденные ИБ программно-аппаратные средства;
- Если Вас кто-либо под каким-либо предлогом попросит сообщить Ваш пароль (социальный инжиниринг, «фишинг»), не поддавайтесь на уловку и незамедлительно доложите об этом Администратору безопасности.

Правила придумывания стойких и запоминающихся паролей

- Использование парольных фраз вместо отдельных слов: True_rule1
- Выборочная замена букв в осмысленном слове спецсимволами p@ssW0rd Pa$$w0rd p@$$w0rD
- Добавление символов в начале (в середине, в конце) парольной фразы -----True___rule2-----
- Использование ассоциаций (букв из ключевых фраз)

Приказ от 30.12.2019 №1/1517-П

3.1.4 Доступ пользователя к ИТ-ресурсам осуществляется на основании присвоенного ему индивидуального уникального идентификатора (учетная запись) и пароля, а в отдельных случаях - с применением СКЗИ. Учетная запись формируется автоматически и не может быть изменена по требованию пользователя.

4.4. При использовании ИТ-ресурса пользователю запрещается:

4.4.2. Передавать другим лицам свои или использовать чужие учетные данные.

РОСАТОМ

ГРИНАТОМ

Ответственность пользователя СКЗИ за разглашение конфиденциальной информации


Ответственность организации
Кодекс РФ об административных правонарушениях
Уголовный кодекс РФ
ст.13.11-13.14 КОАП РФ
Штраф до 25 000 руб. с конфискацией, приостановление деятельности организации на срок до 90 суток
ст.137, 138, 171, 183, 272, 273, 274, 293 УК РФ
Наказание до 7 лет лишения свободы
штраф до 1 млн. руб.

Самая большая ошибка - игнорирование установленных ограничений и правил политики безопасности при работе системы

Будьте внимательны и осторожны!

Помните об угрозах ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ!

ГРИНАТОМ

Приложение №19. Анкета для опроса пользователей

Анкета для опроса пользователей СКЗИ

Заполняется персонально пользователем СКЗИ
(для корректного заполнения просьба отметить один или несколько вариантов ответа)

1. Сколько процентов из общего объема нарушений и преступлений составляют ошибки персонала?
    a) 4%;
    b) 19%;
    c) 20%;
    d) >50%.

2. Кто входит в состав системы обеспечения информационной безопасности?
    a) сотрудники подразделения информационной безопасности;
    b) сотрудники Казначейства;
    c) все сотрудники ГК Росатом, имеющие прямое или косвенное отношение к системе.

3. Имеет ли право пользователь использовать предоставленные ему ресурсы ГК Росатом в личных целях?
    a) да;
    b) нет;
    c) иногда.

4. Что должен сделать пользователь, если он оказался свидетелем порчи имущества ГК Росатом?
    a) попытаться исправить испорченное имущество;
    b) попытаться предотвратить порчу имущества;
    c) незамедлительно сообщить непосредственному руководителю о произошедшем;
    d) не придавать этому значения.

5. Какие операции не имеет право производить пользователь с аппаратно-программными средствами, выданными ему ГК Росатом для исполнения своих служебных обязанностей?
    a) вскрытие системного блока ЭВМ (для протирания пыли), мыши, клавиатуры;
    b) добавление в аппаратную часть ЭВМ дополнительных плат для увеличения производительности ЭВМ;
    c) исполнение своих служебных обязанностей;

d) инсталляция сторонних программ на ЭВМ;
e) внесение изменений в настройки аппаратной части ЭВМ, программных продуктов, установленных на ЭВМ.

6. Что должен сделать пользователь при обнаружении вирусного заражения ЭВМ?
   a) обновить базы антивируса, произвести проверку компьютера и удалить вирус;
   b) прекратить обработку информации на компьютере;
   c) сообщить в подразделение информационной безопасности, эксплуатирующей систему;
   d) перезагрузить компьютер;
   e) выключить компьютер и отсоединить от сети.

7. Что должен сделать пользователь при временном уходе с рабочего места?
   a) убрать в недоступное место записанные на бумаге пароли;
   b) завершить работу всех открытых приложений;
   c) заблокировать экран нажатием клавиш Ctrl-Alt-Del + Enter;
   d) выключить компьютер;
   e) ключевой носитель убрать в запираемое и опечатываемое хранилище.

8. Какие пользователи допускаются к самостоятельной работе с СКЗИ?
   a) все пользователи ГК Росатом;
   b) нуждающиеся в СКЗИ для исполнения своих служебных обязанностей;
   c) прошедшие обучение правилам работы с СКЗИ;
   d) сдавшие зачеты по программе обучения правилам работы с СКЗИ.

9. Какие обстоятельства относятся к компрометации ключей?
   a) утеря ключевого носителя с последующим обнаружением;
   b) утеря ключевого носителя;
   c) временное оставление ключевого носителя без присмотра;
   d) нарушение печатей на сейфе с ключевыми носителями;
   e) утеря ключей от сейфа, в котором хранятся ключевые носители.

10. Как должен действовать пользователь СКЗИ при утере ключевого носителя с последующим обнаружением, в случае когда нельзя достоверно установить, что произошло с ключевым носителем?
    a) незамедлительно поставить в известность о факте компрометации ключей администратора безопасности;
    b) самостоятельно произвести генерацию новых ключей ЭП, поставив в известность банк о факте компрометации;
    c) продолжить работу с найденными ключами.

11. Как обеспечить стойкий и легко запоминающийся пароль?

a) использовать парольные фразы;
b) придумать длинный пароль, но не менее 8-и символов;
c) выборочно заменить буквы спецсимволами;
d) добавить спецсимволы в начале (в середине, в конце);
e) использовать ассоциации;
f) использовать личные данные (ФИО, кличка собаки, марку машины, название улицы и пр.).

12. Какая ответственность предусмотрена законодательством РФ за нарушения правил работы с конфиденциальной информацией?
a) уголовная;
b) административная;
c) ответственность не предусмотрена.

13. Какая ответственность предусмотрена Уголовным кодексом РФ пользователю за разглашение коммерческой тайны?
a) штраф в размере до 1 млн. руб;
b) штраф в размере до 80 000 руб;
c) лишение свободы до двух лет;
d) лишение свободы до трех лет.

14. Ключевые носители ("флешки", "таблетки" и т.п.), содержащие действующие ключи ЭП, используемые для подписания платежных документов разрешается:
a) передавать работникам других департаментов;
b) передавать сотрудникам службы технической поддержки;
c) временно (в процессе генерации новых ключей ЭП) передавать сотрудникам службы технической поддержки;
d) временно (в процессе генерации новых ключей ЭП) передавать сотрудникам службы информационной безопасности;
e) Ничего из вышеперечисленного. Ключевые носители, содержащие действующие ключи ЭП, запрещается передавать другим лицам.

15. Допускается сообщать пароль для доступа к ключевым носителям, содержащим действующие ключи ЭП, и используемым для подписания документов:
a) работникам других департаментов;
b) сотрудникам службы технической поддержки;
c) временно (в процессе генерации новых ключей ЭП) сотрудникам службы технической поддержки;
d) временно (в процессе генерации новых ключей ЭП) сотрудникам службы информационной безопасности;
e) Ничего из вышеперечисленного. Пароль запрещается разглашать другим лицам.

16. В случае потери ключевого носителя, содержащего действующие ключи ЭП:

a) сообщить сотрудникам Госкорпорации для генерации новых ключей ЭП;
b) сообщить сотрудникам службы технической поддержки для генерации новых ключей ЭП;
c) направить администратору безопасности сообщение о компрометации ключей ЭП.

17. В случае обнаружения после потери своего ключевого носителя, содержащего действующие ключи ЭП:
    a) сообщить сотрудникам Госкорпорации для генерации новых ключей ЭП;
    b) сообщить сотрудникам службы технической поддержки для генерации новых ключей ЭП;
    c) продолжить использование данного ключевого носителя без генерации новых ключей ЭП;
    d) направить администратору безопасности сообщение о компрометации ключей ЭП.

18. Свой ключевой носитель, содержащий действующие ключи ЭП, и используемый для подписания документов разрешается временно передавать для работы:
    a) сотрудникам Госкорпорации;
    b) сотрудникам службы технической поддержки;
    c) администратору безопасности;
    d) только своему коллеге по подразделению;
    e) ничего из вышеперечисленного. Ключевой носитель, содержащий действующие ключи ЭП, нельзя передавать другим лицам к ним не допущенным.

19. На ключевой носитель, содержащий действующие ключи ЭП, и используемый для подписания документов разрешается записывать файлы:
    a) если они содержат служебные документы по профилю работы;
    b) если есть свободное место на ключевом носителе и они содержат служебные документы по профилю работы;
    c) нельзя записывать, даже если они содержат служебные документы по профилю работы.

20. Каким образом осуществляется пересылка конфиденциальных сведений ГК Росатом?
    a) в открытом виде с использованием личных почтовых ящиков, зарегистрированных на внешних (сторонних) серверах;
    b) с помощью защищенных с использованием шифровальных (криптографических) средств систем;
    c) возможны оба варианта.

21. Какие требования предъявляются к хранению ключевых носителей, содержащих электронную подпись?
    a) ключевые носители хранятся в спецпомещениях, убранными в опечатанные хранилища;
    b) ключевые носители хранятся в спецпомещении, в ящике рабочего стола, закрытыми на ключ;
    c) ключевые носители хранятся в спецпомещении на рабочем столе пользователя;
    d) ключевые носители хранятся на связке обычных ключей.

22. Какие виды ответственности предусмотрены законодательством РФ для лиц, виновных в нарушении требований по защите конфиденциальной информации?
    a) ответственность не предусмотрена;
    b) дисциплинарная: расторжение трудового договора по инициативе работодателя;
    c) уголовная: 7 лет лишения свободы, штраф до 1 млн. руб;
    d) уголовная: штраф 500 000 руб;
    e) административная: штраф 30 000 руб, приостановление деятельности организации на срок до 90 суток.

Пользователь СКЗИ _____/_____
(подпись) (Ф.И.О)

«___» _____ 201__ г.

Результаты проверки

Всего ответов _____(кол-во)

Правильных ответов _____(кол-во)

Зачтено/не зачтено

Проверил

Администратор безопасности

_____/_____
(подпись) (Ф.И.О)

«___» _____ 201__ г.

Приложение №20. Заключение о сдаче зачетов

Заключение о сдаче зачетов

№ п/п	Наименование организации	ФИО обучающегося	Зачтено/не зачтено

Состав проверяющей комиссии:

<ФИО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ, ДОЛЖНОСТЬ, ОТДЕЛ, УПРАВЛЕНИЕ>

_____/_____
(подпись) (Ф.И.О)

«___» _____ 201__ г.

<ФИО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ, ДОЛЖНОСТЬ, ОТДЕЛ, УПРАВЛЕНИЕ>

_____/_____
(подпись) (Ф.И.О)

«___» _____ 201__ г.

<ФИО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ, ДОЛЖНОСТЬ, ОТДЕЛ, УПРАВЛЕНИЕ>

_____/_____
(подпись) (Ф.И.О)

«___» _____ 201__ г.

Приложение №21. Заключение о возможности эксплуатации СКЗИ

ЗАКЛЮЧЕНИЕ
о возможности эксплуатации средств криптографической защиты информации

г._____ «___» _____ 20__ г.

По результатам проверки готовности обладателя конфиденциальной информации <НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ> к самостоятельному использованию СКЗИ <НАИМЕНОВАНИЕ СКЗИ>, установлено:

1. На основании акта(ов) готовности от __.__.20__ г. №__ АРМ согласно Таблице 1 соответствуют требованиям 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, утвержденной Приказом ФАПСИ от 13.06.2001 №152 и готов(ы) к эксплуатации.

Таблица 1

№ п/п	Учетный номер АРМ	№ печати

2. Пользователи СКЗИ <НАИМЕНОВАНИЕ СКЗИ> (Таблица 2) обучены правилам работы с СКЗИ и допущены к самостоятельной работе с СКЗИ согласно Таблице №2.

Таблица 2

№ п/п	ФИО пользователя СКЗИ

Эксплуатацию СКЗИ <НАИМЕНОВАНИЕ СКЗИ> разрешаю до «___» _____ 20__ г[1]

Начальник отдела
криптографической защиты
АО «Гринатом» _____/_____
(подпись) (ФИО)

М.П.

[1] В случае сохранения доверенной среды функционирования СКЗИ, подтвержденной Актом(ами), указанными в Заключении.

Приложение №22. Журнал выполнения регламентных работ

ЖУРНАЛ
учета выполнения регламентных работ
<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

Начат: «___» _____ 20__ г.

Окончен: «___» _____ 20__ г.

Дата	Наименование работы и причина ее выполнения	Должность, фамилия и подпись		Примечание
		Выполнившего работу	Проверившего работу	

Приложение №23. Порядок проведения расследований фактов нарушения условий использования СКЗИ

ПОРЯДОК

проведения расследований фактов нарушения условий использования средств криптографической защиты информации в организациях Госкорпорации «Росатом»

Москва 2020 г.

Оглавление

1. Назначение и область применения

Настоящий Порядок проведения расследований[1] фактов нарушения условий использования средств криптографической защиты информации (далее – СКЗИ) в организациях-обладателях конфиденциальной информации (далее – ООКИ, далее – Порядок) разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты и предназначен для упорядочения и повышения эффективности деятельности при:

создании и организации работы Комиссий по расследованию фактов нарушения условий использования СКЗИ (далее – Комиссии);

проведении расследований фактов нарушения условий использования СКЗИ (далее – Расследования), выработке предупреждающих действий (профилактических мер) и принятии решений по их реализации.

Порядок является локальным нормативным документом, который регламентирует создание Комиссий, организацию их деятельности по проведению Расследований в ООКИ.

Порядок описывает подпроцесс «Расследование фактов нарушений условий использования СКЗИ» 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».

Требования настоящего Порядка обязательны для исполнения в ООКИ, заключившими с лицензиатом ФСБ России АО «Гринатом» договор на оказание услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств (далее – Договор).

Пользователями настоящего Порядка являются сотрудники органа криптографической защиты АО «Гринатом» (далее – ОКЗ) и ООКИ, участвующие в работе Комиссий.

2. Термины, определения и сокращения

В настоящем Порядке используются термины, определения и сокращения из Порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее – Порядок ОКЗ).

---

[1] Термин «Расследование» нужно понимать в значении 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 № 152 от 13.06.2001 г.

3. Порядок работ

3.1. Организация Расследования

Решение о проведении Расследования в ООКИ принимает одна из сторон по Договору.

Основаниями для создания Комиссии могут являться нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации, а также указания регулятора ФСБ России о необходимости проведения Расследования.

3.2. Порядок формирования Комиссии

Комиссия из числа сотрудников ОКЗ назначается приказом генерального директора АО «Гринатом» о проведении Расследования (далее – Приказ, форма приведена в Приложении №1 к Порядку) в течение десяти рабочих дней после принятия решения одной из сторон по Договору или после поступления указания регулятора ФСБ России о необходимости проведения Расследования.

В Приказе указывается:

ООКИ и причины проведения Расследования;

председатель Комиссии – руководитель ОКЗ;

члены Комиссии - квалифицированные специалисты ОКЗ;

сроки начала и окончания работы Комиссии.

Продолжительность проведения Расследования и состав Комиссии устанавливаются в Приказе, исходя из объёма предстоящих действий по Расследованию, характера и особенностей нарушения, его масштаба и последствий, а также других обстоятельств и не может превышать 30 рабочих дней с момента начала Расследования.

В случае необходимости дополнительной проверки обстоятельств нарушения условий использования СКЗИ, в том числе связанной с проведением технических и иных экспертиз, решение о продлении срока Расследования принимается генеральным директором АО «Гринатом» по представлению председателя Комиссии.

3.3. Порядок работы Комиссии

3.3.1. В течение трех дней после подписания Приказа ОКЗ письмом уведомляет руководителя ООКИ, в которой произошло нарушение условий использования СКЗИ, о предстоящем расследовании. Для проведения Расследования члены Комиссии в течение девяти дней после подписания Приказа командируются в ООКИ, в которой произошло подлежащее Расследованиюнарушение условий использования СКЗИ.

Расследование начинается с ознакомления руководителя ООКИ с основаниями, целями, порядком, сроками и условиями проведения Расследования.

Под руководством председателя Комиссии перед началом основных мероприятий по Расследованию проводится совместное совещание членов Комиссии и должностных лиц ООКИ.

На совещании руководитель ООКИ представляет следующие материалы:

акты предыдущих (за последние три года) проверок ФСБ России и/или ОКЗ условий использования СКЗИ в ООКИ;

планы реализации рекомендаций по результатам проверок ФСБ России и/или ОКЗ.

На совещании проводится заслушивание должностных лиц ООКИ, ответственных за организацию 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, а также руководителей подразделений ООКИ, в которых произошли нарушения условий использования СКЗИ и/или имеются последствия нарушений. Обсуждается план работы Комиссии (форма плана работы Комиссии приведена в Приложении №3 к настоящему Порядку).

3.3.2. Расследование фактов нарушения условий использования СКЗИ проводится в соответствии с планом работы Комиссии, который оформляется в первый день работы Комиссии. План работы Комиссии согласовывается с руководителем ООКИ и утверждается председателем Комиссии.

В плане работы Комиссии указываются:

наименование подразделений и СКЗИ, подлежащих проверке и (или) обследованию;

направления расследования и конкретные вопросы, ответы на которые необходимо получить в ходе расследования;

фамилия, имя, отчество члена Комиссии, уполномоченного на проведение расследования конкретного вопроса, сроки его проведения;

даты начала и окончания проведения расследования;

перечень документов, представляемых ООКИ в ходе расследования;

перечень отчётных документов и/или материалов, содержащих результаты расследования.

3.3.3. Руководитель ООКИ должен обеспечить:

представление документов по вопросам Расследования,

подготовку протоколов опросов очевидцев нарушения условий использования СКЗИ и должностных лиц ООКИ,

в установленном порядке доступ лиц, осуществляющих Расследование, к проверяемым СКЗИ и к сведениям, составляющим конфиденциальную информацию, в случае необходимости.

3.3.4. Комиссией принимаются к рассмотрению только официально зарегистрированные документы, после чего с них снимаются заверенные копии, делаются выписки.

Количество и состав документов и материалов, представляемых ООКИ, определяется и уточняется председателем Комиссии в ходе работы Комиссии.

Все работники ООКИ обязаны оказывать содействие работе Комиссии. Лица, препятствующие расследованию, отстраняются от взаимодействия с Комиссией руководителем ООКИ по ходатайству председателя Комиссии.

Изъятие документации во время проведения расследования оформляется описью (форма Описи документов приведена в Приложении №4 к настоящему Порядку), подписанной председателем и членами Комиссии, а также должностными лицами ООКИ, ответственными за хранение изымаемой документации.

3.3.5. В ходе расследования членами Комиссии выполняются мероприятия, определенные планом работы Комиссии, в том числе:

осмотр и фотографирование, а в необходимых случаях – видеосъемка, оформление протоколов осмотра места нарушения условий использования СКЗИ;

опрос очевидцев, должностных лиц и получение от них письменных объяснений;

выяснение обстоятельств, предшествовавших нарушению условий использования СКЗИ, установление причин их возникновения;

оценка достаточности соблюдения установленных требований по использованию СКЗИ для предупреждения нарушения условий использования СКЗИ;

проверка квалификации администраторов безопасности, обслуживающих СКЗИ, условия использования которых были нарушены.

На основе всей совокупности полученных данных членами Комиссии:

устанавливаются причины нарушения условий использования СКЗИ и сценарий их развития,

определяются лица, ответственные за допущенные нарушения условий использования СКЗИ,

предлагаются корректирующие меры по устранению причин нарушения условий использования СКЗИ, предупреждению повторения нарушений.

3.3.6. При наличии подозрений на причинение вреда от нарушения условий использования СКЗИ ООКИ может осуществить расчет причиненного вреда (экономического ущерба), расчет подписывается руководителем и главным бухгалтером ООКИ.

Расчет вреда (экономического ущерба), если он произведен, прилагается к Заключению по результатам расследования фактов нарушения условий использования СКЗИ (далее – Заключение, форма Заключения приведена в Приложении №2 к настоящему Порядку).

3.3.7. Действия членов Комиссии при Расследовании не должны нарушать деятельность и обеспечение информационной безопасности в ООКИ.

3.3.8. Если в использовании СКЗИ выявлены серьезные нарушения, из-за чего становится реальной утечка конфиденциальной информации, безопасность которой обеспечивается с использованием СКЗИ, то председатель Комиссии вправе дать указание о немедленном прекращении использования СКЗИ до устранения причин выявленных нарушений.

3.4. Оформление и учет материалов расследования, организация устранения причин нарушения условий использования СКЗИ

3.4.1. Результаты работы Комиссии оформляются Заключением.

Заключение состоит из вводной, описательной, заключительной частей и приложений.

Вводная часть Заключения содержит следующую информацию:

основание для Расследования;

полное наименование ООКИ и СКЗИ, правила использования которого были нарушены,

должности, фамилии, имена, отчества должностных лиц (председателя, заместителя председателя и членов Комиссии), проводивших расследование,

даты начала и окончания расследования,

перечень подразделений и должностных лиц ООКИ, участвовавших в мероприятиях по расследованию.

Описательная часть Заключения содержит сведения об СКЗИ, о проведенных мероприятиях по расследованию и их результатах, в том числе о выявленных нарушениях условий использования СКЗИ и, при необходимости, иные дополнительные сведения, подтверждающие результаты расследования и выводы Комиссии.

Заключительная часть Заключения содержит выводы по установлению обстоятельств и причин нарушения условий использования СКЗИ с указанием:

перечня должностных лиц, допустивших нарушения,

принятых мер по ликвидации последствий нарушения,

продолжительности простоя и материальном (экономическом) ущербе (если расчет производился). Здесь же формулируются предложения по устранению причин и последствий нарушения, а также по организационным мероприятиям для предупреждения и профилактики аналогичных нарушений в работе данного и других СКЗИ.

3.4.2. К Заключению оформляются следующие приложения:

копия Приказа,

протокол осмотра места нарушения условий использования СКЗИ с необходимыми фото- и видеоматериалами,

протоколы опроса очевидцев и объяснения лиц, причастных к нарушению условий использования СКЗИ, а также должностных лиц, ответственных за соблюдение условий использования СКЗИ,

копии протоколов и удостоверений об обучении и аттестации администраторов безопасности и пользователей СКЗИ, обслуживающих и работающих с СКЗИ,

справки о размере причиненного вреда и оценке экономического ущерба от нарушения условий использования СКЗИ (если расчет производился),

сведения о нарушениях требований законодательных и нормативных технических документов (перечень нарушений требований информационной безопасности, выявленных в ходе расследования),

предложения Комиссии по проведению соответствующих компенсирующих мероприятий,

другие материалы, характеризующие нарушение условий использования СКЗИ, обстоятельства и причины возникновения нарушения, его развитие, последствия.

Перечень материалов, прилагаемых к Заключению может изменяться и дополняться по письменному решению председателя Комиссии в зависимости от характера и обстоятельств нарушения. Таким решением может быть запрос к руководителю ООКИ о предоставлении Комиссии дополнительных материалов. Указанное решение также оформляется в виде приложения к Заключению.

3.4.3. Результаты расследования, содержащие сведения, составляющие конфиденциальную информацию, оформляются с соблюдением требований, предусмотренных законодательством Российской Федерации о защите конфиденциальной информации.

3.4.4. Заключение после завершения работы Комиссии составляется в двух экземплярах, подписывается всеми членами Комиссии и председателем Комиссии, представляется для ознакомления руководителю управления информационной безопасности АО «Гринатом» и после подписания им два экземпляра направляются руководителю ООКИ для ознакомления и подписания. Один экземпляр Заключения остается в ООКИ, один возвращается в ОКЗ.

В АО «Гринатом» Заключения, а также все иные документы, возникшие в ходе расследования, помещаются в дела и хранятся согласно Инструкции по делопроизводству и сводной номенклатуре дел АО «Гринатом».

В ООКИ документы, возникшие в ходе расследования, помещаются в дела и хранятся согласно сводной номенклатуре дел ООКИ и локальному нормативному акту ООКИ, регламентирующему хранение документов.

3.4.5. Руководитель ООКИ, в которой произошло нарушение условий использования СКЗИ, в течение десяти рабочих дней с момента ознакомления с Заключением утверждает План устранения недостатков по результатам проведения расследования нарушения условий использования СКЗИ (далее – План устранения недостатков, форма Плана устранения недостатков представлена в приложении №33 к Порядку ОКЗ).

3.4.6. Копия плана устранения недостатков в течение трех рабочих дней после его утверждения направляется руководителем ООКИ в ОКЗ.

3.4.7. Руководитель ООКИ в случае несогласия с фактами и выводами, изложенными в Заключении, в течение десяти рабочих дней от даты получения экземпляра Заключения вправе представить руководителю ОКЗ в письменной форме возражения в отношении Заключения в целом или в отношении отдельных положений. При этом он вправе приложить к своим возражениям документы, подтверждающие обоснованность возражений, или их заверенные копии.

3.4.8. Результаты выполнения Плана устранения недостатков ежеквартально оформляются в виде отчётов в произвольной форме, подписываются руководителем ООКИ и направляются в ОКЗ.

4. Нормативные ссылки

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».

5. Внесение изменений в Порядок

Инициатором и координатором работ по изменению Порядка является ОКЗ.

В случае если инициатором изменений выступает не ОКЗ, то инициатор внесения изменений должен представить ОКЗ обоснование практической целесообразности таких изменений.

Изменения Порядка после оценки их целесообразности проходят процедуру согласования в установленном порядке. При внесении изменений утверждается новая редакция Порядка.

6. Контроль и ответственность

Ответственность за выполнение требований Порядка возлагается на сотрудников ОКЗ и ООКИ, участвующих в работе Комиссий.

Контроль выполнения требований Порядка возлагается на ОКЗ.

За бездействие (халатность) при проведении Расследования, а также за недостоверность и несвоевременность передаваемой в ходе Расследования информации члены Комиссии, экспертные специалисты, привлекаемые к работе Комиссии, работники организаций, привлекаемые к Расследованию, несут ответственность в соответствии с действующим законодательством, нормативными правовыми актами Российской Федерации и локальными нормативными актами Государственной корпорации по атомной энергии «Росатом» и ООКИ.

Приложение №1 к Порядку. Форма Приказа о проведении Расследования

Акционерное общество «Гринатом»

« » 20 г. Москва № _____

(дата)

О проведении расследования обстоятельств и причин нарушения условий использования средств криптографической защиты информации в

_____

(наименование организации)

В соответствии с Порядком проведения расследований фактов нарушения условий использования средств криптографической защиты информации Госкорпорации «Росатом» и ее организациях, утв. в рамках договора присоединения от 06 июля 2012 г. на оказание услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств:

1. Назначить комиссию по проведению расследования обстоятельств и причин нарушения условий использования СКЗИ в (на):

_____

(наименование объекта)

в составе:

Фамилия И.О._____, председатель комиссии

(должность)

(руководитель ОКЗ),

Фамилия И.О._____,

(должность)

Фамилия И.О._____.

(должность)

2. Комиссии в период с «___»_____ 20___ г. по «___»_____ 20___ г. провести расследование обстоятельств и причин нарушения условий использования СКЗИ в _____

(наименование организации)

в установленном порядке.

3. Контроль за исполнением настоящего Приказа возложить на руководителя Органа криптографической защиты АО «Гринатом»

_____ .

(Фамилия И.О.)

Генеральный директор _____/_____

(подпись) (И.О. Фамилия)

Приложение №2 к Порядку. Форма заключения по результатам Расследования

УТВЕРЖДАЮ	**ОЗНАКОМЛЕН**
<ДОЛЖНОСТЬ ПРЕДСЕДАТЕЛЯ КОМИССИИ (РУКОВОДИТЕЛЯ ОКЗ), НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>	<ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАНСОСТИ АО «ГРИНАТОМ»>
_____/_____	_____/_____
(подпись) (Ф.И.О)	(подпись) (Ф.И.О)
«___»_____ 20__ г.	«___»_____ 20__ г.

ЗАКЛЮЧЕНИЕ
комиссии Органа криптографической защиты АО «Гринатом»
по результатам расследования фактов
нарушения условий использования СКЗИ в
<ПОЛНОЕ НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

СОГЛАСОВАНО	СОГЛАСОВАНО	ОЗНАКОМЛЕН
<ДОЛЖНОСТЬ ЧЛЕНА КОМИССИИ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>	<ДОЛЖНОСТЬ ЧЛЕНА КОМИССИИ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>	<ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ ООКИ>
_____/_____	_____/_____	_____/_____
(подпись) (Ф.И.О)	(подпись) (Ф.И.О)	(подпись) (Ф.И.О)

«___»_____ 20__ г. «___»_____ 20__ г. «___»_____ 20__ г.

Во исполнение Приказа АО «Гринатом» от «___» _____ 20___ г. о проведении расследования фактов нарушения условий использования СКЗИ и в соответствии с Договором Присоединения от 06 июля 2012 г. №22/2143-Д на оказание услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств (заявление о присоединении от «___» _____ 201__ г. №_____) в период с «___» по «___» _____ 201__ г. комиссией в составе:

1. Председатель комиссии: <ДОЛЖНОСТЬ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ, ФИО ПРЕДСЕДАТЕЛЯ КОМИССИИ>,
2. <ДОЛЖНОСТЬ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ, ФИО ЧЛЕНА КОМИССИИ>
3. <ДОЛЖНОСТЬ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ, ФИО ЧЛЕНА КОМИССИИ>

проведено расследование фактов нарушения условий использования СКЗИ <НАИМЕНОВАНИЕ СКЗИ> в <ПОЛНОЕ НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>.

ПРОВЕРКЕ ПОДВЕРГАЛИСЬ

Сотрудники ОКЗ/администраторы безопасности

1. Приказ о назначении администраторов безопасности и лиц, их замещающих (далее – Приказ):

наличие Приказа,

включение в Приказ всех сотрудников, выполняющих обязанности администратора безопасности,

включение администраторов безопасности в состав комиссии по составлению заключений на основании принятых от пользователей средств криптографической защиты информации (далее - СКЗИ) зачетов по программе обучения правилам работы с СКЗИ, а также по уничтожению СКЗИ и ключевых документов.

2. Уровень квалификации администратора безопасности для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ:

наличие у администратора безопасности подтверждения об обучении и/или повышении квалификации в организации, имеющей лицензию на ведение образовательной деятельности по соответствующим программам.

3. Наличие обязанностей администратора безопасности в должностных инструкциях сотрудников, выполняющих эти обязанности.

4. Ознакомление под расписку с Инструкцией 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, утвержденной Приказом ФАПСИ от 13 июня 2001г. №152 (далее – Инструкция №152).

5. Наличие у администраторов безопасности личных металлических печатей.

Помещение ОКЗ/помещение администраторов безопасности

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения, где хранятся СКЗИ, эксплуатационная и техническая документация к ним (далее – спецпомещения ОКЗ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения ОКЗ,

наличие опечатывающих устройств на дверях спецпомещений ОКЗ,

наличие замков на дверях спецпомещений ОКЗ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений ОКЗ,

учет ключей и их дубликатов от дверей спецпомещений ОКЗ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений ОКЗ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений ОКЗ ответственным должностным лицам.

2. Металлические хранилища для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей:

наличие металлических хранилищ,

наличие внутренних замков и кодовых замков или приспособлений для опечатывания замочных скважин металлических хранилищ,

наличие ключей и дубликатов ключей (как минимум двух экземпляров) от металлических хранилищ,

учет металлических хранилищ в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от металлических хранилищ в журнале учета хранилищ и ключей,

порядок сдачи ключей от металлических хранилищ ответственному должностному лицу по окончании рабочего дня,

порядок сдачи ключей от металлического хранилища ответственного должностного лица, где хранятся ключи от всех остальных хранилищ, в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от металлических хранилищ ответственным должностным лицам.

3. Окна спецпомещений ОКЗ:

наличие металлических решеток или ставней на окнах спецпомещений ОКЗ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения ОКЗ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения ОКЗ посторонних лиц,

наличие на окнах спецпомещений ОКЗ приспособлений для предотвращения просмотра извне спецпомещений ОКЗ.

Документация ОКЗ

1. Наличие утвержденного перечня лиц, допускаемых к самостоятельной работе с СКЗИ и его актуальность;
2. Наличие утвержденного Приказа о предоставлении прав подписей в системах (для банковских платежных систем) и его актуальность;
3. Выписка из номенклатуры дел.
4. Журнал учета хранилищ и ключей.
5. Журнал учета приема (сдачи) под охрану специальных помещений и ключей от них,
6. Журнал учета печатей и штампов.
7. Журнал учета электронных носителей информации, содержащих конфиденциальную информацию.
8. Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – журналы поэкземплярного учета):

наличие журналов поэкземплярного учета,

учет журналов поэкземплярного учета в номенклатуре дел,

правильность ведения журналов поэкземплярного учета (прошит/не прошит, наличие нумерации, правильность заполнения граф и пр.),

актуальность информации в журналах поэкземплярного учета.

9. Акты готовности СКЗИ к эксплуатации (далее – Акты):

наличие Актов,

правильность составления Актов,

актуальность информации в Актах.

10. Заключения о сдаче зачетов, составленные на основании принятых от пользователей СКЗИ зачетов по программе обучения:

наличие заключений о сдаче зачетов,

правильность составления заключений,

актуальность информации в заключениях о сдаче зачетов.

11. Наличие Заключений о возможности эксплуатации СКЗИ и их актуальность.

12. Заключения ПДТК на объекты информатизации, где установлены СКЗИ, но не обрабатывается конфиденциальная информация.

13. Аттестаты соответствия ФСТЭК на объекты информатизации с установленными СКЗИ.

Помещения с установленными СКЗИ

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения с установленными СКЗИ (далее – спецпомещения пользователей СКЗИ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения пользователей СКЗИ,

наличие опечатывающих устройств на дверях спецпомещений пользователей СКЗИ,

наличие замков на дверях спецпомещений пользователей СКЗИ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ,

учет ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений пользователей СКЗИ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений пользователей СКЗИ ответственным должностным лицам.

2. Шкафы (ящики, хранилища) индивидуального пользования:

наличие надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования,

наличие приспособлений для опечатывания замочных скважин на шкафах (ящиках, хранилищах) индивидуального пользования,

учет шкафов (ящиков, хранилищ) в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от шкафов (ящиков, хранилищ) в журнале учета хранилищ,

отметки о выдаче ключей и дубликатов ключей от шкафов (ящиков, хранилищ) ответственным должностным лицам.

3. Окна спецпомещений пользователей СКЗИ:

наличие металлических решеток или ставней на окнах спецпомещений пользователей СКЗИ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения пользователей СКЗИ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения пользователей СКЗИ посторонних лиц,,

наличие на окнах спецпомещений пользователей СКЗИ приспособлений для предотвращения просмотра извне спецпомещений пользователей СКЗИ.

Пользователи СКЗИ

1. Наличие у пользователей СКЗИ ключевых документов.
2. Наличие печатей у пользователей СКЗИ для опечатывания шкафов (ящиков, хранилищ).
3. Знания пользователями требований при работе с СКЗИ.
4. Выполнение пользователями требований при работе с СКЗИ.

АРМ пользователей СКЗИ

1. Наличие и соответствие учетных (серийных) номеров АРМ пользователей СКЗИ с номерами, указанными в ЖПУ и Актах.
2. Наличие и соответствие номеров средств контроля за вскрытием АРМ (печатей, пломб) с установленными СКЗИ с номерами, указанными в Актах.
3. Наличие СКЗИ на АРМ пользователей,
4. Актуальность сертификатов соответствия ФСБ на СКЗИ, установленные на АРМ пользователей СКЗИ.
5. Наличие на АРМ с СКЗИ сертифицированных антивирусных средств.
6. Наличие на АРМ с СКЗИ сертифицированных средств защиты информации от несанкционированного доступа (далее – СЗИ от НСД).
7. Права пользователей СКЗИ на АРМ с СКЗИ (на учетные записи, на антивирусы, на СЗИ от НСД), права на удаленное администрирование и модификацию ОС и ее настроек на АРМ с СКЗИ.
8. Максимальные сроки действия паролей к учетным записям на АРМ с СКЗИ, параметры автоматической блокировки учетных записей.

Сотрудники ООКИ:

1. <ДОЛЖНОСТЬ, НАИМЕНОВАНИЕ ООКИ, ФИО>,
2. <ДОЛЖНОСТЬ, НАИМЕНОВАНИЕ ООКИ, ФИО>,

.

.

СКЗИ и оборудование, в составе которого оно эксплуатируется:

1. <НАИМЕНОВАНИЕ СКЗИ, МЕСТОРАСПОЛОЖЕНИЕ АРМ с СКЗИ, S/N АРМ, НАИМЕНОВАНИЕ И ВЕРСИЯ ОС И ПР.>,
2. <НАИМЕНОВАНИЕ СКЗИ, МЕСТОРАСПОЛОЖЕНИЕ АРМ с СКЗИ, S/N АРМ, НАИМЕНОВАНИЕ И ВЕРСИЯ ОС И ПР.>,
3. <НАИМЕНОВАНИЕ СКЗИ, МЕСТОРАСПОЛОЖЕНИЕ АРМ с СКЗИ, S/N АРМ, НАИМЕНОВАНИЕ И ВЕРСИЯ ОС И ПР.>,

ПРОВЕРКОЙ УСТАНОВЛЕНО

_____

_____

_____

(сведения об СКЗИ, о проведенных мероприятиях по расследованию и их результатах, в том числе о выявленных нарушениях условий использования СКЗИ и иные дополнительные сведения, подтверждающие результаты расследования и выводы Комиссии)

УКАЗАНИЯ И РЕКОМЕНДАЦИИ

.

.

ВЫВОДЫ

1. <ОБСТОЯТЕЛЬСТВА И ПРИЧИНЫ НАРУШЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СКЗИ>,
2. <ПЕРЕЧЕНЬ ДОЛЖНОСТНЫХ ЛИЦ, ДОПУСТИВШИХ НАРУШЕНИЯ>,
3. <ПРОДОЛЖИТЕЛЬНОСТЬ ПРОСТОЯ И МАТЕРИАЛЬНЫЙ (ЭКОНОМИЧЕСКИЙ) УЩЕРБ>, если такой расчет производился,
4. <ПРИНЯТЫЕ/НЕОБХОДИМЫЕ МЕРЫ ПО УСТРАНЕНИЮ НАРУШЕНИЙ/ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ НАРУШЕНИЙ>.

Приложение №3 к Порядку. Форма плана работы Комиссии

ПЛАН

работы комиссии по расследованию фактов нарушения условий использования СКЗИ в

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

№ п/п	Наименование подразделения, местонахождение АРМ с СКЗИ, должность, ФИО пользователя СКЗИ в зоне ответственности которого находятся СКЗИ, условия использования которых были нарушены	Вопросы/ направления расследования	Перечень документов представляемых ООКИ в ходе расследования	Перечень отчетных документов и/или материалов, содержащих результаты расследования	ФИО ответственного члена Комиссии, уполномоченного на проведение расследования конкретного вопроса	Срок проведения расследования конкретного вопроса	Отметка о проведении расследования (выполнено/не выполнено)

Дата начала расследования: «___» _____ 201__ г.

Дата окончания расследования: «___» _____ 201__ г.

«УПОЛНОМОЧЕННОЕ ДОЛЖНОСТНОЕ ЛИЦО ООКИ, НАИМЕНОВАНИЕ ООКИ»

_____/_____
(подпись) (Ф.И.О)

Председатель Комиссии

_____/_____
(подпись) (Ф.И.О)

Приложение №4 к Порядку. Форма описи документов

ОПИСЬ ДОКУМЕНТОВ

Настоящим удостоверяется, что _____
(Ф.И.О., должность, наименование ООКИ)
представил, а Комиссия в лице _____
(Ф.И.О., должность, наименование ООКИ)
приняла следующие документы для проведения расследования фактов нарушений условий использования СКЗИ.

№ п/п	Наименование документа	Количество листов	Дополнительные сведения
1			
2			
3			
Всего:			

Документы сдал: _____/_____
(подпись) (Ф.И.О)

Председатель Комиссии: _____/_____
(подпись) (Ф.И.О)

Члены комиссии:

_____/_____
(подпись) (Ф.И.О)

_____/_____
(подпись) (Ф.И.О)

Приложение №24. Акт уничтожения СКЗИ

АКТ
уничтожения СКЗИ
№ ____

г. _____ « ___ » _____ 20 ___ г.

Комиссия из числа сотрудников органа криптографической защиты в составе:

1. _____
(ФИО, должность)
2. _____
(ФИО, должность)
3. _____
(ФИО, должность)

назначенных приказом от _____ г. № _____ в <НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ> составила настоящий акт о том, что перечисленные в нем СКЗИ, указанные в таблице №1, уничтожены путем <СПОСОБ УНИЧТОЖЕНИЯ>.

Таблица №1

№ п/п	Наименование СКЗИ	Уч. №АРМ	Серийный номер сертификата ключа проверки электронной подписи / номер лицензии	ФИО пользователя СКЗИ

Уничтожено в количестве _____ (цифрами и прописью) наименований и экземпляров ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации.

Члены комиссии:

_____/_____
(подпись) (Ф.И.О)

_____/_____
(подпись) (Ф.И.О)

Приложение №25. Приказ о проведении проверки

АКЦИОНЕРНОЕ ОБЩЕСТВО «ГРИНАТОМ»

П Р И К А З

« » _____ 20__ г. Москва №_____

О проведении проверок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

В рамках оказания услуги CLB.18 по договору №22/2143-Д от 06.07.2012 для осуществления контроля за организацией и обеспечением безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

ПРИКАЗЫВАЮ:

1. Утвердить план-график проведения проверок на 20__ год (Приложение № 1).

2. Работникам отдела криптографической защиты <ФАМИЛИЯ И.О.> и <ФАМИЛИЯ И.О.> провести проверку организации и обеспечения безопасности хранения, обработки и передачи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, согласно плану-графику проведения проверок на 20__ год.

3. Контроль исполнения настоящего приказа возложить на «ДОЛЖНОСТЬ, ФАМИЛИЯ И.О. УПОЛНОМОЧЕННОГО ЛИЦА».

Генеральный директор <И.О. ФАМИЛИЯ>

Приложение №26. План-график проведения проверок

Приложение №1
УТВЕРЖДЕН
приказом АО «Гринатом»
от _____№_____

План-график проведения проверок на 20__ год

№ п/п	Предприятие	Адрес месторасположения	Проверяющие	Срок проведения проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну	Кол-во СКЗИ (на момент составления приказа)

Приложение №27. Информационное письмо о проведении проверки

Акционерное общество «Гринатом»
(АО «Гринатом»)

1-й Нагатинский проезд, д. 10, стр. 1,
Москва, 115230
Телефон (499) 949-49-19, факс (499) 949-44-46
E-mail: info@greenatom.ru
ОКПО 64509942, ОГРН 1097746819720
ИНН 7706729736, КПП 770601001

«ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ЛИЦА»
«НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ»

«И.О.ФАМИЛИЯ»

_____ № _____

На № _____ от _____

О проведении проверки работ по договору №22/2143-Д от 06.07.2012 г.

Уважаемый(-ая) «ИМЯ ОТЧЕСТВО»!

В рамках договора №22/2143-Д от 06.07.2012 г, заявлений на организацию 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 (услуга CLB.18) и заявлений на создание квалифицированных сертификатов ключей проверки электронной подписи (услуга CLB.11) в «НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ» выданы СКЗИ в количестве _____ед. и квалифицированные сертификаты ключей проверки электронной подписи в количестве _____ед.

Приказом от __.__.201_ г. № _____ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну возложено на специалистов лицензиата ФСБ России АО «Гринатом» и утверждён план-график проведения проверок.

Прошу согласовать время и дату проведения проверки в «НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ» и обеспечить доступ к СКЗИ.

Время	Дата	Количество СКЗИ	Количество ключей проверки ЭП	Исполнитель (должность, Ф.И.О)

С уважением,
Начальник отдела криптографической защиты И.О. Фамилия
(по дов. № _____ от _____)

Исп.тел.:

Приложение №28. Сводная таблица по объекту проверки

Сводная таблица по <НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

ПРОВЕРКЕ ПОДВЕРГАЛИСЬ	**ВЫПОЛНЕНО/ ВЫПОЛНЕНО ЧАСТИЧНО/ НЕ ВЫПОЛНЕНО, КОММЕНТАРИЙ**
Сотрудники ОКЗ/администраторы безопасности	
Приказ о назначении администраторов безопасности и лиц, их замещающих (далее – Приказ): – наличие Приказа, – включение в Приказ всех сотрудников, выполняющих обязанности администратора безопасности, – включение администраторов безопасности в состав комиссии по составлению заключений на основании принятых от пользователей средств криптографической защиты информации (далее - СКЗИ) зачетов по программе обучения правилам работы с СКЗИ, а также по уничтожению СКЗИ и ключевых документов.	
Уровень квалификации администратора безопасности для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ: – наличие у администратора безопасности подтверждения об обучении и/или повышении квалификации в организации, имеющей лицензию на ведение образовательной деятельности по соответствующим программам	

Наличие обязанностей администратора безопасности в должностных инструкциях сотрудников, выполняющих эти обязанности	
Ознакомление под расписку с Инструкцией 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, утвержденной Приказом ФАПСИ от 13 июня 2001г. №152 (далее – Инструкция №152)	
Наличие у администраторов безопасности личных металлических печатей	
Помещение ОКЗ/помещение администраторов безопасности	
Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения, где хранятся СКЗИ, эксплуатационная и техническая документация к ним (далее – спецпомещения ОКЗ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ: – наличие утвержденных перечней лиц, допускаемых в спецпомещения ОКЗ; – наличие опечатывающих устройств на дверях спецпомещений ОКЗ; – наличие замков на дверях спецпомещений ОКЗ, гарантирующих надежное закрытие в нерабочее время;	

– наличие ключей и их дубликатов от дверей спецпомещений ОКЗ; – учет ключей и их дубликатов от дверей спецпомещений ОКЗ в журнале учета хранилищ и ключей; – порядок сдачи ключей от дверей спецпомещений ОКЗ в службу охраны или дежурному по организации по окончании рабочего дня; – отметки о выдаче ключей и дубликатов ключей от спецпомещений ОКЗ ответственным должностным лицам	
– Металлические хранилища для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей: – наличие металлических хранилищ; – наличие внутренних замков и кодовых замков или приспособлений для опечатывания замочных скважин металлических хранилищ; – наличие ключей и дубликатов ключей (как минимум двух экземпляров) от металлических хранилищ; – учет металлических хранилищ в журнале учета хранилищ и ключей; – учет ключей и дубликатов ключей от металлических хранилищ в журнале учета хранилищ и ключей; – порядок сдачи ключей от металлических хранилищ	

ответственному должностному лицу по окончании рабочего дня; – порядок сдачи ключей от металлического хранилища ответственного должностного лица, где хранятся ключи от всех остальных хранилищ, в службу охраны или дежурному по организации по окончании рабочего дня; – отметки о выдаче ключей и дубликатов ключей от металлических хранилищ ответственным должностным лицам	
– Окна спецпомещений ОКЗ: – наличие металлических решеток или ставней на окнах спецпомещений ОКЗ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения ОКЗ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения ОКЗ посторонних лиц; – наличие на окнах спецпомещений ОКЗ приспособлений для предотвращения просмотра извне спецпомещений ОКЗ	
– Документация ОКЗ	
– Наличие утвержденного перечня лиц, допускаемых к самостоятельной работе с СКЗИ и его актуальность	
– Наличие утвержденного Приказа о предоставлении прав подписей в системах (для банковских	

платежных систем) и его актуальность	
– Выписка из номенклатуры дел	
– Журнал учета хранилищ и ключей	
– Журнал учета приема (сдачи) под охрану специальных помещений и ключей от них	
– Журнал учета печатей и штампов	
– Журнал учета электронных носителей информации, содержащих конфиденциальную информацию	
– Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – журналы поэкземплярного учета): – наличие журналов поэкземплярного учета; – учет журналов поэкземплярного учета в номенклатуре дел; – правильность ведения журналов поэкземплярного учета (прошит/не прошит, наличие нумерации, правильность заполнения граф и пр.); – актуальность информации в журналах поэкземплярного учета	
Акты готовности СКЗИ к эксплуатации (далее – Акты): – наличие Актов; – правильность составления Актов; – актуальность информации в Актах	
Заключения о сдаче зачетов, составленные на основании принятых от пользователей СКЗИ зачетов по программе обучения: – наличие заключений о сдаче зачетов;	

– правильность составления заключений; – актуальность информации в заключениях о сдаче зачетов	
Наличие Заключений о возможности эксплуатации СКЗИ и их актуальность	
Заключения ПДТК на объекты информатизации, где установлены СКЗИ, но не обрабатывается конфиденциальная информация	
Аттестаты соответствия ФСТЭК на объекты информатизации с установленными СКЗИ	
Помещения с установленными СКЗИ	
Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения с установленными СКЗИ (далее – спецпомещения пользователей СКЗИ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ: – наличие утвержденных перечней лиц, допускаемых в спецпомещения пользователей СКЗИ; – наличие опечатывающих устройств на дверях спецпомещений пользователей СКЗИ; – наличие замков на дверях спецпомещений пользователей СКЗИ, гарантирующих надежное закрытие в нерабочее время; – наличие ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ; – учет ключей и их дубликатов от дверей спецпомещений	

пользователей СКЗИ в журнале учета хранилищ и ключей; – порядок сдачи ключей от дверей спецпомещений пользователей СКЗИ в службу охраны или дежурному по организации по окончании рабочего дня; – отметки о выдаче ключей и дубликатов ключей от спецпомещений пользователей СКЗИ ответственным должностным лицам.	
Шкафы (ящики, хранилища) индивидуального пользования: – наличие надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования; – наличие приспособлений для опечатывания замочных скважин на шкафах (ящиках, хранилищах) индивидуального пользования; – учет шкафов (ящиков, хранилищ) в журнале учета хранилищ и ключей; – учет ключей и дубликатов ключей от шкафов (ящиков, хранилищ) в журнале учета хранилищ; – отметки о выдаче ключей и дубликатов ключей от шкафов (ящиков, хранилищ) ответственным должностным лицам	
Окна спецпомещений пользователей СКЗИ: – наличие металлических решеток или ставней на окнах спецпомещений пользователей СКЗИ, или охранной сигнализации, или других средств, препятствующих неконтролируемому	

проникновению в спецпомещения пользователей СКЗИ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения пользователей СКЗИ посторонних лиц; – наличие на окнах спецпомещений пользователей СКЗИ приспособлений для предотвращения просмотра извне спецпомещений пользователей СКЗИ	
Пользователи СКЗИ	
Наличие у пользователей СКЗИ ключевых документов	
Наличие печатей у пользователей СКЗИ для опечатывания шкафов (ящиков, хранилищ)	
Знания пользователями требований при работе с СКЗИ	
Выполнение пользователями требований при работе с СКЗИ	
АРМ пользователей СКЗИ	
Наличие и соответствие учетных (серийных) номеров АРМ пользователей СКЗИ с номерами, указанными в ЖПУ и Актах	
Наличие и соответствие номеров средств контроля за вскрытием АРМ (печатей, пломб) с установленными СКЗИ с номерами, указанными в Актах	
Наличие СКЗИ на АРМ пользователей;	
Актуальность сертификатов соответствия ФСБ на СКЗИ, установленные на АРМ пользователей СКЗИ	
Наличие на АРМ с СКЗИ сертифицированных антивирусных средств	

Наличие на АРМ с СКЗИ сертифицированных средств защиты информации от несанкционированного доступа (далее – СЗИ от НСД)	
Права пользователей СКЗИ на АРМ с СКЗИ (на учетные записи, на антивирусы, на СЗИ от НСД), права на удаленное администрирование и модификацию ОС и ее настроек на АРМ с СКЗИ	
Максимальные сроки действия паролей к учетным записям на АРМ с СКЗИ, параметры автоматической блокировки учетных записей	

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

№ п/п	АРМ проверен/не проверен	№ сертификата	Дата окончания сертификата	ФИО пользователя СКЗИ	Наименование СКЗИ	Серийный номер СКЗИ			Номер АРМ				Номер печати на АРМ			Обучение пользователей СКЗИ			Приказ о допуске		СЗИ от НСД	Антивирус	Права учётной записи	Аттестат соответствия
						Схема КЗ	ЖПУ	Фактическое состояние	Схема КЗ	Акт готовности	ЖПУ	Фактическое состояние	Схема КЗ	Акт готовности	Фактическое состояние	Схема КЗ	Заключение о сдаче зачетов	Фактическое состояние	Схема КЗ	Фактическое состояние				

Приложение №29. Программа проверки

ПРОГРАММА
проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в

_____
<Наименование организации>

ЦЕЛЬ ПРОВЕРКИ:

В рамках договора №22/2143-Д от 06.07.2012 осуществление контроля за реализацией требований Порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

ПРОВЕРЯЕМЫЕ ВОПРОСЫ:

Сотрудники ОКЗ/администраторы безопасности

1. Приказ о назначении администраторов безопасности и лиц, их замещающих (далее – Приказ):

наличие Приказа,

включение в Приказ всех сотрудников, выполняющих обязанности администратора безопасности,

включение администраторов безопасности в состав комиссии по составлению заключений на основании принятых от пользователей средств криптографической защиты информации (далее - СКЗИ) зачетов по программе обучения правилам работы с СКЗИ, а также по уничтожению СКЗИ и ключевых документов.

2. Уровень квалификации администратора безопасности для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ:

наличие у администратора безопасности подтверждения об обучении и/или повышении квалификации в организации, имеющей лицензию на ведение образовательной деятельности по соответствующим программам.

3. Наличие обязанностей администратора безопасности в должностных инструкциях сотрудников, выполняющих эти обязанности.

4. Ознакомление под расписку с Инструкцией 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, утвержденной Приказом ФАПСИ от 13 июня 2001г. №152 (далее – Инструкция №152).

5. Наличие у администраторов безопасности личных металлических печатей.

Помещение ОКЗ/помещение администраторов безопасности

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения, где хранятся СКЗИ, эксплуатационная и техническая документация к ним (далее – спецпомещения ОКЗ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения ОКЗ,

наличие опечатывающих устройств на дверях спецпомещений ОКЗ,

наличие замков на дверях спецпомещений ОКЗ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений ОКЗ,

учет ключей и их дубликатов от дверей спецпомещений ОКЗ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений ОКЗ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений ОКЗ ответственным должностным лицам.

2. Металлические хранилища для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей:

наличие металлических хранилищ,

наличие внутренних замков и кодовых замков или приспособлений для опечатывания замочных скважин металлических хранилищ,

наличие ключей и дубликатов ключей (как минимум двух экземпляров) от металлических хранилищ,

учет металлических хранилищ в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от металлических хранилищ в журнале учета хранилищ и ключей,

порядок сдачи ключей от металлических хранилищ ответственному должностному лицу по окончании рабочего дня,

порядок сдачи ключей от металлического хранилища ответственного должностного лица, где хранятся ключи от всех остальных хранилищ, в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от металлических хранилищ ответственным должностным лицам.

3. Окна спецпомещений ОКЗ:

наличие металлических решеток или ставней на окнах спецпомещений ОКЗ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения ОКЗ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения ОКЗ посторонних лиц,

наличие на окнах спецпомещений ОКЗ приспособлений для предотвращения просмотра извне спецпомещений ОКЗ.

Документация ОКЗ

1. Наличие утвержденного перечня лиц, допускаемых к самостоятельной работе с СКЗИ и его актуальность;
2. Наличие утвержденного Приказа о предоставлении прав подписей в системах (для банковских платежных систем) и его актуальность;
3. Выписка из номенклатуры дел.
4. Журнал учета хранилищ и ключей.
5. Журнал учета приема (сдачи) под охрану специальных помещений и ключей от них,
6. Журнал учета печатей и штампов.
7. Журнал учета электронных носителей информации, содержащих конфиденциальную информацию.
8. Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – журналы поэкземплярного учета):

наличие журналов поэкземплярного учета,

учет журналов поэкземплярного учета в номенклатуре дел,

правильность ведения журналов поэкземплярного учета (прошит/не прошит, наличие нумерации, правильность заполнения граф и пр.),

актуальность информации в журналах поэкземплярного учета.

9. Акты готовности СКЗИ к эксплуатации (далее – Акты):

наличие Актов,

правильность составления Актов,

актуальность информации в Актах.

10. Заключения о сдаче зачетов, составленные на основании принятых от пользователей СКЗИ зачетов по программе обучения:

наличие заключений о сдаче зачетов,

правильность составления заключений,

актуальность информации в заключениях о сдаче зачетов.

11. Наличие Заключений о возможности эксплуатации СКЗИ и их актуальность.

12. Заключения ПДТК на объекты информатизации, где установлены СКЗИ, но не обрабатывается конфиденциальная информация.

13. Аттестаты соответствия ФСТЭК на объекты информатизации с установленными СКЗИ.

Помещения с установленными СКЗИ

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения с установленными СКЗИ (далее – спецпомещения пользователей СКЗИ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения пользователей СКЗИ,

наличие опечатывающих устройств на дверях спецпомещений пользователей СКЗИ,

наличие замков на дверях спецпомещений пользователей СКЗИ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ,

учет ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений пользователей СКЗИ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений пользователей СКЗИ ответственным должностным лицам.

2. Шкафы (ящики, хранилища) индивидуального пользования:

наличие надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования,

наличие приспособлений для опечатывания замочных скважин на шкафах (ящиках, хранилищах) индивидуального пользования,

учет шкафов (ящиков, хранилищ) в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от шкафов (ящиков, хранилищ) в журнале учета хранилищ,

отметки о выдаче ключей и дубликатов ключей от шкафов (ящиков, хранилищ) ответственным должностным лицам.

3. Окна спецпомещений пользователей СКЗИ:

наличие металлических решеток или ставней на окнах спецпомещений пользователей СКЗИ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения пользователей СКЗИ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения пользователей СКЗИ посторонних лиц,,

наличие на окнах спецпомещений пользователей СКЗИ приспособлений для предотвращения просмотра извне спецпомещений пользователей СКЗИ.

Пользователи СКЗИ

1. Наличие у пользователей СКЗИ ключевых документов.
2. Наличие печатей у пользователей СКЗИ для опечатывания шкафов (ящиков, хранилищ).
3. Знания пользователями требований при работе с СКЗИ.
4. Выполнение пользователями требований при работе с СКЗИ.

АРМ пользователей СКЗИ

1. Наличие и соответствие учетных (серийных) номеров АРМ пользователей СКЗИ с номерами, указанными в ЖПУ и Актах.
2. Наличие и соответствие номеров средств контроля за вскрытием АРМ (печатей, пломб) с установленными СКЗИ с номерами, указанными в Актах.
3. Наличие СКЗИ на АРМ пользователей,
4. Актуальность сертификатов соответствия ФСБ на СКЗИ, установленные на АРМ пользователей СКЗИ.
5. Наличие на АРМ с СКЗИ сертифицированных антивирусных средств.
6. Наличие на АРМ с СКЗИ сертифицированных средств защиты информации от несанкционированного доступа (далее – СЗИ от НСД).
7. Права пользователей СКЗИ на АРМ с СКЗИ (на учетные записи, на антивирусы, на СЗИ от НСД), права на удаленное администрирование и модификацию ОС и ее настроек на АРМ с СКЗИ.
8. Максимальные сроки действия паролей к учетным записям на АРМ с СКЗИ, параметры автоматической блокировки учетных записей.

ОСНОВАНИЕ ДЛЯ ПРОВЕРКИ: _____

ВРЕМЯ ПРОВЕДЕНИЯ ПРОВЕРКИ: «__» _____ - «__» _____ 20__ года

ПРОГРАММА-ГРАФИК ПРОВЕРКИ:

№ п.п.	Вид выполняемых работ	Срок выполнения, ответственный
1	**Подготовка к проверке**	
1.1	Изучение материалов по объекту проверки: • выписка из Схемы организации криптографической защиты конфиденциальной информации; • выписка из Центра Регистрации Удостоверяющего центра Госкорпорации «Росатом». Уточнение перечня объектов, подлежащих проверке: • перечень СКЗИ; • перечень сертификатов ключей проверки электронной подписи.	
1.2.	Подготовка сводной таблицы по объекту проверки.	
2	**Проведение проверки**	
2.1	• Прибытие на предприятие; • Встреча с руководителем, проведение установочного совещания (разъяснение цели проверки); • Проверка сотрудников ОКЗ/администраторов безопасности; • Проверка помещения(ий) ОКЗ/помещения(ий) администраторов безопасности; • Проверка документации ОКЗ.	
2.2	• Проверка помещений с установленными СКЗИ; • Проверка пользователей СКЗИ; • Проверка АРМ пользователей СКЗИ.	
3	**Подведение итогов проверки**	
3.1	Формирование акта проверки и отправка на предприятие	

Начальник отдела криптографической защиты _____/_____
(подпись) (Ф.И.О)

Начальник Управления информационной безопасности _____/_____
(подпись) (Ф.И.О)

Приложение №30. Акт проверки

Рег. № _____
от _____

Для служебного пользования
(По заполнении)
Экз №__

УТВЕРЖДАЮ

<ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ ПРОВЕРКИ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

ОЗНАКОМЛЕН

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ЛИЦА, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

АКТ
проверки организации и обеспечения безопасности информации с использованием средств криптографической защиты в

_____
<Наименование организации>

СОГЛАСОВАНО

<ДОЛЖНОСТЬ ЧЛЕНА КОМИССИИ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

СОГЛАСОВАНО

<ДОЛЖНОСТЬ ЧЛЕНА КОМИССИИ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

В соответствии с Приказом АО «Гринатом»[1] от _____ №_____ «О проведении проверок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» органа криптографической защиты АО «Гринатом» (далее – ОКЗ) в период с «___» по «___»_____ 20__ г. комиссией в составе:

1. <ФИО ПРОВЕРЯЮЩЕГО>,
2. <ФИО ПРОВЕРЯЮЩЕГО>.

проведена проверка организации работ и состояния защиты с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее – защита информации) в <НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>, расположенном по адресу: _____.

ПРОВЕРКЕ ПОДВЕРГАЛИСЬ

Сотрудники ОКЗ/администраторы безопасности

1. Приказ о назначении администраторов безопасности и лиц, их замещающих (далее – Приказ):

наличие Приказа,

включение в Приказ всех сотрудников, выполняющих обязанности администратора безопасности,

включение администраторов безопасности в состав комиссии по составлению заключений на основании принятых от пользователей средств криптографической защиты информации (далее - СКЗИ) зачетов по программе обучения правилам работы с СКЗИ, а также по уничтожению СКЗИ и ключевых документов.

2. Уровень квалификации администратора безопасности для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ:

наличие у администратора безопасности подтверждения об обучении и/или повышении квалификации в организации, имеющей лицензию на ведение образовательной деятельности по соответствующим программам.

---

[1] Лицензия от 19.01.2017 ЛСЗ №0014254 Рег.№15686 на осуществление 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).

3. Наличие обязанностей администратора безопасности в должностных инструкциях сотрудников, выполняющих эти обязанности.

4. Ознакомление под расписку с Инструкцией 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, утвержденной Приказом ФАПСИ от 13 июня 2001г. №152 (далее – Инструкция №152).

5. Наличие у администраторов безопасности личных металлических печатей.

Помещение ОКЗ/помещение администраторов безопасности

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения, где хранятся СКЗИ, эксплуатационная и техническая документация к ним (далее – спецпомещения ОКЗ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения ОКЗ,

наличие опечатывающих устройств на дверях спецпомещений ОКЗ,

наличие замков на дверях спецпомещений ОКЗ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений ОКЗ,

учет ключей и их дубликатов от дверей спецпомещений ОКЗ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений ОКЗ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений ОКЗ ответственным должностным лицам.

2. Металлические хранилища для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей:

наличие металлических хранилищ,

наличие внутренних замков и кодовых замков или приспособлений для опечатывания замочных скважин металлических хранилищ,

наличие ключей и дубликатов ключей (как минимум двух экземпляров) от металлических хранилищ,

учет металлических хранилищ в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от металлических хранилищ в журнале учета хранилищ и ключей,

порядок сдачи ключей от металлических хранилищ ответственному должностному лицу по окончании рабочего дня,

порядок сдачи ключей от металлического хранилища ответственного должностного лица, где хранятся ключи от всех остальных хранилищ, в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от металлических хранилищ ответственным должностным лицам.

3. Окна спецпомещений ОКЗ:

наличие металлических решеток или ставней на окнах спецпомещений ОКЗ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения ОКЗ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения ОКЗ посторонних лиц,

наличие на окнах спецпомещений ОКЗ приспособлений для предотвращения просмотра извне спецпомещений ОКЗ.

Документация ОКЗ

1. Наличие утвержденного перечня лиц, допускаемых к самостоятельной работе с СКЗИ и его актуальность;
2. Наличие утвержденного Приказа о предоставлении прав подписей в системах (для банковских платежных систем) и его актуальность;
3. Выписка из номенклатуры дел.
4. Журнал учета хранилищ и ключей.
5. Журнал учета приема (сдачи) под охрану специальных помещений и ключей от них,
6. Журнал учета печатей и штампов.
7. Журнал учета электронных носителей информации, содержащих конфиденциальную информацию.
8. Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – журналы поэкземплярного учета):

наличие журналов поэкземплярного учета,

учет журналов поэкземплярного учета в номенклатуре дел,

правильность ведения журналов поэкземплярного учета (прошит/не прошит, наличие нумерации, правильность заполнения граф и пр.),

актуальность информации в журналах поэкземплярного учета.

9. Акты готовности СКЗИ к эксплуатации (далее – Акты):

наличие Актов,

правильность составления Актов,

актуальность информации в Актах.

10. Заключения о сдаче зачетов, составленные на основании принятых от пользователей СКЗИ зачетов по программе обучения:

наличие заключений о сдаче зачетов,

правильность составления заключений,

актуальность информации в заключениях о сдаче зачетов.

11. Наличие Заключений о возможности эксплуатации СКЗИ и их актуальность.
12. Заключения ПДТК на объекты информатизации, где установлены СКЗИ, но не обрабатывается конфиденциальная информация.

13. Аттестаты соответствия ФСТЭК на объекты информатизации с установленными СКЗИ.

Помещения с установленными СКЗИ

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения с установленными СКЗИ (далее – спецпомещения пользователей СКЗИ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения пользователей СКЗИ,

наличие опечатывающих устройств на дверях спецпомещений пользователей СКЗИ,

наличие замков на дверях спецпомещений пользователей СКЗИ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ,

учет ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений пользователей СКЗИ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений пользователей СКЗИ ответственным должностным лицам.

2. Шкафы (ящики, хранилища) индивидуального пользования:

наличие надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования,

наличие приспособлений для опечатывания замочных скважин на шкафах (ящиках, хранилищах) индивидуального пользования,

учет шкафов (ящиков, хранилищ) в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от шкафов (ящиков, хранилищ) в журнале учета хранилищ,

отметки о выдаче ключей и дубликатов ключей от шкафов (ящиков, хранилищ) ответственным должностным лицам.

3. Окна спецпомещений пользователей СКЗИ:

наличие металлических решеток или ставней на окнах спецпомещений пользователей СКЗИ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения пользователей СКЗИ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения пользователей СКЗИ посторонних лиц,,

наличие на окнах спецпомещений пользователей СКЗИ приспособлений для предотвращения просмотра извне спецпомещений пользователей СКЗИ.

Пользователи СКЗИ

1. Наличие у пользователей СКЗИ ключевых документов.
2. Наличие печатей у пользователей СКЗИ для опечатывания шкафов (ящиков, хранилищ).
3. Знания пользователями требований при работе с СКЗИ.
4. Выполнение пользователями требований при работе с СКЗИ.

АРМ пользователей СКЗИ

1. Наличие и соответствие учетных (серийных) номеров АРМ пользователей СКЗИ с номерами, указанными в ЖПУ и Актах.
2. Наличие и соответствие номеров средств контроля за вскрытием АРМ (печатей, пломб) с установленными СКЗИ с номерами, указанными в Актах.
3. Наличие СКЗИ на АРМ пользователей,
4. Актуальность сертификатов соответствия ФСБ на СКЗИ, установленные на АРМ пользователей СКЗИ.
5. Наличие на АРМ с СКЗИ сертифицированных антивирусных средств.
6. Наличие на АРМ с СКЗИ сертифицированных средств защиты информации от несанкционированного доступа (далее – СЗИ от НСД).
7. Права пользователей СКЗИ на АРМ с СКЗИ (на учетные записи, на антивирусы, на СЗИ от НСД), права на удаленное администрирование и модификацию ОС и ее настроек на АРМ с СКЗИ.
8. Максимальные сроки действия паролей к учетным записям на АРМ с СКЗИ, параметры автоматической блокировки учетных записей.

ПРОВЕРКОЙ УСТАНОВЛЕНО

Услуги по защите информации в осуществляет АО «Гринатом» в соответствии с договором присоединения от 06.07.2012 г. №22/2143-Д на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств (заявление о присоединении от _____ № _____, далее – Договор).

Объем работ по договорам на дату проверки:

1.	CLB.11	Предоставление услуг Удостоверяющего центра	___ ед.
2.	CLB.18	Обеспечение безопасности информации с использованием средств криптографической защиты информации	___ ед.
3.	GEN.23	Услуга Администратора безопасности	___ ед.

НАРУШЕНИЯ

Сотрудники ОКЗ/администраторы безопасности

6.1. …
6.2. …

Помещение ОКЗ/помещение администратора безопасности

1. ...
2. ...

Документация ОКЗ

1. ...
2. ...

Помещения пользователей СКЗИ

1. ...
2. ...

Пользователи СКЗИ

1. ...
2. ...

АРМ пользователей СКЗИ

1. ...
2. ...

УКАЗАНИЯ И РЕКОМЕНДАЦИИ

Сотрудники ОКЗ/администраторы безопасности

1. ...
2. ...

Помещение ОКЗ/помещение администратора безопасности

1. ...
2. ...

Документация ОКЗ

1. ...
2. ...

Помещения пользователей СКЗИ

1. ...
2. ...

Пользователи СКЗИ

1. ...
2. ...

АРМ пользователей СКЗИ

1. ...
2. ...

ВЫВОДЫ

1. ...
2. ...

<И.О. ФАМИЛИЯ>
<ТЕЛ>
__ экз. на __ л. каждый:
1 – в адрес
2 – в дело

Приложение №31. План устранения недостатков

«___» _____ 20___ г

ПЛАН

реализации рекомендаций по результатам проверки лицензиата ФСБ России АО «Гринатом»
в «НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ»

№ п/п	Недостатки, указанные в Акте проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в «Наименование организации»	Рекомендации по устранению выявленных недостатков	Ответственный	Срок	Отметка о выполнении (выполнено/не выполнено)

«ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ЛИЦА,
НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ»

_____/_____
(подпись) (Ф.И.О)

Приложение № 4

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

ФОРМА АКТА СДАЧИ-ПРИЕМКИ ОКАЗАННЫХ УСЛУГ

по Договору №_____ от «___» _____г.

г. Москва «_____» _____201__ г.

_____(_____), именуемое в дальнейшем «Заказчик», в лице _____, действующего на основании _____, с одной стороны, и

Акционерное общество «Гринатом» (АО «Гринатом»), именуемое в дальнейшем «Исполнитель», в лице _____, действующего на основании _____, с другой стороны, подписали настоящий акт сдачи-приемки оказанных Услуг по Договору №_____ от _____ (далее по тексту – Договор) о нижеследующем:

1. Состав и стоимость Услуг, оказанных Исполнителем за _____:

№	Код вида Услуги	Наименование вида Услуги	Кол-во	Ед.	Цена с НДС, руб.	Стоимость с НДС, руб.
1.						
2.						
					Итого:	
					В том числе НДС:	

Итого: _____(_____) рублей _____ копеек, включая НДС 20%_____(_____) рублей _____копеек.

2. Заказчик не имеет претензий к Исполнителю по качеству и объему оказанных Услуг. Никаких отступлений от Договора и иных недостатков в Услугах Исполнителя Заказчиком не обнаружено.

3. **Подписи Сторон:**

Заказчик:

_____

_____

_____

М.П.

Исполнитель:

АО «Гринатом»

_____

_____

М.П.

От Исполнителя:

Директор департамента

по информационным технологиям

_____А.Н. Киселёв

Приложение № 5
к Договору присоединения № 22/2143-Д от 06 июля 2012 г.

Перечень и стоимость услуг Исполнителя

г. Москва « ____ » _____ 2021 года

Стоимость услуг, оказываемых Исполнителем по настоящему Договору, составляет:

№	Код услуги	Код вида услуги	Наименование услуги	Единица измерения	Стоимость услуги с НДС, руб.[1]	В том числе НДС, руб.	Отчетный период
1.	CLB.11	**Предоставление услуг Корпоративного удостоверяющего центра (с 01.01.2021 до 30.06.2021)**					
		CLB.11 (УКЭП)	Выпуск квалифицированного сертификата ЭП	Ключевой документ	1 110,48	185,08	Квартал
		CLB.11 (УНЭП)	Выпуск неквалифицированного сертификата ЭП с записью на ключевой носитель	Ключевой документ	1 031,45	171,91	
		Предоставление услуг Корпоративного удостоверяющего центра (с 01.07.2021)					
		CLB.11 (УКЭП21)	Выпуск квалифицированного сертификата ЭП по требования 476-ФЗ	Ключевой документ	4441,92	740,32	Единовременно за один сертификат
2.	CLB.18	**Обеспечение безопасности информации с использованием средств криптографической защиты информации (СКЗИ в собственности АО «Гринатом» / Заказчика)**					
		CLB.18 (КриптоПро CSP клиентская)	СКЗИ «КриптоПро CSP» клиентская лицензия в собственности АО «Гринатом»	СКЗИ	1 117,15	186,19	Квартал
		CLB.18 (КриптоПро CSP серверная)	СКЗИ «КриптоПро CSP» серверная лицензия в собственности АО «Гринатом»	СКЗИ	4 359,67	726,61	

[1] Стоимость указана за одну единицу измерения, действующую в течение отчетного периода, кроме услуг, оказываемых единоразово.

№	Код услуги	Код вида услуги	Наименование услуги	Единица измерения	Стоимость услуги с НДС, руб.[1]	В том числе НДС, руб.	Отчетный период
		CLB.18 (S-Terra CSP VPN Client)	СКЗИ «S-Terra CSP VPN Client» в собственности АО «Гринатом»	СКЗИ	1 709,78	284,96	
		CLB.18 (ViPNet Client)	СКЗИ «ViPNet Client» в собственности АО «Гринатом»	СКЗИ	1 197,25	199,54	
		CLB.18 (КриптоПро TSP Client клиентская)	Клиентская лицензия «КриптоПро TSP Client»	Рабочее место с СКЗИ	967,36	161,23	
		CLB.18 (КриптоПро OCSP Client клиентская)	Клиентская лицензия «КриптоПро OCSP Client»	Рабочее место с СКЗИ	967,36	161,23	
		CLB.18 (КриптоПро JCP серверная)	СКЗИ «КриптоПро JCP» серверная лицензия в собственности АО «Гринатом»	СКЗИ	8 059,36	1 343,23	
		CLB.18 (СКЗИ заказчика)	СКЗИ в собственности Заказчика	СКЗИ	859,36	143,23	
3.	CLB.21	**Контроль (оценка) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем**					
		CLB.21 (серверная часть системы)	Серверная часть системы	Система	33 119,24	5 519,87	Квартал
		CLB.21 (клиентская часть системы)	Клиентская часть системы	Система	13 497,44	2 249,57	
4.	CLB.23	-	Предоставление услуг Платформы доверенных сервисов в отношении облачных неквалифицированных сертификатов (ПДС облачная УНЭП)	Ключевой документ	449,93	74,99	Квартал

№	Код услуги	Код вида услуги	Наименование услуги	Единица измерения	Стоимость услуги с НДС, руб.[1]	В том числе НДС, руб.	Отчетный период
5.	CLB.26	**Подключение и обслуживание абонентского пункта комплекса «ViPNet-Гринатом»**					
		CLB.26 (ДП)	Подключение и обслуживание абонентского пункта «Деловой почты» комплекса «ViPNet-Гринатом» (Деловая почта)	Абонентский пункт	1 431,76	238,63	Квартал
		CLB.26 (ИС)	Подключение и обслуживание абонентского пункта для предоставления доступа к корпоративным и локальным информационным системам (ИС)	Абонентский пункт	1 431,76	238,63	
		CLB.26 (Координатор)	Подключение и обслуживание ПАК ViPNet Coordinator в составе сети комплекса «ViPNet-Гринатом» (Координатор)	Координатор	1 431,76	238,63	
6.	CLB.32	**Предоставление услуги интеграционной поддержки ПДС**					
		CLB.32 (Функциональная поддержка)	Функциональная поддержка.	Система	320 672,23	53 445,37	Квартал
		CLB.32 (Поддержка интеграционных сервисов)	Поддержка интеграционных процессов	Система	855 125,93	142 520,99	Единоразово
7.	GEN.23	**Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом»**					
		GEN.23 (Москва)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Москва	Рабочее место с СКЗИ	3 088,37	514,73	Квартал
		GEN.23 (Ангарск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Ангарск	Рабочее место с СКЗИ	1 450,15	241,69	

№	Код услуги	Код вида услуги	Наименование услуги	Единица измерения	Стоимость услуги с НДС, руб.[1]	В том числе НДС, руб.	Отчетный период
		GEN.23 (Владимир)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Владимир	Рабочее место с СКЗИ	494,10	82,35	
		GEN.23 (Глазов)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Глазов	Рабочее место с СКЗИ	843,19	140,53	
		GEN.23 (Димитровград)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Димитровград	Рабочее место с СКЗИ	853,96	142,33	
		GEN.23 (Зеленогорск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Зеленогорск	Рабочее место с СКЗИ	1 315,87	219,31	
		GEN.23 (Ковров)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Ковров	Рабочее место с СКЗИ	547,81	91,30	
		GEN.23 (Нижний Новгород)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Нижний Новгород	Рабочее место с СКЗИ	1 396,44	232,74	
		GEN.23 (Новосибирск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Новосибирск	Рабочее место с СКЗИ	1 084,90	180,82	
		GEN.23 (Новоуральск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Новоуральск	Рабочее место с СКЗИ	1 015,06	169,19	
		GEN.23 (Подольск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Подольск	Рабочее место с СКЗИ	1 197,68	199,61	

№	Код услуги	Код вида услуги	Наименование услуги	Единица измерения	Стоимость услуги с НДС, руб.[1]	В том числе НДС, руб.	Отчетный период
		GEN.23 (Санкт-Петербург)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Санкт-Петербург	Рабочее место с СКЗИ	1 219,18	203,20	
		GEN.23 (Саров)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Саров	Рабочее место с СКЗИ	2 567,34	427,89	
		GEN.23 (Северск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Северск	Рабочее место с СКЗИ	1 127,84	187,97	
		GEN.23 (Электросталь)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Электросталь	Рабочее место с СКЗИ	1 047,31	174,55	
		GEN.23 (Мурманск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Мурманск	Рабочее место с СКЗИ	2 402,32	400,39	
		GEN.23 (Краснокаменск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в г. Краснокаменск	Рабочее место с СКЗИ	1 179,11	196,52	
8.	GEN.43	**Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищённой средствами криптографической защиты на АРМ пользователя**					
		GEN.43 (Москва)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Москва	Учетная запись с ключевым документом в ИС	3 810,74	635,12	Квартал
		GEN.43 (Новосибирск)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами	Учетная запись с ключевым	2 128,46	354,74	

№	Код услуги	Код вида услуги	Наименование услуги	Единица измерения	Стоимость услуги с НДС, руб.[1]	В том числе НДС, руб.	Отчетный период
			криптографической защиты информации на АРМ пользователя в г. Новосибирск	документом в ИС			
		GEN.43 (Глазов)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Глазов	Учетная запись с ключевым документом в ИС	1 944,94	324,16	
		GEN.43 (Северск)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Северск	Учетная запись с ключевым документом в ИС	2 105,32	350,89	
		GEN.43 (Мурманск)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Мурманск	Учетная запись с ключевым документом в ИС	2 980,26	496,71	
		GEN.43 (Димитровград)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Димитровград	Учетная запись с ключевым документом в ИС	1 525,75	254, 29	
		GEN.43 (Санкт-Петербург)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Санкт-Петербург	Учетная запись с ключевым документом в ИС	2 831,36	471,89	
		GEN.43 (Подольск)	Услуга по сопровождению учетной записи с электронной подписью в информационной	Учетная запись с	2 454,95	409,16	

№	Код услуги	Код вида услуги	Наименование услуги	Единица измерения	Стоимость услуги с НДС, руб.[1]	В том числе НДС, руб.	Отчетный период
			системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Подольск	ключевым документом в ИС			
		GEN.43 (Нижний Новгород)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Нижний Новгород	Учетная запись с ключевым документом в ИС	2 595,46	432,58	
		GEN.43 (Электросталь)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Электросталь	Учетная запись с ключевым документом в ИС	2 156,29	359,38	
		GEN.43 (Новоуральск)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Новоуральск	Учетная запись с ключевым документом в ИС	2 066,47	344,41	
		GEN.43 (Саров)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Саров	Учетная запись с ключевым документом в ИС	3 602,84	600,47	
		GEN.43 (Ангарск)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Ангарск	Учетная запись с ключевым документом в ИС	2 925,36	487,56	

№	Код услуги	Код вида услуги	Наименование услуги	Единица измерения	Стоимость услуги с НДС, руб.[1]	В том числе НДС, руб.	Отчетный период
		GEN.43 (Ковров)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Ковров	Учетная запись с ключевым документом в ИС	1 729,33	288,22	
		GEN.43 (Зеленогорск)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Зеленогорск	Учетная запись с ключевым документом в ИС	2 493,04	415,51	
		GEN.43 (Владимир)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Владимир	Учетная запись с ключевым документом в ИС	1 545,23	257,54	
		GEN.43 (Краснокаменск)	Услуга по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя в г. Краснокаменск	Учетная запись с ключевым документом в ИС	1 689,59	281,60	

От Исполнителя:

АО «Гринатом»

Директор по
информационным технологиям

Акционерное общество "Гринатом" * ОГРН 1097746819720 * МОСКВА *
Гринатом

А.Н. Киселёв

М.П.

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

У Т В Е Р Ж Д А Ю
Директор по информационным технологиям
АО «Гринатом»

_____/ А.Н. Киселёв /

М.П.

ПОРЯДОК

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

Москва 2021 г.

Содержание

1. Назначение и область применения

Настоящий порядок контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем» (далее – Порядок), разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты.

Настоящий Порядок определяет условия предоставления и правила пользования услугой органа криптографической защиты АО «Гринатом» 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 органа криптографической защиты АО «Гринатом». Порядок имеет статус локального.

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

1. Руководитель Органа криптографической защиты АО «Гринатом»,
2. Проверяющий.

Настоящий Порядок использует ссылки на следующие документы, необходимые для контроля (оценки) уровня доверия и контроля 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.№15686 Н 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	Действует	Лицензия	Волков С.П.

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 06.04.11 г. № 63-ФЗ "Об электронной подписи"	Действует	Федеральный закон	Волков С.П.
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	Волков С.П.
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	Волков С.П.
Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты	Действует	Требование	Волков С.П.

информации в Госкорпорации «Росатом» и ее организациях» (с пометкой «Для служебного пользования»)			
Единые отраслевые методические указания по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утв. Приказом от 22.10.2015 №1/1009-П	Действует	Указания	Руководители организаций ГК «Росатом»

2. Термины, определения и сокращения

Термин	Определение
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 работников, назначенных Приказом «О возложении дополнительных функциональных обязанностей работников Органа криптографической защиты АО «Гринатом» на штатных работников»
Пользователи СКЗИ	Физические лица, непосредственно допущенные к работе с СКЗИ
Система	Информационная/телекоммуникационная система, защищенная с использованием шифровальных (криптографических) средств

Средства криптографической защиты информации (СКЗИ)	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
ООКИ	Организация-обладатель конфиденциальной информации
ОКЗ	Орган криптографической защиты АО «Гринатом»
Руководитель ООКИ	Руководитель организации-обладателя конфиденциальной информации
СКЗИ	Средства криптографической защиты информации
СПДС	Средство построения доверенной среды
СФК	Среда функционирования криптосредства

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

- оценка уровня доверия к криптографическим сервисам Систем;
- периодический (ежемесячный) контроль (оценка) уровня доверия к Системам;
- выдача Заключения ОКЗ о возможности эксплуатации Систем (далее – Заключение);
- контроль приведения Систем и документации на них в соответствие с требованиями по информационной безопасности;
- мониторинг актуальности документов Минкомсвязи России, ФСБ России, ФСТЭК России, производителей программного обеспечения, органа по аттестации объекта информатизации, владельца системы, органа криптографической защиты.

3.3. Участники группы процессов и их роли

№ п.п.	Участники	Основные роли
1	Проверяющий	• оценивает уровень доверия к криптографическим сервисам Систем; • периодически (ежемесячно) контролирует (оценивает) уровень доверия к Системам; • составляет Заключения Органа криптографической защиты о возможности эксплуатации Систем (далее – Заключения); • контролирует приведение Систем и документации на них в соответствие с требованиями по информационной безопасности; • осуществляет мониторинг актуальности документов Минкомсвязи России, ФСБ России, ФСТЭК России, производителей программного обеспечения, органа по аттестации объекта информатизации, владельца системы, органа криптографической защиты.
2	Руководитель Органа криптографической защиты АО «Гринатом»	• Принимает решение об оказании/завершении 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; • Согласовывает выдачу Заключений.

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	Письмо в Банк о предоставлении информации, необходимой для контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем	Банк	Организация
2	Письмо в Банк с запросом на приведение Системы в соответствие с ЕОМУ	Банк	Организация
3	Заключение Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе	ООКИ	Организация
4	Отчет о проведении регламентных работ	ООКИ	Организация
5	Выписка из Заключения Органа криптографической	Банк	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация,/ Дивизион/ Организация)
	защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе		

3.5. Основные входы процесса

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
1	Заявление на подключение/отключение услуги по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем	ООКИ	Организация
2	Скан-копии заключенных/проекты заключаемых договоров	ООКИ	Организация

	(доп. соглашений) на Системы		
3	Скан-копии документов по аттестации на соответствие требованиям безопасности объекта информатизации, где обрабатывается конфиденциальная информация	ООКИ	Организация
4	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
5	Выписка из Заключения Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе	АО «Гринатом»	Организация
6	Документы из Банка	Банк	Организация
7	Отчет о проведении регламентных работ	АО «Гринатом»	Организация
8	Ответ Банка о приведении Системы в соответствие с ЕОМУ	Банк	Организация
9	Заключение Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе	АО «Гринатом»	Организация

3.6. Описание процесса

В случае если ООКИ подключается к услуге по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем (далее – услуга CLB.21) с Едиными отраслевыми методическими указаниями по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» (далее – ЕОМУ):

в ОКЗ из ООКИ поступает следующий комплект документов:

– оригинал подписанного Заявления на подключение услуги по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем (Приложение №4),

– скан-копии заключенных/проекты заключаемых договоров (доп. соглашений) на Системы,

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

В случае если ООКИ отключается от услуги CLB.21:

в ОКЗ из ООКИ поступает Заявление на отключение от услуги по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем (Приложение №4)

Руководитель ОКЗ:

- Принимает решение об оказании/завершении оказания услуги CLB.21 в соответствии с поступившим Заявлением на подключение, либо на отключение от услуги CLB.21.

Если принято решение об оказании услуги CLB.21:

Проверяющий:

- Запрашивает официальным письмом (Приложение №5) в Банке следующую документацию:

  Для оценки доверия к технологии, реализующей инфраструктуру ключевой системы:

  – лицензию ФСБ России на соответствующие виды деятельности,
  – лицензию на программное обеспечение,
  – сертификаты соответствия в соответствии с системой сертификации РОСС RU.0001.030001 по классу КС2 или КС3 на средство, реализующем инфраструктуру ключевой системы;

- документацию на СКЗИ (копия формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника));
- документацию, регламентирующую жизненный цикл ключевой системы;
- свидетельство об аккредитации;
- документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации);
- сертификат соответствия на средство автоматизации удостоверяющего центра (соответствует/не соответствует «Требованиям к средствам удостоверяющего центра» (приложение № 2 к приказу ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»);
- документацию о наличии дополнительных служб удостоверяющего центра (службы онлайновой проверки статусов сертификатов и службы штампов времени);
- документацию о поддержке формата усовершенствованной подписи.

Для оценки доверия к средствам криптографической защиты, входящим в состав системы обработки данных:

- сертификаты соответствия ФСБ России на средства криптографической защиты информации, использующиеся в Системе (класс защиты применяемых шифровальных (криптографических) средств);
- документацию на СКЗИ (копия формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника));
- сертификаты соответствия на ключевые носители.

Для оценки доверия к СФК, средствам обработки и отображения данных:

- заключение ОКЗ о возможности эксплуатации СКЗИ;
- сертификат соответствия ФСТЭК на СЗИ от НСД;
- сертификат соответствия ФСТЭК на антивирусное ПО;
- заключение о корректности встраивания СКЗИ в Систему;
- документация на Систему;
- документация с зафиксированной версией Системы и операционной системой;
- аттестата соответствия по требованиям по информационной безопасности на АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация;
- сертификат соответствия ФСБ России на СПДС.

Для оценки доверия к участникам процессов обработки данных:

- Локальные нормативные акты, обеспечивающие повышение осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации и использования технических средств защиты информации;
- Локальные нормативные акты, определяющие права и роли работников в системе.

- Анализирует полученную от Банка документацию,
- Составляет и согласовывает Заключение Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе (далее – Заключение, Приложение №6).

Руководитель ОКЗ:

- Утверждает Заключение.

Если Система соответствует ЕОМУ:

Проверяющий:

- Отправляет Заключение в ООКИ,
- Осуществляет регламентные работы (ежемесячно):

Мониторинг актуальности документов ФСБ России:

– лицензии ФСБ России на соответствующие виды деятельности,

– сертификата соответствия ФСБ России на средство, реализующие инфраструктуру ключевой системы,

– сертификата соответствия ФСБ России на средства криптографической защиты информации,

– сертификата соответствия ФСБ на СПДС.

Мониторинг документов производителей программного обеспечения:

– заключения о корректности встраивания СКЗИ в систему,

– документации на программное обеспечение системы ДБО.

Мониторинг актуальности документов ФСТЭК:

– сертификата соответствия ФСТЭК на антивирусное ПО,

– сертификата соответствия ФСТЭК на СЗИ от НСД,

– аттестата соответствия ФСТЭК на АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация.

Мониторинг документов банка:

– генеральной лицензии на осуществление банковских операций,

– документа о выполнении Стандарта Банка России,

– заключения Органа криптографической защиты о возможности эксплуатации СКЗИ,

– лицензии на программное обеспечение,

– документов, регламентирующих жизненный цикл ключевой системы.

Мониторинг документов Минкомсвязи России:

– свидетельства об аккредитации,

- формирует и отправляет в ООКИ отчет о проведении регламентных работ.

Если после проведения регламентных работ выяснилось, что уровень доверия к криптографическим сервисам изменился, то

Проверяющий:

- формирует, согласовывает и направляет в ООКИ новое Заключение.

Если Система не соответствует ЕОМУ, либо если в ходе проведения регламентных работ выяснилось, что уровень доверия к криптографическим сервисам понизился/повысился до неприемлемого, то

Проверяющий:

- Формирует выписку из Заключения,
- Направляет в Банк письмо с запросом на приведение Системы в соответствие с ЕОМУ выписку из Заключения,
- Анализирует полученный ответ от Банка по приведению Системы в соответствие с ЕОМУ.

Если Система приведена в соответствие с ЕОМУ, то формируется новое Заключение и проводятся (ежемесячно) регламентные работы.

Если Система не приведена в соответствие с ЕОМУ, то процесс взаимодействия с Банком повторяется.

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.№15686 Н 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);
- Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» (с пометкой «Для служебного пользования»);
- 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 Порядок, а также в приложения к нему, производится посредством утверждения новой редакции Порядка.

6. Контроль и ответственность

6.1 Порядок обязаны соблюдать все следующие участники процесса

Руководитель ОКЗ;

Проверяющий.

6.2. Ответственность работников за несоблюдение требований Порядка

За несоблюдение Порядка 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.	Форма Заявления на подключение/отключение услуги по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
Приложение №5.	Форма письма в Банк с запросом о предоставлении информации, необходимой для контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
Приложение №6.	Форма Заключения Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе.

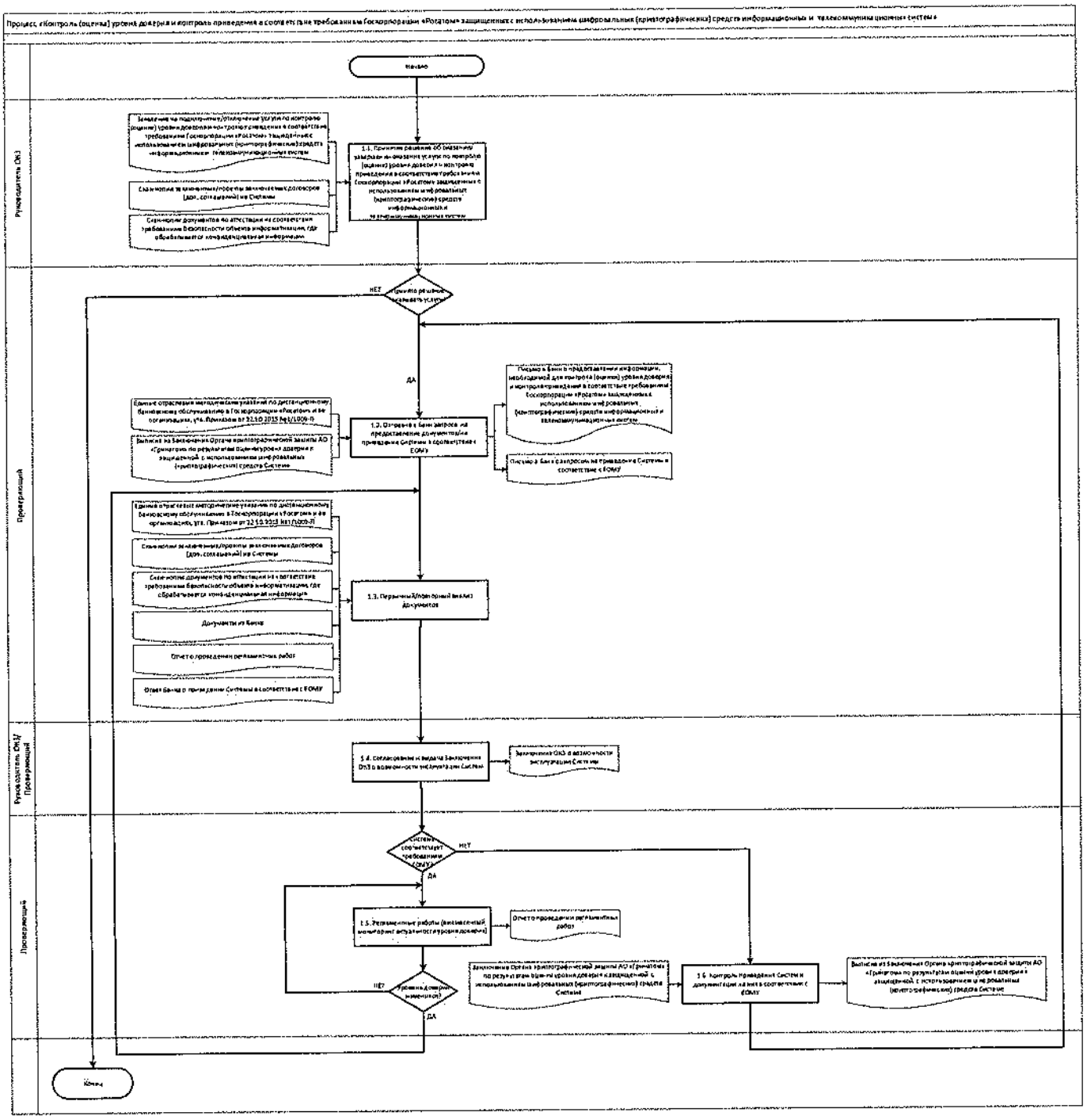
Приложение №1. Матрица ответственности

Процесс	**Участники процесса**	
	Руководитель ОКЗ	**Проверяющий**
Контроль (оценка) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем	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



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. Форма Заявления на подключение/отключение услуги по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем

ЗАЯВЛЕНИЕ
на
ПОДКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ

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

ПОДКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ «_____» _____ 201__ г.
(нужное подчеркнуть)

_____
наименование организации, включая организационно-правовую форму

в лице _____,
должность

_____,
фамилия, имя, отчество

действующего на основании _____

просит Орган криптографической защиты АО «Гринатом» осуществить/завершить
(нужное подчеркнуть)

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 №1.

Копии заключаемых/заключенных договоров на Систему(ы) (доп. соглашений) и приложения к ним прилагаются

Таблица №1

№ п/п	Наименование информационной/ телекоммуникационной системы, защищенной с использованием шифровальных (криптографических) средств	Вид защищаемой информации	Учетный номер АРМ, на котором установлена/ планируется установка Системы	Адрес месторасположения АРМ, на котором установлена/ планируется установка Системы	Операционная система, антивирусные средства, средства защиты информации от несанкционированного доступа, установленные на АРМ. Реквизиты аттестата соответствия по требованиям безопасности информации

Администратор безопасности

_____/_____
(подпись) (ФИО)

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ДОЛЖНОСТНОГО ЛИЦА>

_____ _____/_____
(подпись) (ФИО)

м.п.

Приложение №5. Форма письма в Банк с запросом о предоставлении информации, необходимой для контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем

Акционерное общество «Гринатом»
(АО «Гринатом»)

1-й Нагатинский проезд, д. 10, стр. 1,
Москва, 115230
Телефон (499) 949-49-19, факс (499) 949-44-46
E-mail: info@greenatom.ru
ОКПО 64509942, ОГРН 1097746819720
ИНН 7706729736, КПП 770601001

«ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ЛИЦА»
«НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ»

«И.О.ФАМИЛИЯ»

_____ № _____

На № _____ от _____

О проведении оценки уровня доверия
к «НАИМЕНОВАНИЕ СИСТЕМЫ»

Уважаемый(ая) <ИМЯ, ОТЧЕСТВО>!

Орган криптографической защиты лицензиата ФСБ России АО «Гринатом» (лицензия ЛСЗ №0014254 Рег. №15686Н от 19.01.2017г.) в рамках контроля (оценки) уровня доверия и приведения в соответствие требованиям Госкорпорации «Росатом» «НАИМЕНОВАНИЕ СИСТЕМЫ» (договор от _____ №_____) просит Вас предоставить документацию:

копию лицензии ФСБ России на разработку, производство, распространение шифровальных(криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных(криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных(криптографических) средств;

копию лицензии на программное обеспечение, передаваемое Банком Клиенту в рамках договора от _____ №_____;

копию сертификата соответствия ФСБ России на средство, реализующее инфраструктуру ключевой системы;

копию документации на СКЗИ (копию учтенного формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника));

копию документации, регламентирующей жизненный цикл ключевой системы;

копию свидетельства Минкомсвязи России об аккредитации удостоверяющего центра Банка;

копию документа, подтверждающего соответствие Стандарту Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации СТО БР ИББС-1.0-2014»;

копию сертификата соответствия ФСБ России на средство автоматизации удостоверяющего центра;

копию регламентов служб TSP и OCSP (документацию на службу онлайновой проверки статусов сертификатов и службы штампов времени);

копию документации о поддержке формата усовершенствованной подписи;

копию сертификата соответствия ФСБ России на средства криптографической защиты информации, использующиеся в «НАИМЕНОВАНИЕ СИСТЕМЫ»;

копию сертификата соответствия ФСТЭК России на ключевые носители;

копию сертификата соответствия ФСТЭК России на СЗИ от НСД;

копию сертификата соответствия ФСТЭК России на антивирусное ПО;

копию заключения о корректности встраивания СКЗИ в «НАИМЕНОВАНИЕ СИСТЕМЫ»;

копию документации на «НАИМЕНОВАНИЕ СИСТЕМЫ»;

копию документа, подтверждающего оценку соответствия по требованиям безопасности информации (копия аттестата соответствия по требованиям безопасности информации на АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация);

копию сертификата соответствия ФСБ России на СПДС;

копию локальных нормативных актов, обеспечивающих повышение осведомленности работников в области обеспечения защиты информации;

копию локальных нормативных актов по порядку применения организационных мер защиты информации и использования технических средств защиты информации;

Непредоставление указанных документов будет рассматриваться как их отсутствие при контроле (оценке) уровня доверия, и приведении в соответствие требованиям Госкорпорации «Росатом» «НАИМЕНОВАНИЕ СИСТЕМЫ».

С уважением,

Начальник Отдела криптографической защиты <И.О. ФАМИЛИЯ>

(по дов. № _____-_____ от __.__.__)

Приложение №6. Форма Заключения Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе

УТВЕРЖДАЮ

Начальник
отдела криптографической защиты
АО «Гринатом»

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

ЗАКЛЮЧЕНИЕ

по результатам оценки уровня доверия
к *«наименование системы»*

Москва 20__ г.

1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

2. ВВОДНАЯ ЧАСТЬ

2.1. Основание для выдачи заключения

Основанием для выдачи настоящего заключения является договор от _____ № _____.

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

«Наименование системы».

2.3. Вопросы для исследования

– Обеспечение доверия к технологии, реализующей инфраструктуру ключевой системы;
– Обеспечение доверия к средствам криптографической защиты информации, входящим в состав системы обработки данных;
– Обеспечение доверия к средствам обработки и отображения данных;
– Обеспечение доверия к участникам процессов обработки данных.

3. ИССЛЕДОВАТЕЛЬСКАЯ ЧАСТЬ

Оценка уровня доверия к системе проводится в соответствии с ЕОМУ.
Методы исследования:
- анализ представленной в ОКЗ АО «Гринатом» документации на систему;
- анализ документа *«наименование договора/соглашения на использование системы».*

4. В ПРОЦЕССЕ ИССЛЕДОВАНИЯ УСТАНОВЛЕНО

4.1. Описание системы

4.2. Инфраструктура ключевой системы

4.3. Жизненный цикл ключевых документов

4.3.1 Получение, создание и замена ключевых документов

4.3.2 Хранение ключевых документов

4.3.3 Уничтожение ключевых документов

4.4. Жизненный цикл СКЗИ

4.4.1 Получение СКЗИ

4.4.2 Проверка готовности, установка и эксплуатация СКЗИ

4.4.3 Уничтожение СКЗИ

4.5. Механизм обеспечения конфиденциальности и целостности информации в системе

4.6. Выполнение требований по безопасности информации на стороне Клиента и Банка

4.7. Анализ документа *«наименование договора/соглашения на использование системы»*

5. ОЦЕНКА СООТВЕТСТВИЯ

5.1. Результаты исследования технологии, реализующей инфраструктуру ключевой системы

Критерий оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия
Лицензия ФСБ России Банка на осуществление лицензируемых видов деятельности					
Документ, подтверждающий наличие прав Банка на использование средства, реализующего инфраструктуру ключевой системы и СКЗИ, применяемого 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, реализующее инфраструктуру ключевой системы с указанием на соответствие «Требованиям к средствам удостоверяющего центра» (приложение №2 к приказу ФСБ России от 27.12.2011 №796 «Об утверждении Требований к средствам электронной подписи и требований к средствам удостоверяющего центра»					
Действующий сертификат соответствия ФСБ России на СКЗИ, применяемое для работы средства, реализующего инфраструктуру ключевой системы с классом защиты не ниже КС2					
Использование Клиентом сертифицированных ФСТЭК России/ФСБ России или несертифицированных (типа токен/смарт-карты или flash-носитель/жесткий диск ПЭВМ) ключевых носителей					
Использование Банком сертифицированных ФСТЭК России/ФСБ России или несертифицированных (типа токен/смарт-карты или flash-носитель/жесткий диск ПЭВМ) ключевых носителей					
Документы, регламентирующие жизненный цикл ключевой системы					
Свидетельство об аккредитации УЦ в Минкомсвязи России					

В Системе для подписи используется усиленная квалифицированная/ усиленная неквалифицированная электронная подпись					
Документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации)					
Наличие дополнительных служб удостоверяющего центра (службы проверки статуса сертификата (online certificate status protocol) и штампов времени (time-stamp protocol)) и использование формата усовершенствованной электронной подписи в Системе					

5.2. Результаты исследования СКЗИ, входящих в состав системы обработки данных

Критерий оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия
Использование сертифицированных ФСБ России СКЗИ на АРМ Пользователей Клиента для обеспечения конфиденциальности информации					
Использование сертифицированных ФСБ России СКЗИ на АРМ Пользователей Клиента для обеспечения целостности информации					
Использование сертифицированных ФСБ России СКЗИ на АРМ Пользователей Банка для обеспечения целостности информации					
Документы, подтверждающие право передачи Клиенту СКЗИ и эксплуатационной и технической документации к ним, использующихся в работе Системы (договор, лицензия и пр.)					
Класс защиты применяющихся на рабочих местах пользователей Клиента Системы шифровальных (криптографических) средств					
Класс защиты применяющихся на рабочих местах пользователей Банка Системы шифровальных (криптографических) средств					

5.3. Результаты исследования средств обработки и отображения данных

Критерий оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия
Лицензия на программное обеспечение Системы					
Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Клиента					
Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Банка					
Заключение о корректности встраивания СКЗИ в Систему					
Документация на систему дистанционного банковского обслуживания (техническое описание или техническая записка, инструкция пользователя, инструкция администратора безопасности)					
Аттестат соответствия ФСТЭК на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация на стороне Клиента					

Аттестат соответствия ФСТЭК России на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация на стороне Банка					
Установлено сертифицированное антивирусное ПО на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы					
Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Клиента					
Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Банка					
Установлено сертифицированное СЗИ от НСД на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы					
Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Клиента					
Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Банка					

5.4. Результаты исследования участников процессов обработки данных

Критерий оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия
Документ, подтверждающий допуск пользователей Клиента к работе с СКЗИ в Системе					
Документ, подтверждающий допуск пользователей Банка к работе с СКЗИ в Системе					
Документ, подтверждающий прохождение обучения пользователями Системы на стороне Клиента					
Документ, подтверждающий прохождение обучения пользователями Системы на стороне Банка					
Локальные нормативные акты, определяющие права и роли работников Клиента в Системе (подписантов, администраторов безопасности)					
Локальные нормативные акты, определяющие права и роли работников Банка в Системе (подписантов, администраторов безопасности)					
Контроль администраторами безопасности условий использования СКЗИ на стороне Клиента					
Контроль администраторами безопасности условий использования СКЗИ на стороне Банка					

6. ВЫВОДЫ И РЕКОМЕНДАЦИИ

6.1. Выводы

«Наименование системы» обеспечивает _____ уровень доверия, согласно ЕОМУ.

6.2. Рекомендации

7. Список приложений

Приложение № 7 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю
Директор по информационным
технологиям
АО «Гринатом»

_____/ А.Н. Киселёв /

М.П.

ПОРЯДОК

организации и обслуживания защищённой сети комплекса «ViPNet-Гринатом»

Москва 2021 г.

Содержание

1. Назначение и область применения

Настоящий порядок организации и обслуживания защищённой сети комплекса «ViPNet-Гринатом» (далее – Порядок), разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты (далее – ОКЗ).

Настоящий Порядок определяет условия подключения и обслуживания автоматизированных рабочих мест, а также сетевого оборудования в сети №11296 комплекса «ViPNet-Гринатом» для работы с продуктами на базе решений от разработчика средств криптографической защиты информации (далее – СКЗИ) ОАО «ИнфоТеКС».

Требования настоящего Порядка распространяются на организации и предприятия использующие программное обеспечение (далее – ПО), сетевое оборудование в сети №11296 комплекса «ViPNet-Гринатом», и обязательны для выполнения работниками, исполняющими следующие функциональные роли:

1. Руководитель организации-обладателя конфиденциальной информации;
2. Администратор сети комплекса «ViPNet-Гринатом» (далее – Администратор сети ViPNet);
3. Администратор безопасности органа криптографической защиты;
4. Пользователь сети комплекса «ViPNet-Гринатом».

Настоящий Порядок использует ссылки на следующие документы, необходимые для управления процессом Организация и обслуживание защищённой сети комплекса «ViPNet-Гринатом»:

Документ	Статус	Тип документа	Ответственный
Лицензия ФСБ России ЛСЗ № 0014254 Рег.№15686 Н 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,	Действует	Лицензия	Волков С.П.

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	Волков С.П.
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	Волков С.П.
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	Волков С.П.
Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» (с	Действует	Требование	Волков С.П.

пометкой «Для служебного пользования»)			
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Действует	Требование	Волков С.П.
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).	Действует	Требование	Волков С.П.
Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности"	Действует	Требование	Волков С.П.

и является основой для регламентации следующих процессов и подпроцессов:

Процесс:

Подключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»
Подпроцессы:
«Подключение/отключение абонентских пунктов, обслуживание Деловой почты»
«Создание связей новому пользователю и отправка обновления справочников и ключей»
«Обеспечение функционирования Деловой почты»
«Выпуск и обмен ключей и межсетевой информацией с доверенными сетями ViPNet»
«Вывод из эксплуатации Деловой почты»

Процесс:
«Подключение/отключение и обслуживание ViPNet Coordinator в сети комплекса «ViPNet-Гринатом»
Подпроцесс:
«Подключение/отключение и обслуживание ViPNet Coordinator в сети комплекса «ViPNet-Гринатом»
«Создание связей ViPNet Coordinator и отправка обновления справочников и ключей»
«Обеспечение функционирования ViPNet Coordinator»
«Вывод из эксплуатации ViPNet Coordinator»

Процесс:
«Предоставление доступа к корпоративной/локальной информационной системе»
Подпроцесс:
«Организация межсетевого взаимодействия (кроссертификация)»
«Предоставление канала связи до информационной системы»
«Создание связей и отправка обновления справочников и ключей»

2. Термины, определения и сокращения

Термин	Определение
Деловая почта	Защищенная электронная почта «Деловая почта» комплекса «ViPNet-Гринатом»
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,

Термин	Определение
	индивидуальные предприниматели и физические лица
Администратор сети ViPNet	Работник ОКЗ, осуществляющий предоставление услуги Организация и обслуживание защищённой сети комплекса «ViPNet-Гринатом», администрирование сети
ViPNet Coordinator (Координатор)	Универсальный сервер защищённой сети ViPNet
Кроссертификация	Организация межсетевого взаимодействия с обменом ключевой информацией и справочниками

Сокращение	Расшифровка
АБ	Администратор безопасности ОКЗ
ОКЗ	Орган криптографической защиты
Пользователь	Работник организации-обладателя конфиденциальной информации, эксплуатирующий абонентский пункт в сети «ViPNet-Гринатом»
Руководитель ООКИ	Руководитель организации-обладателя конфиденциальной информации
СКЗИ	Средство криптографической защиты информации
ЦУС	Центр управления сетью «ViPNet-Гринатом»
СУ ИТ	Система управления информационными технологиями АО «Гринатом»
ПАК	Программно-аппаратный комплекс
АП	Абонентский пункт сети «ViPNet-Гринатом»

3. Описание процесса «Подключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»

3.1. Цель процесса

Предоставление услуг по подключению и обслуживанию Деловой почты.

3.2. Задачи процесса

- Подключение/отключение АП и обслуживание Деловой почты;
- Создание связей пользователю и отправка обновления адресной книги;
- Обеспечение функционирования Деловой почты;
- Вывод из эксплуатации Деловой почты.

3.3. Участники процесса и их роли

№ п.п.	Участники	Основные роли
1	Руководитель ООКИ	• Принимает решение о необходимости подключения/отключения и обслуживания Деловой почты; • Согласовывает документы, необходимые для подключения/отключения и обслуживания Деловой почты комплекса «ViPNet-Гринатом».
2	Администратор сети ViPNet	• Создание связей пользователю; • Обновление адресных книг пользователей; • Консультация АБ и пользователей по вопросам работы Деловой почты.

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 подключение/отключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»	АО «Гринатом»	Организация
2	Таблица связей в «Деловой почте» ViPNet-Гринатом - в случае, если	АО «Гринатом»	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация, / Дивизион/ Организация)
	организация вне периметра атомной отрасли		
3	Обновление адресной книги	Предприятие	Организация

3.5. Основные входы процесса

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
1	Единые отраслевые методические указания по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях	ГК «Росатом»	Корпорация
2	Заявление на подключение/отключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»	Предприятие	Организация
3	Таблица связей в «Деловой почте» ViPNet-Гринатом - в случае, если организация вне периметра атомной отрасли	Предприятие	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
4	Инцидент в СУ ИТ	Предприятие	Организация

3.6. Описание подпроцессов

3.6.1. Подпроцесс «Подключение/отключение абонентских пунктов, обслуживание Деловой почты»

На рабочем месте, где будет установлена защищенная электронная почта «Деловая почта» комплекса «ViPNet-Гринатом», предварительно, должно быть установлено СКЗИ «ViPNet Client».

Руководитель ООКИ:

– Принимает решение о необходимости подключения/отключения и обслуживания Деловой почты в соответствии с Едиными отраслевыми методическими указаниями по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях

– Направляет в адрес ОКЗ АО «Гринатом»

– Заявление на подключение и обслуживание абонентского пункта комплекса «ViPNet-Гринатом» (далее – Заявление на подключение/отключение услуги, Приложение №3);

– Направляет по защищенной электронной почте «Деловая почта» комплекса «ViPNet-Гринатом» на абонентский пункт «Главный администратор сети 11296» или на электронный адрес ViPNet@greenatom.ru письмо с просьбой добавить связи в адресный справочник (Таблица связей в «Деловой почте» ViPNet-Гринатом, Приложение №4) – в случае, если организация вне периметра атомной отрасли.

Исходящая информация поступает в подпроцесс «Создание связей новому пользователю в ЦУС» или в подпроцесс «Вывод из эксплуатации Деловой почты».

3.6.2. Подпроцесс «Создание связей новому пользователю и отправка обновления адресной книги»

Входящая информация поступает из подпроцесса «Подключение/отключение и обслуживание Деловой почты».

Администратор сети ViPNet:

- В случае, если организация находится вне периметра атомной отрасли, запрашивает согласованную таблицу связей в «Деловой почте» ViPNet-Гринатом (Приложение №4) с отделом информационной безопасности департамента защиты государственной тайны и информации Госкорпорации «Росатом» (далее – ДЗГТИ) и куратором отраслевой организации от Госкорпорации «Росатом»*.
- Создаёт абонентский пункт в сети «ViPNet-Гринатом» в соответствии с правилом наименования: «Организация Город ФИО (подразделение)»** или добавляет пользователя в уже существующий АП в соответствии с Заявлением.
- Добавляет в ЦУС связи новому пользователю в соответствии с полученным Заявлением на подключение/отключение услуги и таблицей связей (если применимо, в случае успешного согласования отделом информационной безопасности ДЗГТИ Госкорпорации «Росатом»);
- Отправляет обновление справочника связей по ViPNet. Централизованная рассылка справочников и ключей производится раз в сутки до 12:00 по МСК.

* Организация внутри периметра атомной отрасли направляет запрос в адрес управления информационной безопасности АО «Гринатом», загрузив «Таблицу связей» и документ, на основании которого планируется осуществлять взаимодействие посредством ViPNet, в единую отраслевую систему документооборота (далее – ЕОСДО), добавив в первую очередь согласования куратора от Госкорпорации «Росатом» и представителя Департамента защиты государственной тайны и информации во вторую В случае отсутствия ЕОСДО у организации отрасли, необходимо пройти аналогичные шаги по согласованию официальными запросами на имя куратора от Госкорпорации «Росатом», затем на имя представителя Департамента защиты государственной тайны и информации Госкорпорации «Росатом» с приложением согласования от куратора любым удобным способом (например, письмо почтой, с помощью «Деловой почты» ViPNet и т.д.). После направить запрос на добавление связей в адрес управления информационной безопасности АО «Гринатом», приложив необходимые согласования. Запросить ФИО и должность адресатов можно по электронной почте: ViPNet@Greenatom.ru.

** В случае, если требуется создать обезличенный АП «Канцелярия», являющийся общим входом электронных писем в адрес Организации в сети ViPNet, требуется наличие приказа «О назначении ответственного и замещающих лиц по работе с абонентским пунктом ViPNet «Канцелярия», Приложение № 5. Каждому лицу, указанному в Приказе, требуется получить сертификат ключа проверки электронной подписи (далее - СКП ЭП) в соответствии с Регламентом процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации

«Росатом»» и подписывать исходящие письма в сети «ViPNet-Гринатом» с использованием личной СКП ЭП.

Исходящая информация поступает в подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ» или в конец процесса.

3.6.3. Подпроцесс «Обеспечение функционирования Деловой почты»

В случае, если возникли проблемы с работоспособностью Деловой почты:

- Консультирует АБ или пользователя по телефону и электронной почте по вопросам работы Деловой почты на основании полученного инцидента в SM;

В случае, если необходимо вывести Деловую почту из эксплуатации, исходящая информация поступает в подпроцесс «Подключение/отключение и обслуживание Деловой почты».

3.6.4 Подпроцесс «Формирование комплекта поставки и учёт СКЗИ»

Порядок описан в Порядке организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

3.6.5. Подпроцесс «Вывод из эксплуатации Деловой почты»

Входящая информация поступает из подпроцесса «Подключение/отключение и обслуживание Деловой почты».

Администратор сети ViPNet:

- Удаляет в ЦУС пользователя сети;
- Обновляет справочник связей.

Исходящая информация поступает в конец процесса (процесс завершается).

4. Описание процесса «Подключение/отключение и обслуживание ViPNet Coordinator в сети комплекса «ViPNet-Гринатом»

Обязательным условием подключения и обслуживания ПАК ViPNet Coordinator Заказчика является наличие действующего договора на техническую поддержку не ниже уровня поддержки программного обеспечения и программно-аппаратной части сети «ViPNet-Гринатом».

Требуется:

- официальный запрос на имя начальника управления информационной безопасности АО «Гринатом» с обоснованием необходимости добавления оборудования в состав сети «ViPNet Гринатом», предоставлением технического решения на сетевую инфраструктуру с использованием ViPNet Coordinator,
- согласование начальника управления информационной безопасности АО «Гринатом».

Администратор сети ViPNet осуществляет:

1. Разовые работы:
   - Добавление координатора в ЦУС, автоматически создаётся одноимённый пользователь;
   - Настройку сетевого взаимодействия координатора в сети ViPNet;
   - Настройку сетевых параметров координатора во внешней сети (если известны) и настройку межсетевого экрана (режимов работы) координатора;
   - Добавление связей с другими узлами сети ViPNet и, если необходимо, добавление клиентов за этот координатор;
   - Формирование справочников и ключевой информации для координатора в удостоверяющем ключевом центре и выпуск дистрибутива ключей для разворачивания на координаторе;
   - Установку дистрибутива ключей на координаторе и первичную настройку координатора (если координатор физически доступен);
   - Формирование, генерация и рассылка справочников и ключевой информации на всю сеть ViPNet;
   - Настройку координатора для отслеживания состояния через систему мониторинга (если применимо).
2. Поддержка работоспособности в сети:
   - Актуализацию сетевых параметров координатора во внешней сети и сетевого взаимодействия координатора в сети ViPNet;
   - Формирование, генерация и рассылка обновлённых справочников и ключевой информации для координатора;
   - Добавление связей с другими узлами сети ViPNet;
   - Настройку сетевых фильтров координатора.

5. Описание процесса «Предоставление доступа к корпоративной/локальной информационной системе»

5.1 Подпроцесс «Организация межсетевого взаимодействия (кроссертификация)»

Реализуется в случае, если необходимо создать связи пользователю с абонентами внешних сетей, предоставить шифрованный доступ к ресурсам доверенной сети.

Требуется:

- Заявление на установление межсетевого взаимодействия, Приложение №6 к Порядку;
- Подписанное «Соглашение об установлении межсетевого взаимодействия», Приложение № 7 к Порядку.

5.2 Подпроцесс «Предоставление шифрованного канала связи до корпоративной/локальной информационной системы»

Реализуется в случае, если необходимо предоставить шифрованный доступ к ресурсу/информационной системе доверенной сети или ресурсу/информационной системе в сети «ViPNet-Гринатом» при наличии возможности такого подключения в техническом решении на отдельно взятый ресурс/информационную систему;

- Согласование межсетевого взаимодействия со смежными управлениями и владельцами ресурсов;
- Добавление связей с туннелирующим координатором;
- Добавление необходимых связей узлам;
- Взаимодействие с владельцем предоставляемых (туннелируемых) посредствам сети «ViPNet-Гринатом» ресурсов/информационных систем;
- Настройка сетевых параметров координатора во внешней сети и сетевого взаимодействия координатора в сети ViPNet;
- Формирование, генерация и рассылка обновлённых справочников и ключевой информации для координатора.

5.3 Подпроцесс «Создание связей и отправка обновления справочников и ключей»

Входящая информация поступает из процесса «Предоставление доступа к сетевому информационному ресурсу организации».

Администратор сети ViPNet:

- Добавляет в ЦУС связи пользователю;
- Отправляет обновление справочника связей по ViPNet;
- Направляет информацию по проведению локальных настроек на АП пользователя.

Централизованная рассылка справочников и ключей производится раз в сутки до 12:00 по МСК.

6. 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.№15686 Н 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);
- Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» (с пометкой «Для служебного пользования»);
- 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).

7. Порядок внесения изменений

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

8. Контроль и ответственность

8.1 Порядок обязаны соблюдать все следующие участники процесса:

- Руководитель ООКИ;
- Администратор сети ViPNet;
- Администратор ОКЗ;
- Пользователь АП.

8.2. Ответственность работников за несоблюдение требований Порядка.

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

9. Перечень приложений

Приложение №1.	Матрица ответственности.
Приложение №2.	Схема процесса
Приложение №3.	Заявление на подключение/отключение услуги
Приложение №4.	Таблица связей в «Деловой почте» ViPNet-Гринатом
Приложение №5.	Приказ о назначении ответственного и замещающих лиц по работе с абонентским пунктом ViPNet «Канцелярия»
Приложение №6.	Соглашение об установлении межсетевого взаимодействия
Приложение №7.	Заявление на установление межсетевого взаимодействия
Приложение №8.	Заявление на предоставление канала связи до локальных ресурсов

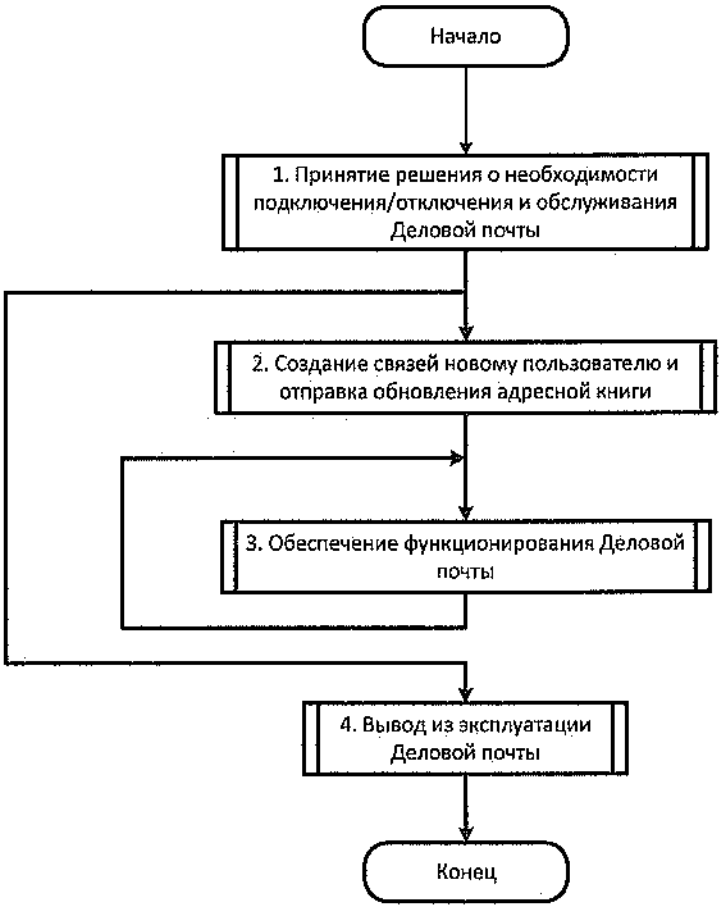
Приложение №1. Матрица ответственности

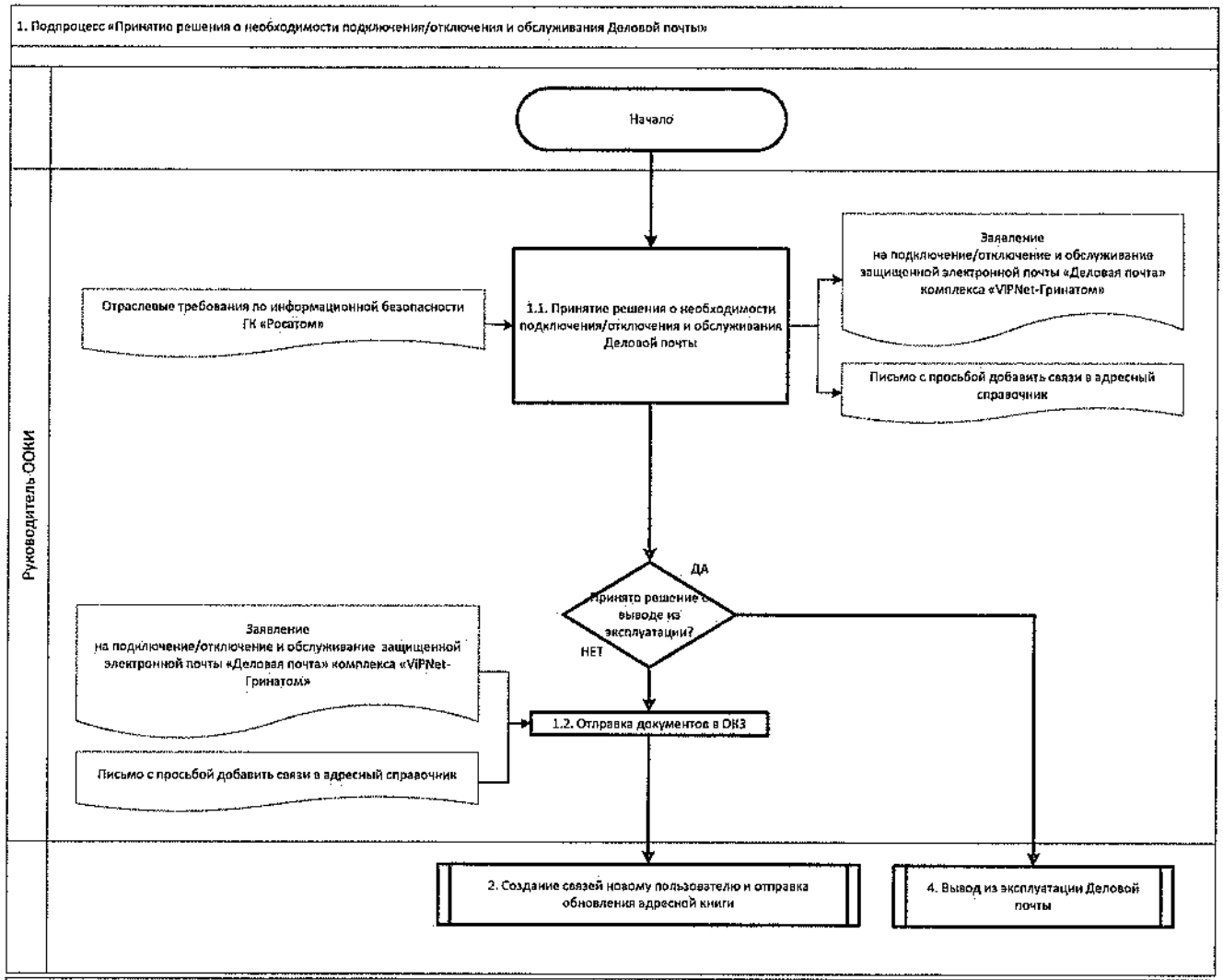
Подпроцессы в составе процесса	Участники процесса	
	Руководитель ООКИ	Администратор сети ViPNet
Подпроцесс «Подключение/отключение и обслуживание Деловой почты»	Утв	Инф
Подпроцесс «Создание связей новому пользователю и отправка обновления адресной книги»	Инф	О
Подпроцесс «Обеспечение функционирования Деловой почты»	Инф	О
Подпроцесс «Вывод из эксплуатации Деловой почты»	Утв	О

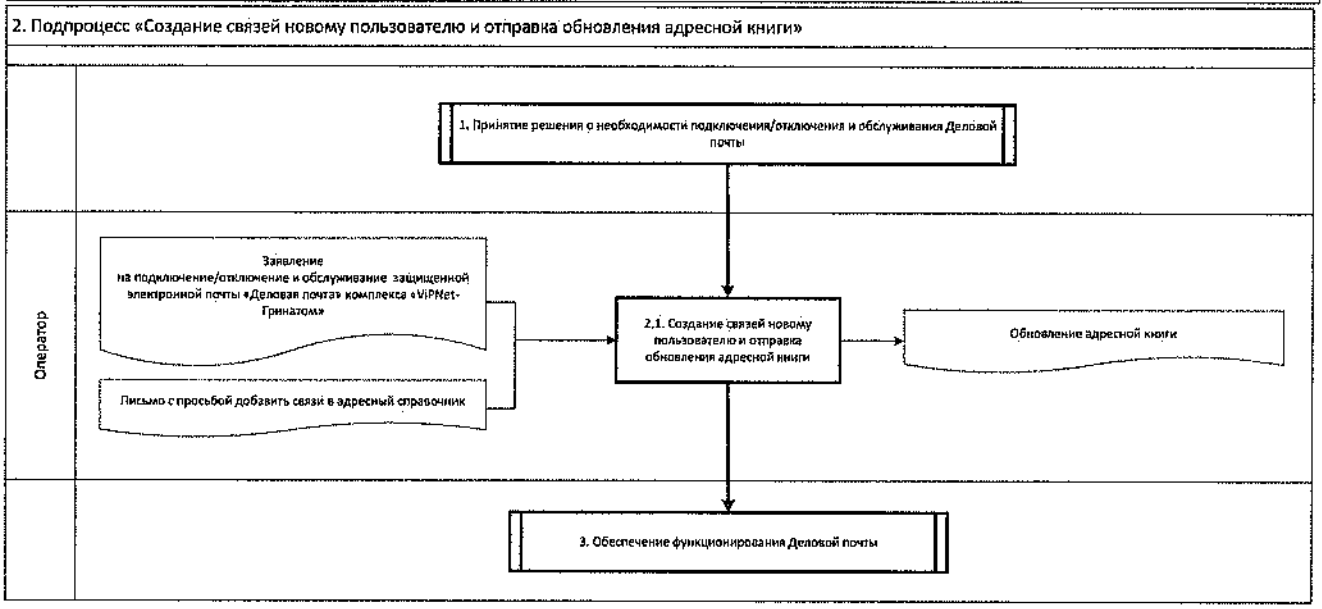
Сокращение	Название роли	Определение	Исполнитель Роли
О	Ответственный	Несет ответственность за достижение результата по подпроцессу/процедуре в своей предметной области	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
Утв	Утверждающий	Утверждает - принимает окончательное решение по результату подпроцессу/процедуре	Коллегиальные органы (Наблюдательный совет, Правление и прочие) Генеральный директор Корпорации, Руководители Корпорации /Дивизионов/Организаций
Инф	Информируемый	Получает информацию о ходе/результате подпроцесса /процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации Коллегиальные органы

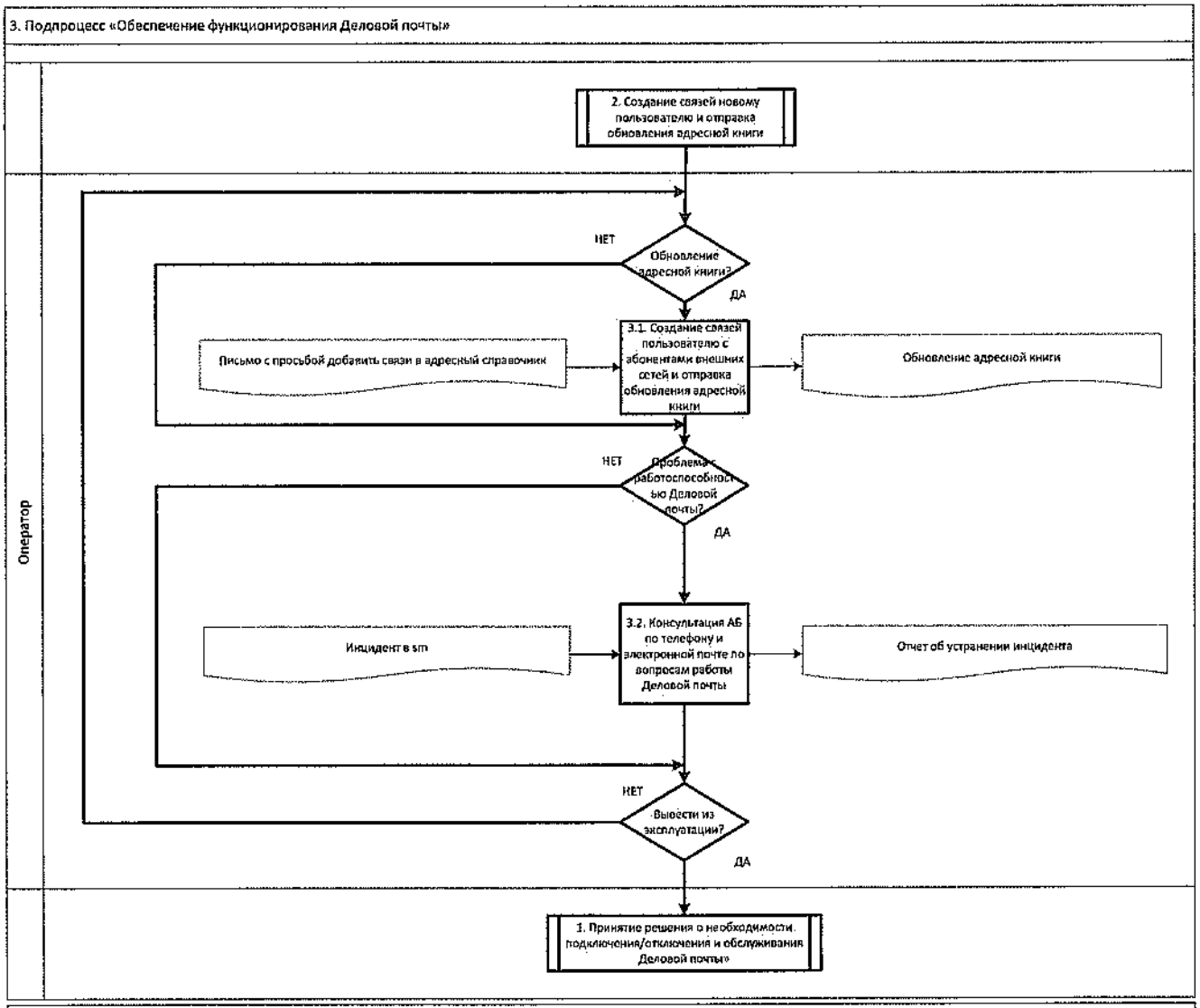
Приложение №2. Схема процесса

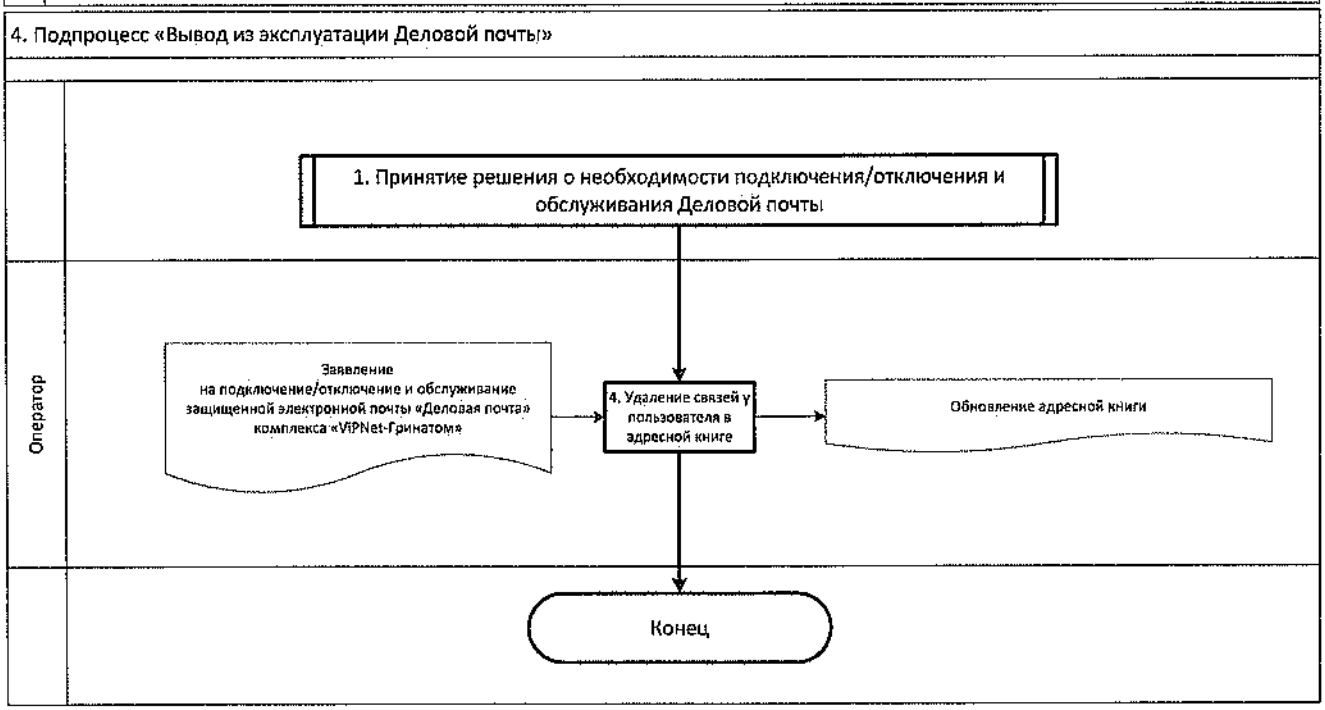
Процесс «Подключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «VipNet-Гринатом»




1. Подпроцесс «Принятие решения о необходимости подключения/отключения и обслуживания Деловой почты»
Руководитель ООКИ
Начало
Отраслевые требования по информационной безопасности ГК «Росатом»
1.1. Принятие решения о необходимости подключения/отключения и обслуживания Деловой почты
Заявление на подключение/отключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»
Письмо с просьбой добавить связи в адресный справочник
ДА
Принято решение о выводе из эксплуатации?
НЕТ
Заявление на подключение/отключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»
Письмо с просьбой добавить связи в адресный справочник
1.2. Отправка документов в ОКЗ
2. Создание связей новому пользователю и отправка обновления адресной книги
4. Вывод из эксплуатации Деловой почты


2. Подпроцесс «Создание связей новому пользователю и отправка обновления адресной книги»
1. Принятие решения о необходимости подключения/отключения и обслуживания Деловой почты
Оператор
Заявление на подключение/отключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»
Письмо с просьбой добавить связи в адресный справочник
2.1. Создание связей новому пользователю и отправка обновления адресной книги
Обновление адресной книги
3. Обеспечение функционирования Деловой почты


3. Подпроцесс «Обеспечение функционирования Деловой почты»
Оператор
2. Создание связей новому пользователю и отправка обновления адресной книги
НЕТ
Обновление адресной книги?
ДА
Письмо с просьбой добавить связи в адресный справочник
3.1. Создание связей пользователю с абонентами внешних сетей и отправка обновления адресной книги
Обновление адресной книги
НЕТ
Проблемы с работоспособностью Деловой почты?
ДА
Инцидент в sm
3.2. Консультация АБ по телефону и электронной почте по вопросам работы Деловой почты
Отчет об устранении инцидента
НЕТ
Вывести из эксплуатации?
ДА
1. Принятие решения о необходимости подключения/отключения и обслуживания Деловой почты»


4. Подпроцесс «Вывод из эксплуатации Деловой почты»
Оператор
1. Принятие решения о необходимости подключения/отключения и обслуживания Деловой почты
Заявление
на подключение/отключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»
4. Удаление связей у пользователя в адресной книге
Обновление адресной книги
Конец

Приложение №3. Заявление на подключение/отключение услуги

Заявление
на подключение и обслуживание абонентского пункта комплекса «ViPNet-Гринатом»

« _____ » _____ 20 ____ г.

_____
(наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____

просит Орган криптографической защиты АО «Гринатом» предоставить услугу по

(нужное выбрать):

☐ подключению и обслуживанию абонентского пункта комплекса «ViPNet-Гринатом»;

☐ отключению от обслуживания абонентского пункта комплекса «ViPNet-Гринатом»;

☐ подключению доступа к корпоративным и локальным информационным системам (ИС);

☐ отключению доступа к корпоративным и локальным информационным системам (ИС).

№ п/п	Пользователь СКЗИ (Ф.И.О. полностью)	Учетный номер АРМ, на котором установлено СКЗИ	Подразделение (отдел)	Адрес месторасположения АРМ	Операционная система, установленная на АРМ	Подключение АП (через интернет или КСПД)	Наименование ИС
1							
2							

Администратор безопасности _____ _____
(должность) (подпись) (ФИО)

Уполномоченное должностное лицо _____ _____
(должность) (подпись) (ФИО)

м.п.

Приложение №4. Таблица связей в «Деловой почте» ViPNet-Гринатом

Таблица связей в «Деловой почте» ViPNet-Гринатом для организаций вне периметра.

Наименование абонентского пункта пользователя для добавления связей	**Наименование абонентского пункта, которое нужно добавить/ФИО, отдел, организация пользователя**

Основания для взаимодействия (договор, соглашение): _____

_____	_____	_____
(должность уполномоченного лица организации)	(подпись)	(фамилия, инициалы)
_____	_____	_____
(должность уполномоченного лица ДЗГТИ)	(подпись)	(фамилия, инициалы)

Приложение №5. Приказ о назначении ответственного и замещающих лиц по работе с абонентским пунктом ViPNet «Канцелярия»

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

ПРИКАЗ

«____» _____ 20___ г. № _____

(дата)

О назначении ответственного и замещающих лиц по работе с абонентским пунктом ViPNet «Канцелярия»

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

ПРИКАЗЫВАЮ:

1. Назначить «ФИО, структурное подразделение, должность» ответственным за эксплуатацию абонентского пункта (далее - АП) «Канцелярия» в сети «ViPNet-Гринатом».
2. К работе с АП «Канцелярия» допустить следующих работников:

№	ФИО пользователя	Структурное подразделение	Должность
1			
2			

3. Контроль исполнения настоящего Приказа оставляю за собой.

_____ _____ _____

(должность руководителя) (подпись руководителя) (Ф.И.О. руководителя)

Приложение №6. Заявление на установление межсетевого взаимодействия

Заявление на установление межсетевого взаимодействия

_____
(наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании: _____

просит Орган криптографической защиты АО «Гринатом» рассмотреть возможность организовать межсетевое взаимодействие, присвоить статус «доверенная» с сетью <Номер сети, Наименование ИС, Организация-владелец> в связи с необходимостью:

_____

_____

_____

_____

_____

_____

Контакты для взаимодействия:

Контактное лицо в сети «ViPNet-Гринатом» (ФИО, эл. почта, тел.) – инициатор запроса	
Номер и наименование сети, с которой требуется установить взаимодействие	
Администратор сети, с которой требуется установить взаимодействие (ФИО, эл. почта, тел.)	

_____ _____ _____
(Должность уполномоченного должностного лица) (подпись) (ФИО)

М.П.

Приложение №7. Соглашение об установлении межсетевого взаимодействия

СОГЛАШЕНИЕ №_
об установлении межсетевого взаимодействия

г. Москва «___» _____ 20___ г.

Акционерное общество «Гринатом», в лице_____,
действующего на основании Доверенности №_____,
именуемое в дальнейшем АО «Гринатом», с одной стороны и
_____
с другой стороны, совместно именуемые «Стороны», заключили настоящее Соглашение о нижеследующем.

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. Стороны договорились об установлении межсетевого взаимодействия между своими ViPNet-сетями и установлении доверия между абонентами ViPNet-сети № 11296 (АО «Гринатом») и ViPNet-сети №_____. Межсетевое взаимодействие между ViPNet-сетями должно обеспечивать защищенный электронный документооборот между разрешенными абонентами ViPNet-сетей Сторон.

1.2. Отношения между Сторонами регулируются Гражданским кодексом Российской Федерации, Федеральным законом от 27.08.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».

1.3 Права Организации на оказание услуг по передаче средств криптографической защиты информации подтверждаются копией лицензии ЛСЗ № 0014254 Рег..№ 15686 Н от 19.01.2017 Центра по лицензированию, сертификации и защите государственной тайны ФСБ России, на осуществление 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).

1.4. Организация предоставляет заключение о корректности встраивания средств СКЗИ в программные средства собственной разработки.

2. ОПЛАТА СОГЛАШЕНИЯ

2.1. Соглашение является безвозмездным.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. При организации информационного обмена АО «Гринатом» и_____ принимает на себя следующие права и обязанности.

3.1.1. Обеспечивает поддержание в работоспособном состоянии аппаратных и программных средств ViPNet-сетей и телекоммуникационных средств в границах своей зоны ответственности (Приложение 1 к настоящему Соглашению).

3.1.2. Обеспечивает установку взаимосвязи с абонентами ViPNet сетей, согласно разделу 4 настоящего Соглашения.

3.2 При организации информационного обмена с ViPNet сетями принимает на себя следующие права и обязанности.

3.2.1. Обеспечивает поддержание в работоспособном состоянии аппаратных и программных средств ViPNet-сетей и телекоммуникационных средств в границах своей зоны ответственности (Приложение 1 к настоящему Соглашению).

3.2.2. Обеспечивает установку и сопровождение средств криптографической защиты информации абонентам ViPNet-сетей, согласно разделу 4 настоящего Соглашения.

3.3. Установка взаимосвязи с абонентами ViPNet сетей производится по взаимному согласию Сторон.

4. ОРГАНИЗАЦИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

4.1. Ответственными лицами Сторон для организации межсетевого взаимодействия назначаются Администраторы ViPNet-сетей Сторон.

4.2. Организация межсетевого взаимодействия (установление доверенных отношений) между ViPNet-сетями Сторон осуществляется в соответствии с технической документацией на программное обеспечение (ПО) ViPNet-Администратор.

4.3. По завершении процедуры организации межсетевого взаимодействия (установления доверенных отношений) между ViPNet-сетями Сторон, подписывается Протокол установления межсетевого взаимодействия (Приложение 2 к настоящему Соглашению).

4.4. Для установления взаимодействия между сетевыми узлами пользователей ViPNet-сетей Сторон, Стороны согласовывают списки таких сетевых узлов, и устанавливают данное взаимодействие в рабочем порядке, руководствуясь технической документацией на ПО ViPNet-Администратор.

5. ХАРАКТЕРИСТИКИ ТЕЛЕКОММУНИКАЦИОННЫХ СРЕДСТВ

5.1. Характеристики телекоммуникационных средств и границы зоны ответственности АО «Гринатом» и _____ определяются в Приложении 1 к настоящему Соглашению, являющимся его неотъемлемой частью.

6. ПРОВЕДЕНИЕ ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ

6.1. Стороны обязаны заблаговременно, не позднее, чем за 5 (пять) рабочих дней до дня проведения профилактических мероприятий оповещать друг друга о сроках проведения профилактических мероприятий, нарушающих работоспособность телекоммуникационных средств и средств ViPNet, участвующих в межсетевом взаимодействии ViPNet-сетей Сторон.

7. ГРАНИЦЫ ЗОНЫ ОТВЕТСТВЕННОСТИ СТОРОН

7.1. Стороны несут ответственность за нарушение конфиденциальности информации ограниченного доступа в соответствии с законодательством Российской Федерации и настоящим Соглашением.

7.2. Стороны не несут ответственность за содержание информации, передаваемой абонентами друг другу.

7.3. Стороны несут ответственность в соответствии с законодательством Российской Федерации перед Абонентами, которые имеют договорные отношения со Сторонами

7.4. Стороны несут ответственность за работоспособность телекоммуникационного оборудования и выполнения требований законодательства РФ, а также условий настоящего Соглашения, в своей зоне ответственности за:

7.4.1 Работоспособность транспортного сервера Организации.

7.4.2. Техническую поддержку абонентов.

7.4.3. Администрирование внутренних сетевых ресурсов.

8. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ

8.1. Разбор конфликтных ситуаций осуществляется в два этапа. На первом этапе Сторона, у которой возникли претензии, взаимодействует с Администратором безопасности другой стороны. На втором этапе, в случае отсутствия взаимного соглашения, для разрешения конфликтной ситуации проводится техническая экспертиза экспертной комиссией.

8.2. Экспертная комиссия созывается на основании письменного заявления (претензии) одной из Сторон.

8.3. Не позднее 10 (десяти) рабочих дней с момента получения претензии назначается дата, место и время начала работы комиссии, о чем письменно уведомляются обе Стороны. Состав экспертной комиссии формируется в равных пропорциях из представителей Сторон. В состав комиссии также могут включаться эксперты – представители организаций-разработчиков средств СКЗИ.

8.4. Акты, составленные экспертной комиссией, с приложенными распечатками материалов, предоставленных на экспертизу, могут направляться для дальнейшего рассмотрения споров в арбитражном суде.

9. СРОКИ ДЕЙСТВИЯ СОГЛАШЕНИЯ

9.1. Настоящее Соглашение вступает в силу с момента его подписания и действует в течение одного года с момента подписания.

9.2. Действие настоящего Соглашения автоматически продлевается на каждый последующий календарный год, если ни одна из сторон не заявит о его прекращении не позднее, чем за месяц до истечения строка действия настоящего Соглашения.

9.3. Настоящее Соглашение может быть досрочно расторгнуто по обоюдному согласию сторон, либо в одностороннем порядке с предупреждением другой стороны за два месяца до расторжения Соглашения.

10. ФОРС – МАЖОР

10.1. При возникновении обстоятельств, которые делают полностью или частично невозможным выполнение настоящего Соглашения одной из сторон, таких как стихийные бедствия, военные действия и другие обстоятельства непреодолимой силы, не зависящие от сторон, сроки исполнения обязательств продлеваются на время, в течение которого действуют эти обстоятельства.

10.2. Сторона, подвергшаяся действию форс-мажорных обстоятельств, обязуется уведомить письменно другую сторону в течение 3 (трех) рабочих дней с предоставлением документов компетентных органов, подтверждающих наличие данных обстоятельств.

10.3. Если обстоятельства непреодолимой силы действуют более одного месяца, Соглашение может быть досрочно расторгнуто в одностороннем порядке, путем заключения дополнительного соглашения.

11. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

11.1. В случае возникновения споров и разногласий Стороны прилагают все усилия, чтобы устранить их путём переговоров.

11.2. При возникновении обстоятельств, которые не позволяют обеспечить информационный обмен данными между абонентами ViPNet-сетей Сторон по телекоммуникационным каналам связи, АО «Гринатом» и _____ прилагают совместные усилия по устранению этих обстоятельств.

11.3. Любые изменения и дополнения к Соглашению действительны, если они совершены в письменной форме и подписаны надлежащим образом уполномоченными на то представителями Сторон.

11.4. Соглашение составлено в 2-х (двух) экземплярах, имеющих одинаковую юридическую силу – по одному для каждой из Сторон.

11.5. Нижеуказанные Приложения являются неотъемлемой частью настоящего Соглашения.

11.6 Переговорный порядок урегулирования споров и разногласий не исключает права каждой из Сторон на обращение в Арбитражный суд.

Приложение 1. Характеристики телекоммуникационных средств и границы зоны ответственности сторон.

Приложение 2. Протокол установления межсетевого взаимодействия между сетями.

12. АДРЕСА И РЕКВИЗИТЫ СТОРОН:

Полное наименование: Акционерное общество «Гринатом» Краткое наименование: АО «Гринатом» Место нахождения: 119017, Россия, Москва, ул. Большая Ордынка, д. 24 Почтовый адрес: 115230, г. Москва, 1-й Нагатинский проезд, д.10, строение 1 ОГРН: 1097746819720 ИНН: 7706729736 Телефон: +7 (499) 949-49-19	Полное наименование: Краткое наименование: Место нахождения: Почтовый адрес: ОГРН: ИНН: Телефон:
ФИО Ответственного ДЛ	
_____ М.П.	_____ М.П.

Приложение № 1
к Соглашению об установлении
межсетевого взаимодействия

Характеристики телекоммуникационных средств и границы зоны ответственности сторон

1. Характеристики телекоммуникационных средств

1.1. Состав телекоммуникационных средств АО «Гринатом».

ViPNet-Администратор – центр управления сетью и ключевой центр ViPNet-сети АО «Гринатом» (сеть № 11296);

Корпоративная сеть АО «Гринатом» - телекоммуникационное оборудование, подключенное к выделенной линии связи, межсетевой экран и абонентские пункты.

Шлюзовой ViPNet-Координатор – сетевой узел, через который проходит весь межсетевой обмен со стороны АО «Гринатом» (сеть № 11296).

Сетевые узлы – ViPNet-Клиенты пользователей ViPNet-сети АО «Гринатом» (сеть № 11296).

2. Характеристики телекоммуникационных средств _____

2.1. Состав телекоммуникационных средств _____.

ViPNet-Администратор –_____;

Корпоративная сеть _____.

Шлюзовой ViPNet-Координатор – _____

Сетевые узлы – ViPNet-Клиенты пользователей от _____

4. Границы зоны ответственности Сторон

4.1. АО «Гринатом» несет ответственность за работоспособность своего шлюзового ViPNet-Координатора, сетевого и телекоммуникационного оборудования своей сети.

4.2. _____ несет ответственность за работоспособность своего шлюзового ViPNet-Координатора, сетевого и телекоммуникационного оборудования своей сети.

4.3. Стороны несут ответственность за контроль передачи данных через своего провайдера.

4.4. Стороны не несут ответственность за прекращение передачи данных, вызванных по вине провайдера.

5. Ответственность Сторон

5.1. Ответственность АО «Гринатом».

В случае нарушения работоспособности телекоммуникационных средств, при представлении электронных документов по телекоммуникационным каналам связи в границах зоны ответственности, АО «Гринатом» несет ответственность в соответствии с законодательством Российской Федерации перед _____.

5.2. Ответственность _____

В случае нарушения работоспособности телекоммуникационных средств, при представлении электронных документов по телекоммуникационным каналам связи в границах зоны ответственности, _____ несет ответственность в соответствии с законодательством Российской Федерации перед АО «Гринатом».

АО «Гринатом»
ФИО Ответственного ДЛ

_____ _____

М.П. М.П.

Приложение № 2
к Соглашению об установлении
межсетевого взаимодействия

ПРОТОКОЛ
установления межсетевого взаимодействия между сетями

"___" _____ 201_ г.

Межсетевое взаимодействие устанавливается между сетями:

Номер ViPNet сети	Наименование предприятия
№ 11296	АО «Гринатом» - Акционерное общество «Гринатом»

Процедуру установления межсетевого взаимодействия осуществляли:

Номер ViPNet сети	Наименование предприятия	ФИО	Контактные данные
№ 11296	АО «Гринатом» - Акционерное общество «Гринатом»		Тел. 8 499 949 49 19 п/я vipnet@greenatom.ru

1. Целью установления межсетевого взаимодействия является защищенное информационное взаимодействие сетевых узлов ViPNet сетей АО «Гринатом» и _____

2. Передача начального и ответного экспорта между сетями № 11296 и № _____ была осуществлена доверенным способом.

3. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети _____.

4. Для установления межсетевого взаимодействия, в качестве шлюзовых ViPNet-Координатором были назначены:
- в сети № 11296 АО «Гринатом» - core-s-vpncoord__
-в сети № _____

5. При установлении доверительных отношений на уровне Удостоверяющих центров ViPNet-сетей Сторон, в рамках организации межсетевого взаимодействия были произведены импорты корневых сертификатов и Списков аннулированных сертификатов ViPNet-сетей Сторон.

6. Смена межсетевых ключей, изменение состава сетевых узлов, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем Администраторы ViPNet-сетей Сторон уведомляют друг друга с помощью ПО ViPNet-Клиент (Деловая почта) с указанием производимых изменений.

7. Стороны обязуются производить изменения в настройках и структуре ViPNet-сетей, которые могут привести к нарушению межсетевого взаимодействия, только после предварительного согласования.

Администратор ViPNet-сети
АО «Гринатом» (№ 11296)

_____/_____

Администратор ViPNet-сети

_____/_____

Приложение №8. Заявление на предоставление канала связи до локальных ресурсов

Заявление на предоставление канала связи до локальных ресурсов

_____
(наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании: _____

просит Орган криптографической защиты АО «Гринатом» рассмотреть возможность предоставления шифрованного канала связи к ресурсам «сети ViPNet-Гринатом» в связи с необходимостью:

_____

_____

_____

_____

_____

_____

Контакты для взаимодействия:

Контактное лицо (ФИО, эл. почта, тел.) - инициатор запроса	
Наименование информационной системы, к которой требуется предоставить доступ	
Администратор информационной системы, к которой требуется предоставить доступ	

_____ _____ _____
(Должность уполномоченного должностного лица) (подпись) (ФИО)

М.П.

Приложение № 8 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю

Директор по информационным технологиям

АО «Гринатом»

_____/ А.Н. Киселёв /

М.П.

ПОРЯДОК

предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с использованием информационной системы Органа криптографической защиты»

Москва 2020 г.

Содержание

Назначение и область применения

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

Общая информация о КУЦ:

Официальный сайт: https://crypto.rosatom.ru

Официальный E-mail: ca@rosatom.ru

Телефон: +7 (499) 949-49-19 доб. 54-54

Адрес нахождения: г. Москва, 1-й Нагатинский проезд, дом 10, стр. 1

Официальный адрес ИС ОКЗ: https://crypto.rosatom.local

Адрес публикации списков отозванных сертификатов:

http://crl1.rosatom.ru/ra/cdp/

http://crl2.rosatom.ru/ra/cdp/

http://crl1.rosatom.local/ra/cdp/

http://crl2.rosatom.local/ra/cdp/

Адрес публикации служб OCSP:

http://ocsp1.rosatom.ru/ocsp4/ocsp.srf

http://ocsp2.rosatom.ru/ocsp4/ocsp.srf

http://ocsp1.rosatom.local/ocsp4/ocsp.srf

http://ocsp2.rosatom.local/ocsp4/ocsp.srf

Адрес публикации служб TSP:

http://tsp1.rosatom.ru/tsp3/tsp.srf

http://tsp2.rosatom.ru/tsp3/tsp.srf

http://tsp1.rosatom.local/tsp3/tsp.srf

http://tsp2.rosatom.local/tsp3/tsp.srf

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

Руководитель предприятия/организации;

Пользователь КУЦ;

Администратор безопасности;

Сотрудник HR;

Оператор КУЦ;

Администратор КУЦ;

Порядок распространяется в форме электронного документа по адресу: URL= https://crypto.rosatom.ru/dokumentatsiya/reglamenty/reglament-kuts/

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

Документ	Статус	Тип документа
Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686 Н 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)	Действует	Лицензия
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
Свидетельство об аккредитации удостоверяющего центра №758 от 21 августа 2017 г.	Действует	Свидетельство

Термины, определения и сокращения

Термин	Определение
Администратор безопасности	уполномоченный работник АО «Гринатом» (по договору) или уполномоченный сотрудник предприятия-заказчика наделенный полномочиями по вручению сертификатов ключей проверки электронных подписей от имени удостоверяющего центра.
Аккредитация удостоверяющего центра	признание уполномоченным федеральным 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
Информационная система органа криптографической защиты	Информационная система, предназначенная для автоматизации деятельности по управлению электронными ключами пользователей и средствами криптографической защиты
Квалифицированный сертификат ключа проверки электронной подписи (УКЭП)	сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом №63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным центром сертификации
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
Ключевой носитель	Отчуждаемый носитель информации, предназначенный для хранения ключа электронной подписи и ключа проверки электронной подписи
Неквалифицированный сертификат ключа проверки электронной подписи (УНЭП)	сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом №63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, позволяющий формировать электронную подпись в соответствии со ст.5, часть 3 Федерального закона №63-ФЗ «Об электронной подписи»
Подписка	Заказ предприятия в ИС ОКЗ в соответствии с условиями договора присоединения на обеспечение сертификатами или средствами криптографической защиты и информации. Подписка подразумевает владение Пользователем КУЦ одним действующим сертификатом выбранного шаблона.
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;
Уполномоченное лицо	Работник юридического лица, указанный в ЕГРЮЛ и имеющий возможность обращаться в Удостоверяющий центр от имени юридического лица, либо работник имеющий право действовать от имени юридического лица на основании доверенности
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
ИАСУП	Информационная автоматизированная система управления персоналом Госкорпорации «Росатом»
ИС ОКЗ	Информационная система органа криптографической защиты
КУЦ	Корпоративный Удостоверяющий центр
Сертификат	Сертификат ключа проверки электронной подписи
СОС	Список отозванных сертификатов
УКЭП	Квалифицированный сертификат ключа проверки электронной подписи
УНЭП	Неквалифицированный сертификат ключа проверки электронной подписи
ЭД	Электронный документ
ЭП	Электронная подпись

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;
- установления сроков действия сертификатов;
- аннулирования 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.

3.3. Участники группы процессов и их роли

№	Участники	Основные роли
1	Пользователь КУЦ	• Обладает учётной записью в домене GK • Создаёт обращение • Получает сертификаты
2	Уполномоченное лицо предприятия	• Согласовывает и подписывает электронные заявки в ИС ОКЗ на создание и сокращение подписок предприятия;
3	Сотрудник HR	• Согласование создания подписки на обеспечение сертификатом в части кадровых данных пользователя КУЦ • Корректировка подписки на обеспечение сертификатом в части кадровых данных пользователя КУЦ

4	Администратор безопасности ОКЗ	• Обработка и формализация обращения • Создание подписки на обеспечение сертификатом • Корректировка подписки на обеспечение сертификатом; • Сокращение подписки на обеспечение сертификатом • Согласование Перевыпуска сертификата • Вручение сертификата УКЭП и УНЭП • Контроль действия сертификата
5	Оператор КУЦ	• Создание сертификата УКЭП • Создание сертификата УНЭП
6	Администратор КУЦ	• Аннулирование сертификата

3.4 Описание подпроцессов

3.4.1. Подпроцесс «Обработка обращения»

Администратор безопасности получает обращение от следующих возможных инициаторов:

Пользователь КУЦ;

АБ;

уполномоченное лицо предприятия;

контактное лицо;

одним из следующих способов:

заявка в ИС ОКЗ;

заявка через порталы АО «Гринатом» или «Страна Росатом»;

заявка через СУ ИТ;

электронное письмо на п/я 1111@greenatom.ru;

электронное письмо на п/я ca@rosatom.ru;

звонок в центр поддержки пользователей АО «Гринатом»;

Администратор безопасности определяет наличие подписки и учётной записи в домене GK у пользователей КУЦ, указанных в обращении;

Администратор безопасности формализует обращение в соответствии с правилами формализации, изложенными на официальном сайте КУЦ в зависимости от следующих условий:

В случае если подписка на пользователя КУЦ, указанного в обращении, отсутствует и обращение на создание подписки, то исходящая информация

поступает в подпроцесс «Создание подписки на обеспечение сертификатом» в соответствии с выбранным шаблоном.

Администратор безопасности должен определить шаблон для выпуска сертификата на основании неформализованного обращения Пользователя КУЦ.

В случае если подписка на обеспечение сертификатом на пользователя КУЦ, указанного в обращении, есть и обращение связано с изменением данных пользователя КУЦ, то исходящая информация поступает в подпроцесс «Корректировка подписки»

В случае если подписка на обеспечение сертификатом на пользователя КУЦ, указанного в обращении, есть и обращение на сокращение подписки, то исходящая информация поступает в подпроцесс «Сокращение подписки на обеспечение сертификатом» в соответствии с указанным в обращении сертификатом.

В случае если подписка на обеспечение сертификатом на пользователя КУЦ, указанного в обращении, есть и обращение связано с компрометацией или подозрением на компрометацию, то исходящая информация поступает в подпроцесс «Перевыпуск сертификата».

Если обращение содержит иные данные, процесс оканчивается.

Исходящая информация поступает в подпроцесс «Создание сертификата», либо в подпроцесс «Сокращение подписки на обеспечение сертификатом», либо в подпроцесс «Корректировка подписки», либо в подпроцесс «Перевыпуск сертификата».

3.4.2. Подпроцесс «Создание подписки на обеспечение сертификатом»

Входящая информация поступает из подпроцесса «Обработка обращений»

Администратор безопасности получает электронное уведомление и визирует заявку. Если заявка отклонена – процесс завершается. Если заявка не отклонена – Администратор безопасности выбирает шаблон для выпуска сертификата и одобряет заявку.

В случае, если выбран шаблон Сертификат УНЭП, то сотрудник HR получает электронное уведомление, проверяет корректность информации о Сотруднике в объеме, необходимом для выпуска сертификата УНЭП и одобряет заявку. Данный шаг может быть произведён автоматически, при наличии данных о Пользователе КУЦ в Информационной автоматизированной системе управления персоналом Госкорпорации «Росатом» (далее - ИАСУП)

В случае если выбран шаблон Сертификат УКЭП, то сотрудник HR получает электронное уведомление, проверяет корректность информации о Сотруднике, вносит в информацию пользователе КУЦ, в объеме, необходимом для выпуска сертификата УКЭП и регистрации его в ЕСИА и

одобряет заявку. Данный шаг может быть произведён автоматически, при наличии данных о Пользователе КУЦ в ИАСУП.

Для выпуска Сертификата УКЭП ИС ОКЗ с использованием инфраструктуры осуществляет проверку достоверности документов и сведений: производится проверка СНИЛС в сервисе ПФР, получение выписки из ЕГРЮЛ в сервисе ФНС, проверка паспортных данных в сервисе МВД. В случае не получения ответа от любого сервиса СМЭВ процесс возвращается на предыдущий шаг.

Уполномоченному лицу формируется и отправляется электронное уведомление. Уполномоченное лицо подписывает PDF-документ, печатный аналог электронной заявки, с использованием сервиса электронной подписи КриптоПро DSS. Если заявка отклонена – процесс завершается, если заявка одобрена – Оператору УЦ формируется и отправляется электронное уведомление. Оператор УЦ вычисляется автоматически в соответствии с настройками ИС ОКЗ согласно принадлежности заявителя к той или иной организации.

Исходящая информация поступает в подпроцесс «Создание сертификата УКЭП» или подпроцесс «Создание сертификата УНЭП» в зависимости от выбранного шаблона.

3.4.3. Подпроцесс «Корректировка подписки на обеспечение сертификатом»

Входящая информация поступает из подпроцесса «Обработка обращений»

Корректировка подписки на обеспечение сертификатом УКЭП/УНЭП производится самостоятельно Пользователем КУЦ при помощи веб-интерфейса сервиса «Управление инфраструктурой открытых ключей».

Корректировка подписки на обеспечение сертификатом УНЭП может производиться в автоматическом режиме получении данных из ИАСУП, входящих в перечень полей «Имя субъекта» в сертификате УНЭП.

После подтверждения необходимости корректировки подписки Администратор безопасности одобряет заявку.

В случае корректировки подписки на обеспечение сертификатом УКЭП, Сотруднику HR формируется и отправляется электронное уведомление. Сотрудник HR получает электронное уведомление, вносит в информацию пользователе КУЦ, в объеме, необходимом для выпуска сертификата УКЭП и регистрации его в ЕСИА. Данный шаг может быть произведён автоматически, при наличии данных о Пользователе КУЦ в ИАСУП.

Для выпуска Сертификата УКЭП ИС ОКЗ с использованием инфраструктуры осуществляет проверку достоверности документов и сведений: производится проверка СНИЛС в сервисе ПФР, получение выписки из ЕГРЮЛ в сервисе ФНС, проверка паспортных данных в сервисе

МВД. В случае не получения ответа от любого сервиса СМЭВ процесс возвращается на предыдущий шаг.

Исходящая информация поступает в подпроцесс «Создание сертификата УКЭП»

3.4.4. Подпроцесс «Сокращение подписки на обеспечение сертификатом».

Входящая информация поступает из подпроцесса «Обработка обращений»

Сокращение подписки на обеспечение сертификатом УКЭП производится самостоятельно при помощи личного кабинета Пользователя ИС ОКЗ.

Сокращение подписки на обеспечение сертификатом УНЭП может производиться в автоматическом режиме при выборе соответствующего шаблона.

Инициирование сокращения подписки на обеспечение сертификатом УКЭП/УНЭП пользователю КУЦ (инициирование должно быть доступно пользователю КУЦ и Администратору безопасности).

Администратору безопасности формируется и отправляется электронное уведомление.

Администратор безопасности получает электронное уведомление и визирует заявку. Если заявка отклонена – процесс завершается, если заявка одобрена – Уполномоченному лицу формируется и отправляется электронное уведомление.

Уполномоченному лицу формируется и отправляется электронное уведомление.

Уполномоченное лицо получает электронное уведомление и визирует заявку. Если заявка отклонена – процесс завершается, если заявка одобрена – ИС ОКЗ автоматически отзывает сертификат на УЦ.

Исходящая информация поступает в подпроцесс «Аннулирование сертификата»

3.4.5. Подпроцесс «Перевыпуск сертификата».

Входящая информация поступает из подпроцесса «Обработка обращений»

Инициатором перевыпуска сертификата может быть Пользователь КУЦ, имеющий действующую подписку на сертификат с совпадающим шаблоном.

Перевыпуск сертификата производится при компрометации или подозрении на компрометацию сертификата ключа проверки электронной подписи.

Исходящая информация поступает в подпроцесс «Аннулирование сертификата»

3.4.6. Подпроцесс «Аннулирование сертификата».

Входящая информация поступает из подпроцессов «Корректировка подписки на обеспечение сертификатом», «Сокращение подписки на обеспечение сертификатом» и «Перевыпуск сертификата УКЭП»

Подпроцесс «Аннулирование сертификата» регламентирует аннулирование сертификатов КУЦ.

КУЦ уведомляет Пользователя КУЦ и всех лиц, зарегистрированных в КУЦ, об аннулировании сертификата не позднее 12 часов с момента наступления описанного события.

КУЦ аннулирует сертификат Пользователя КУЦ в следующих случаях:

- При сокращении Руководителем предприятия подписки на обеспечение сертификатом ключа проверки электронной подписи;
- по заявке Пользователя КУЦ в ИС ОКЗ;
- в случае прекращения действия Договора;
- в случае, если не подтверждено, что владелец сертификата 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;
- в случае, если вступило в силу решение суда, которым, в частности, установлено, что сертификат 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.

Администратор УЦ получает электронное уведомление, проверяет отзыв сертификата на УЦ и визирует заявку. Администратор УЦ осуществляет обработку электронного заявления на аннулирование сертификата и вносит информацию об аннулировании в ИС ОКЗ.

Если заявка отклонена – процесс завершается, если заявка одобрена – сертификат принимает статус отозванного в ИС ОКЗ.

При наличии действующей подписки на обеспечение сертификатом, исходящая информация поступает в подпроцесс «Создание сертификата УКЭП»

При отсутствии действующей подписки на обеспечение сертификатом процесс заканчивается.

3.4.7. Подпроцесс «Создание сертификата УКЭП»

Входящая информация поступает из подпроцессов «Создание подписки на обеспечение сертификатом» и «Аннулирование сертификата»

Оператор КУЦ получает электронное уведомление, подключает ключевой носитель (при необходимости использования ключевого носителя) к рабочему месту Оператора КУЦ.

Оператор КУЦ выбирает параметры ключевого контейнера, создает ключевой контейнер и запрос на сертификат. Выполняется выпуск сертификата на УЦ, соответствующему шаблону сертификата в УЦ.

Оператор КУЦ устанавливает выпущенный сертификат на ключевой носитель (при необходимости использования ключевого носителя).

При выдаче квалифицированного ИС ОКЗ 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 (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

Оператор КУЦ создаёт пакет для передачи выпущенного сертификата Администратору безопасности лично или Службой специальной связи.

Исходящая информация поступает в подпроцесс «Вручение сертификата УКЭП»

3.4.8. Подпроцесс «Вручение сертификата УКЭП»

Входящая информация поступает из подпроцесса «Создание сертификата УКЭП»

Администратору безопасности формируется и отправляется электронное уведомление о необходимости получения ключевого носителя.

В случае использования ключевого носителя, Оператор УЦ передает ключевой носитель Администратору безопасности.

Администратор безопасности подтверждает получение в ИС ОКЗ.

Пользователю КУЦ формируется и отправляется электронное уведомление о выпуске сертификата.

Администратор безопасности верифицирует пользователя КУЦ и одобряет заявку. При вручении сертификата Администратор безопасности обязан установить личность Пользователя КУЦ и получить подтверждение правомочия обращаться за получением квалифицированного сертификата.

Пользователь КУЦ получает ключевой носитель с выпущенным сертификатом (при наличии).

В присутствии Администратора безопасности Пользователь КУЦ аутентифицируется в личном кабинете ИС ОКЗ, где ознакамливается с

информацией, содержащейся в квалифицированном сертификате и нажимает кнопку «Сертификат получен». Нажатие Пользователем КУЦ на кнопку «Сертификат получен» является равнозначным применению простой электронной подписи в Сертификате УКЭП.

Исходящая информация поступает в подпроцесс «Контроль действия сертификата»

3.4.9. Подпроцесс «Создание сертификата УНЭП»

Входящая информация поступает из подпроцессов «Создание подписки на обеспечение сертификатом УНЭП» и «Перевыпуск сертификата УНЭП»

При выборе шаблона для выпуска Сертификата УНЭП в автоматическом режиме, выпуск сертификата УНЭП производится без участия Оператора КУЦ.

В случае, если сертификат УНЭП выпускается на ключевом носителе, Оператор КУЦ получает электронное уведомление, подключает ключевой носитель к рабочему месту Оператора КУЦ.

Оператор КУЦ выбирает параметры ключевого контейнера, создает ключевой контейнер и запрос на сертификат. Выполняется выпуск сертификата на УЦ, соответствующему шаблону сертификата в УЦ.

Оператор КУЦ устанавливает выпущенный сертификат на ключевой носитель (при необходимости использования ключевого носителя).

Оператор КУЦ устанавливает выпущенный сертификат на ключевой носитель пользователя КУЦ (при необходимости использования ключевого носителя).

Создаёт пакет для передачи выпущенного сертификата Администратору безопасности лично или Службой специальной связи.

Исходящая информация поступает в подпроцесс «Вручение сертификата УНЭП»

3.4.10. Подпроцесс «Вручение сертификата УНЭП»

Входящая информация поступает из подпроцесса «Создание сертификата УНЭП»

При выдаче сертификата УНЭП на ключевом носителе Администратору безопасности формируется и отправляется электронное уведомление. Оператор УЦ передает ключевой носитель Администратору безопасности.

Администратор безопасности получает электронное уведомление и визирует заявку.

Пользователю КУЦ формируется и отправляется электронное уведомление о выпуске сертификата.

Администратор безопасности верифицирует пользователя КУЦ и одобряет заявку. При вручении сертификата Администратор безопасности обязан установить личность Пользователя КУЦ.

В присутствии Администратора безопасности Пользователь КУЦ аутентифицируется в личном кабинете ИС ОКЗ, где ознакамливается с информацией, содержащейся в квалифицированном сертификате, руководством по обеспечению безопасности Средства электронной подписи, ПИН-кодом и нажимает кнопку «Сертификат получен».

Исходящая информация поступает в подпроцесс «Контроль действия сертификата»

3.4.11. Подпроцесс «Контроль действия сертификата»

Контроль действия сертификата УКЭП инициируется автоматически за 90 дней до окончания действия сертификата.

Администратору безопасности формируется и отправляется электронное уведомление.

Администратор безопасности получает электронное уведомление и визирует заявку. Если заявка отклонена – процесс завершается. Если заявка не отклонена – Администратор безопасности выбирает шаблон для выпуска сертификата и одобряет заявку.

Сотруднику HR формируется и отправляется электронное уведомление.

Сотрудник HR получает электронное уведомление и визирует заявку. Сотрудник HR проверяет корректность информации о Сотруднике, заполняет недостающую информацию и одобряет заявку.

При выпуске сертификата УКЭП производится проверка СНИЛС в сервисе ПФР, получение выписки из ЕГРЮЛ в сервисе ФНС, проверка паспортных данных в сервисе МВД.

В случае не получения ответа от любого сервиса СМЭВ процесс возвращается на предыдущий шаг.

Исходящая информация поступает в подпроцесс «Создание сертификата УКЭП»

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”.

Порядок внесения изменений

КУЦ в одностороннем порядке вносит изменения в Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с использованием Информационной системы органа криптографической защиты.

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

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

Контроль и ответственность

6.1 Контроль выполнения требований Порядка

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

Пользователь КУЦ несёт ответственность за:

- обеспечение конфиденциальности ключей ЭП, в частности не допущение использования принадлежащих ему ключей ЭП без его согласия;
- уведомление КУЦ 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.

Администратор безопасности несёт ответственность за:

- точность и своевременность формализации обращений пользователей КУЦ;
- идентификацию и аутентификацию Пользователя КУЦ и проверку представленных документов;
- выдачу Пользователю КУЦ ключевых документов;

Оператор КУЦ несёт ответственность за:

- формирование комплекта ключевых документов, выдаваемых КУЦ;
- передачу (отправку) комплекта документов, выдаваемых КУЦ;
- 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 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.

6.2 Ответственность работников за несоблюдение требований Порядка

За несоблюдение Порядка ответственные лица несут административную и дисциплинарную ответственность в соответствии с действующим законодательством и в соответствии со следующей матрицей ответственности:

Подпроцессы в составе процесса	Участники процесса					
	Руководитель организации	Пользователь КУЦ	Администратор безопасности	HR	Оператор КУЦ	Администратор КУЦ
Подпроцесс «Обработка обращения»			О			К
Подпроцесс «Создание подписки на обеспечение сертификатом»	Инф		О	О		К
Подпроцесс «Корректировка подписки на обеспечение сертификатом»			О	О		К
Подпроцесс «Сокращение подписки на обеспечение сертификатом»	Инф		О			К
Подпроцесс «Перевыпуск сертификата»		Инф	О			К
Подпроцесс «Аннулирование сертификата»		Инф				О
Подпроцесс «Создание сертификата УКЭП»		Инф			О	К
Подпроцесс «Вручение сертификата УКЭП»		Инф	О			К
Подпроцесс «Создание сертификата УНЭП»		Инф			О	К
Подпроцесс «Вручение сертификата УНЭП»		Инф	О			К
Подпроцесс «Контроль действия сертификата»			О			К

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

Сокращение	Название роли	Определение
	Контролер	Осуществляет контроль выполнения и достижения результатов подпроцесса/процедуры
О	Ответственный	Несет ответственность за достижение результата по подпроцессу/процедуре в совей предметной области

Сокращение	Название роли	Определение
Инф	Информируемый	Получает информацию о ходе/результате подпроцесса /процедуры

Перечень приложений

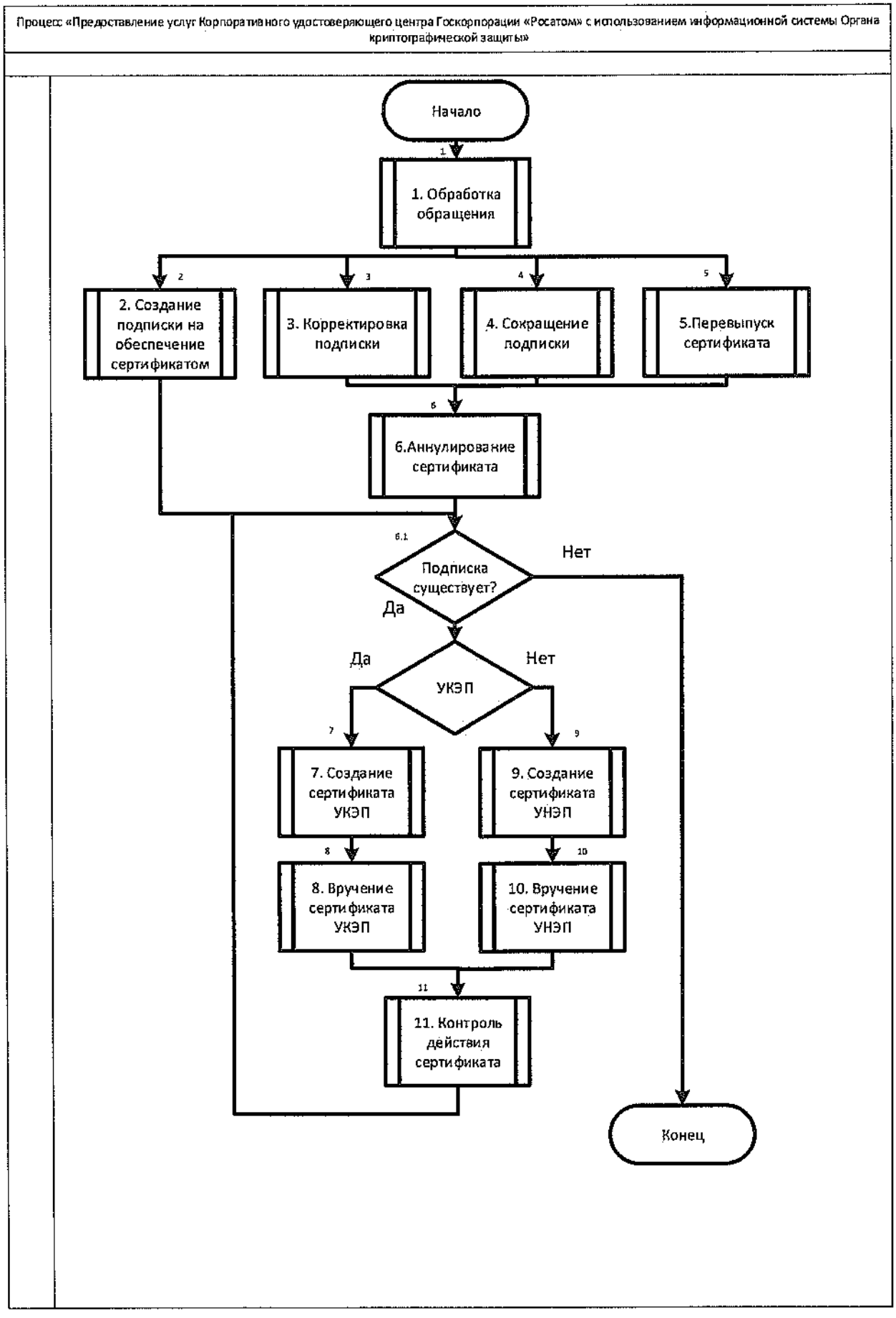
Приложение №1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

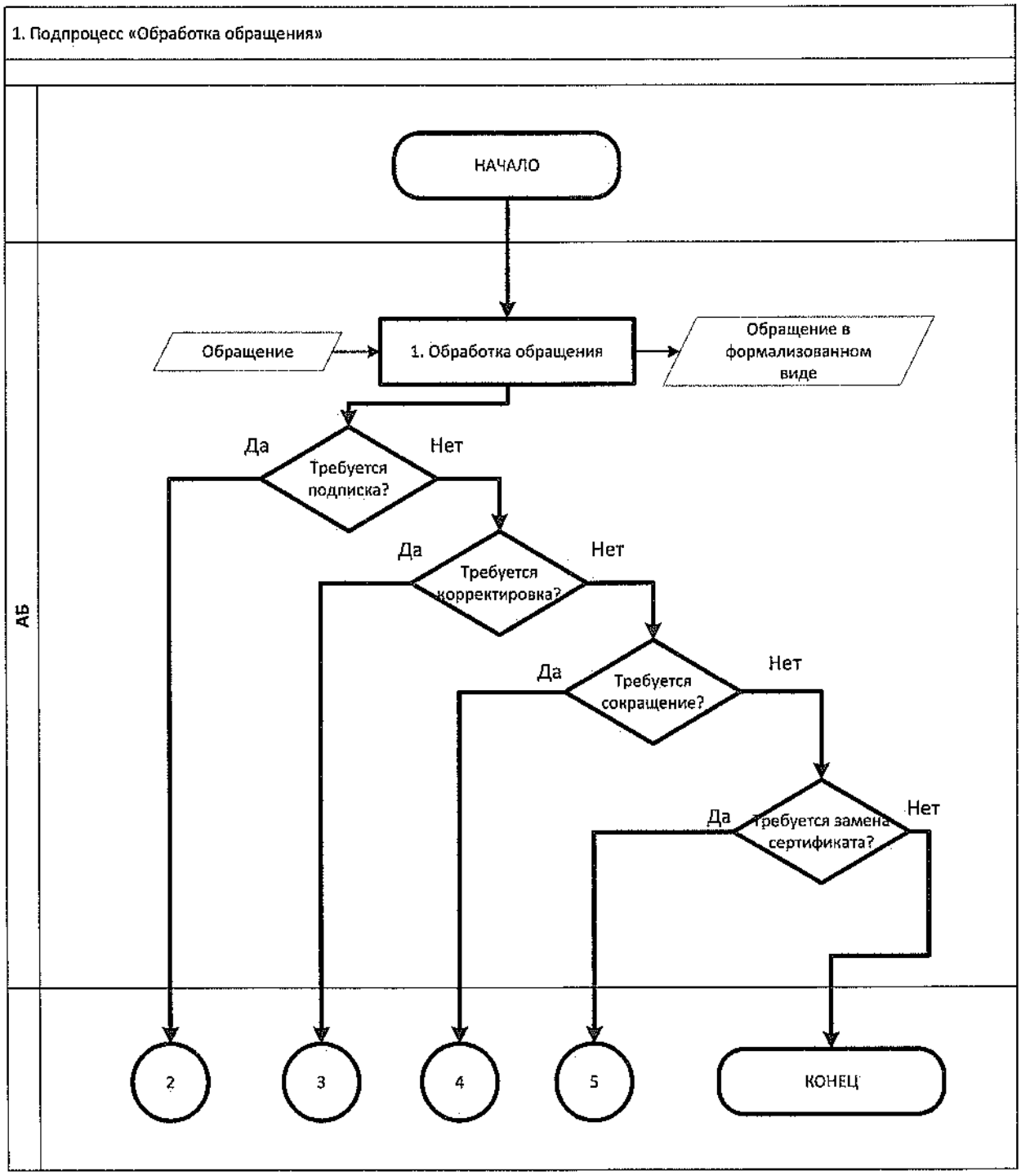
Приложение №2. Формат сертификатов ключа проверки электронной подписи

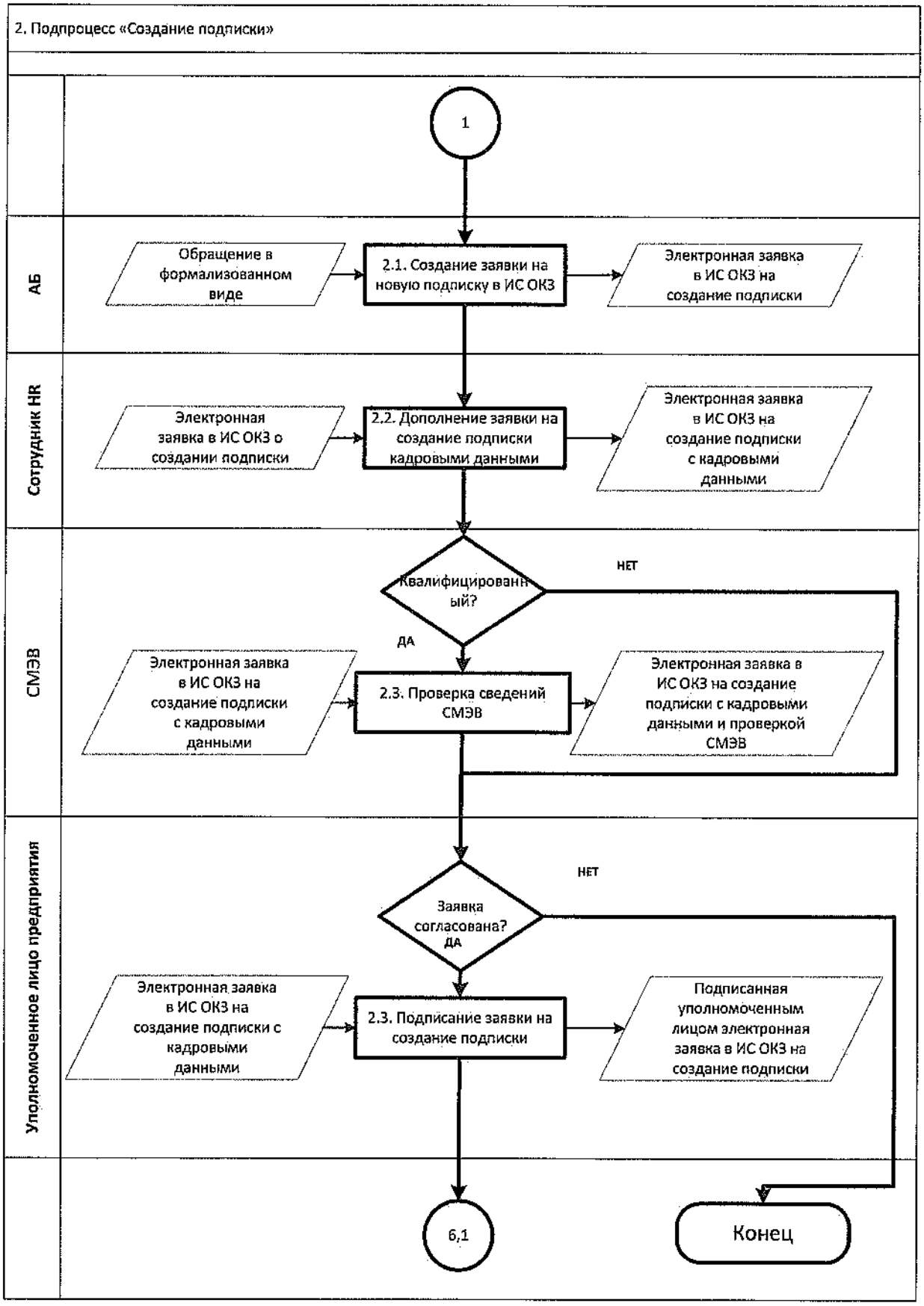
Приложение №3. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

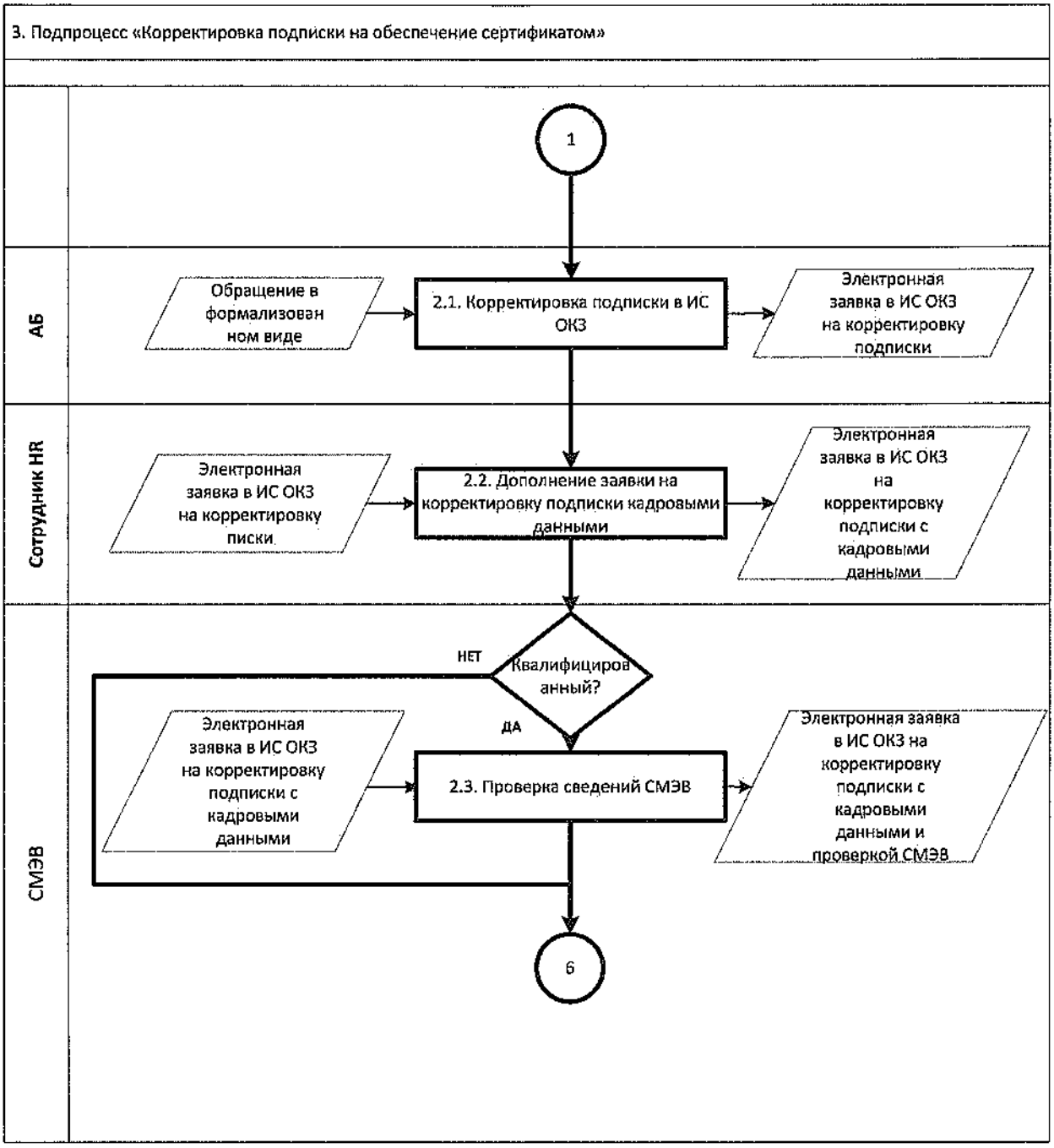
Приложение №4. Шаблоны сертификатов ключей проверки электронной подписи

Приложение №1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

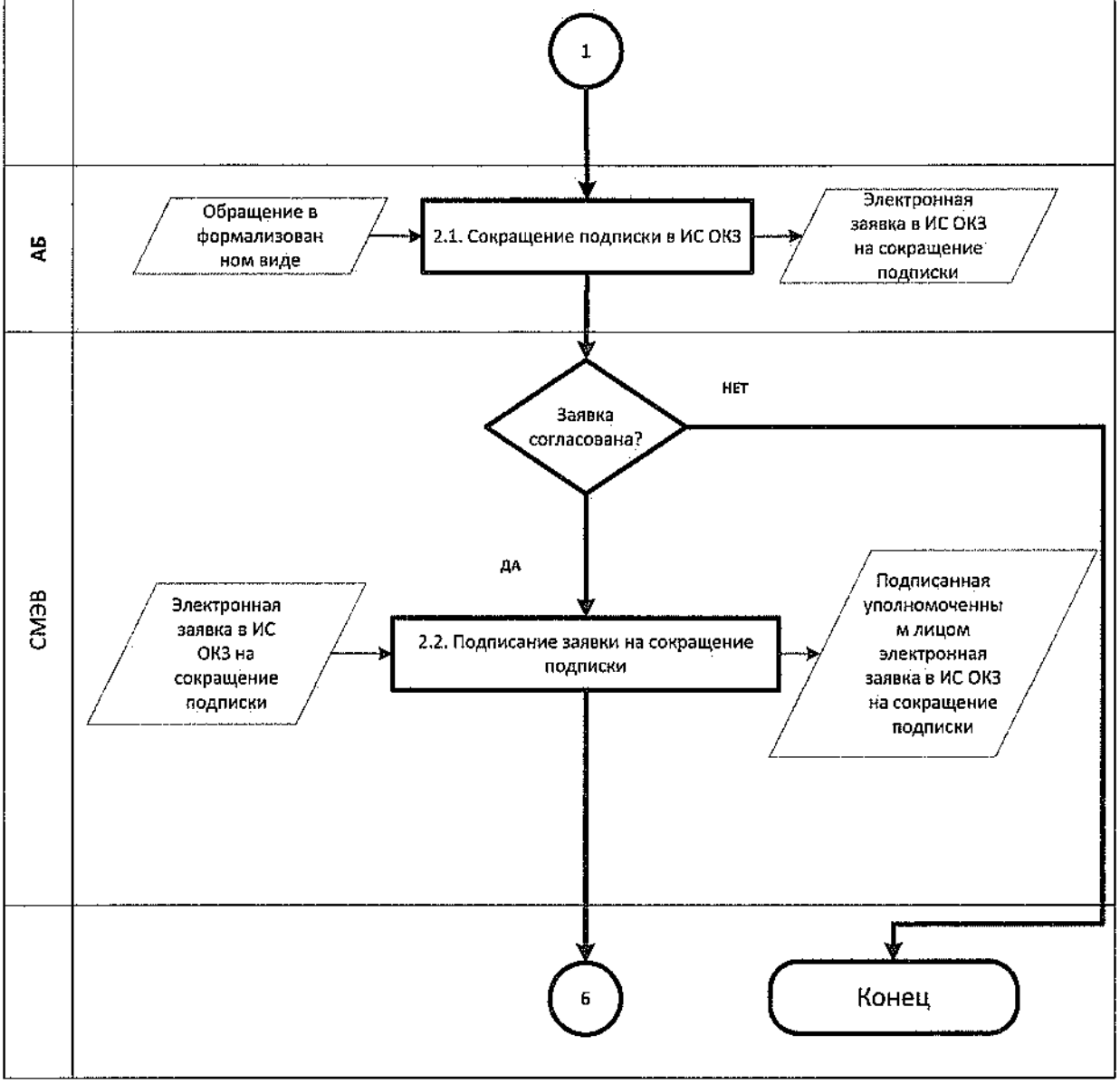


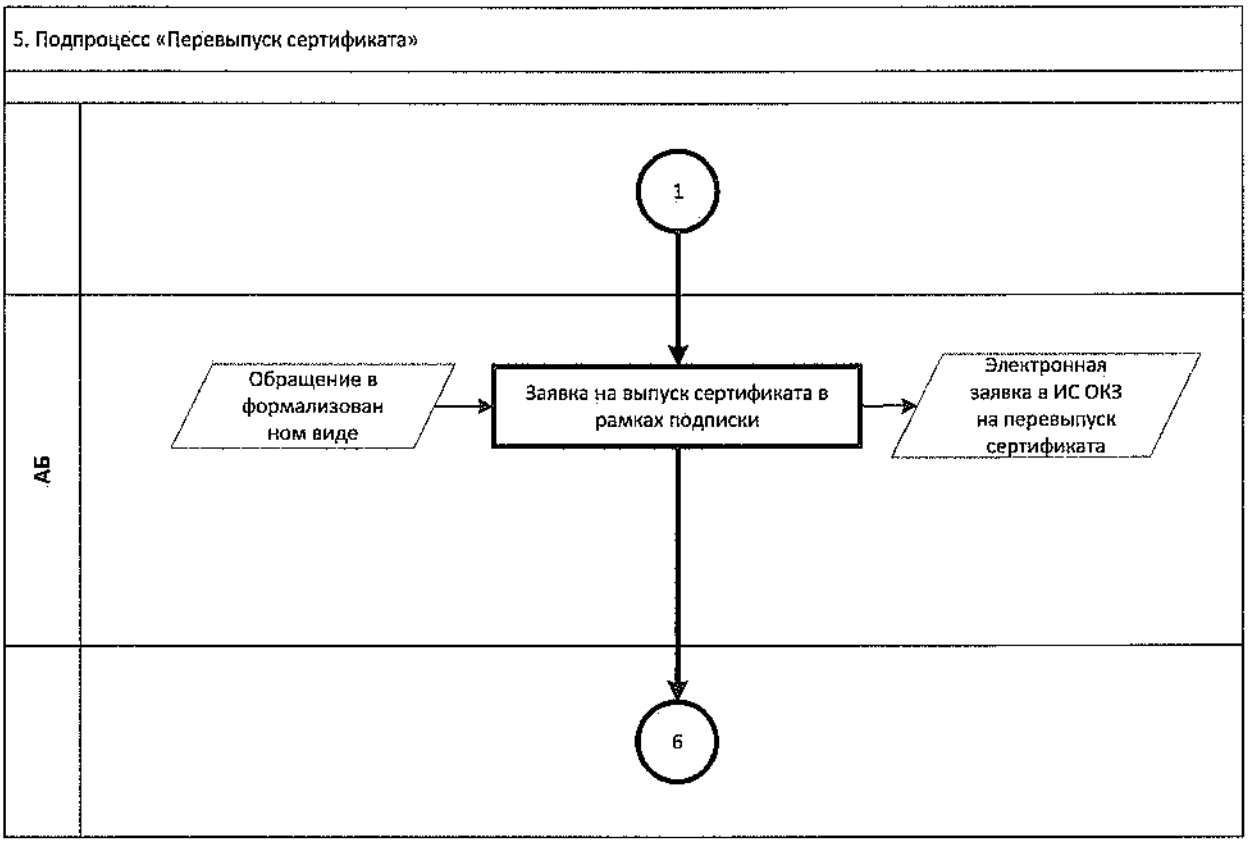

1. Подпроцесс «Обработка обращения»
АБ
НАЧАЛО
Обращение
1. Обработка обращения
Обращение в формализованном виде
Да
Требуется подписка?
Нет
Да
Требуется корректировка?
Нет
Да
Требуется сокращение?
Нет
Да
Требуется замена сертификата?
Нет
2
3
4
5
КОНЕЦ

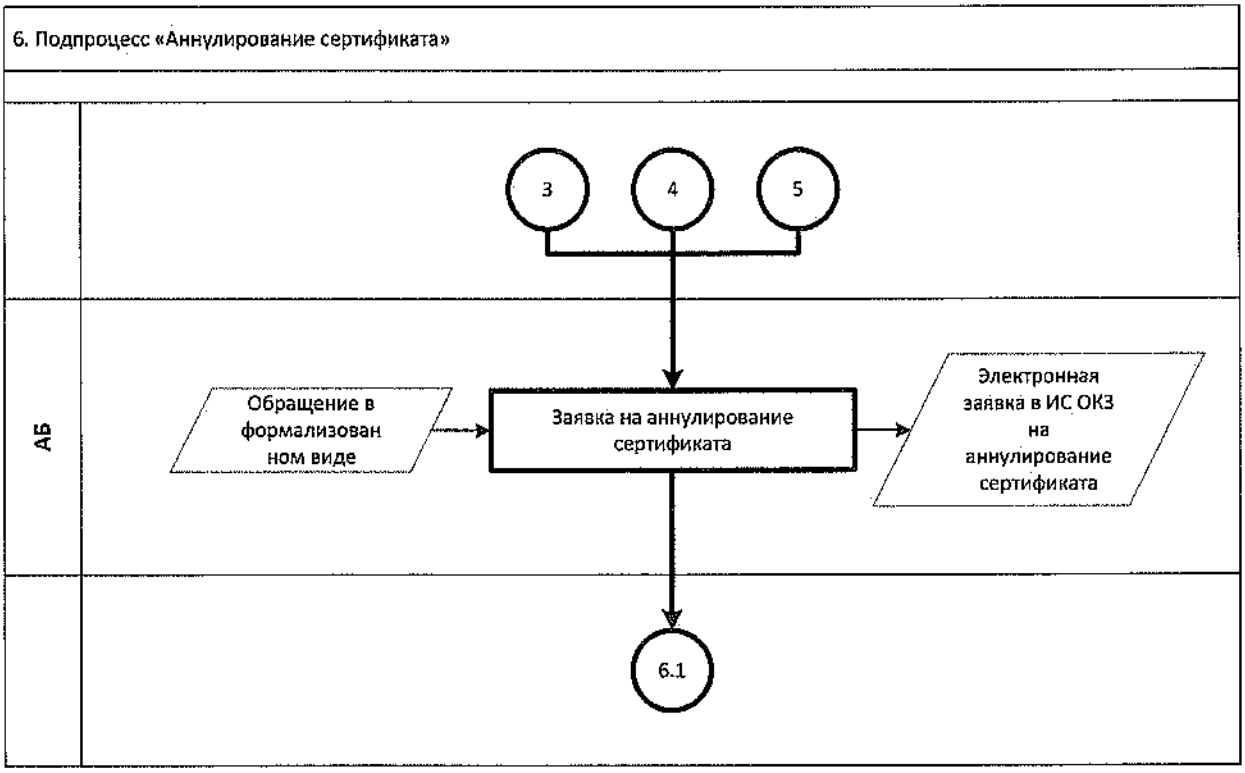

2. Подпроцесс «Создание подписки»
АБ
Сотрудник HR
СМЭВ
Уполномоченное лицо предприятия
1
Обращение в формализованном виде
2.1. Создание заявки на новую подписку в ИС ОКЗ
Электронная заявка в ИС ОКЗ на создание подписки
Электронная заявка в ИС ОКЗ о создании подписки
2.2. Дополнение заявки на создание подписки кадровыми данными
Электронная заявка в ИС ОКЗ на создание подписки с кадровыми данными
Квалифицированный?
НЕТ
ДА
Электронная заявка в ИС ОКЗ на создание подписки с кадровыми данными
2.3. Проверка сведений СМЭВ
Электронная заявка в ИС ОКЗ на создание подписки с кадровыми данными и проверкой СМЭВ
Заявка согласована?
НЕТ
ДА
Электронная заявка в ИС ОКЗ на создание подписки с кадровыми данными
2.3. Подписание заявки на создание подписки
Подписанная уполномоченным лицом электронная заявка в ИС ОКЗ на создание подписки
6,1
Конец


3. Подпроцесс «Корректировка подписки на обеспечение сертификатом»
АБ
Сотрудник HR
СМЭВ
1
Обращение в формализован ном виде
2.1. Корректировка подписки в ИС ОКЗ
Электронная заявка в ИС ОКЗ на корректировку подписки
Электронная заявка в ИС ОКЗ на корректировку писки
2.2. Дополнение заявки на корректировку подписки кадровыми данными
Электронная заявка в ИС ОКЗ на корректировку подписки с кадровыми данными
НЕТ
Квалифициров анный?
ДА
Электронная заявка в ИС ОКЗ на корректировку подписки с кадровыми данными
2.3. Проверка сведений СМЭВ
Электронная заявка в ИС ОКЗ на корректировку подписки с кадровыми данными и проверкой СМЭВ
6

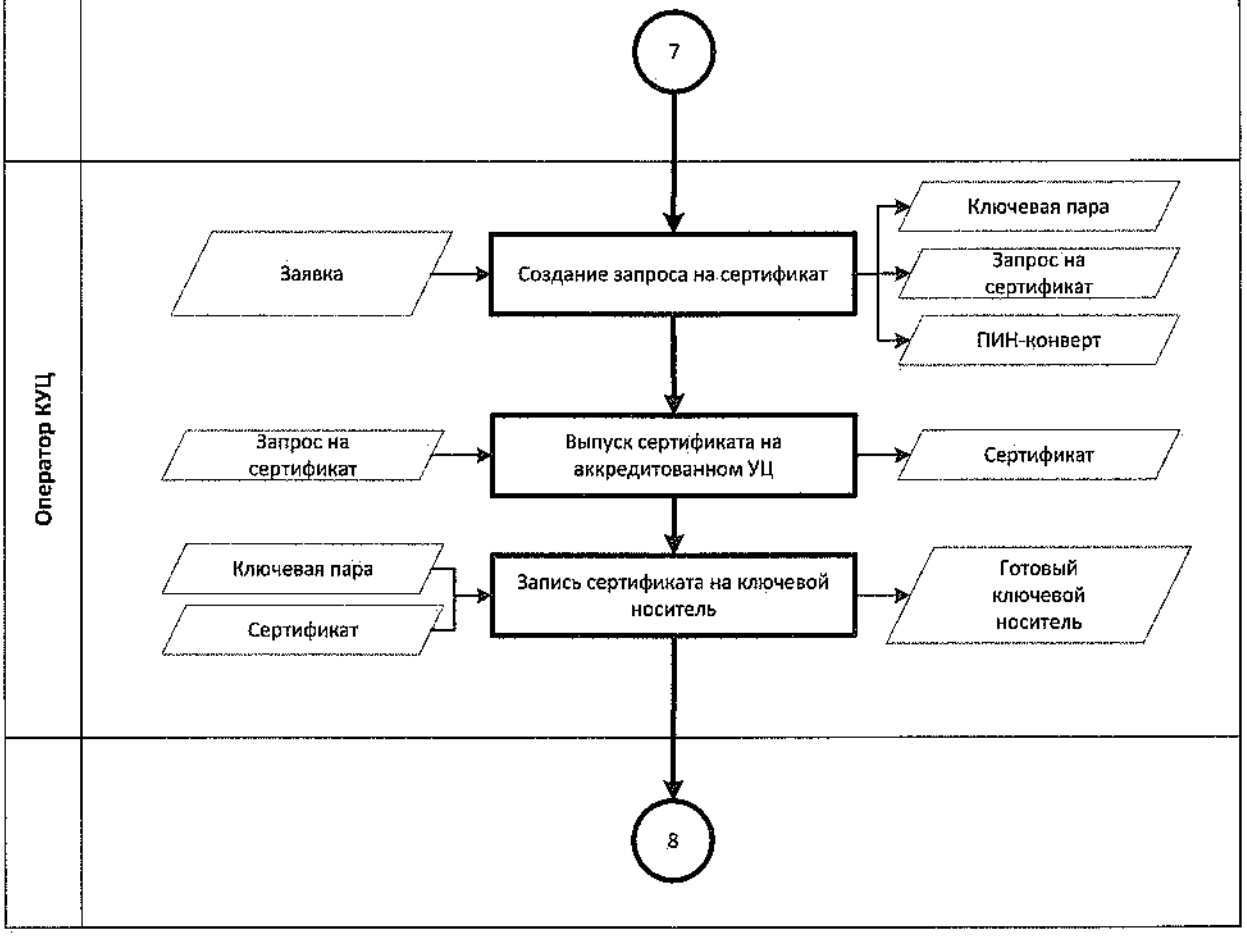
4. Подпроцесс «Сокращение подписки на обеспечение сертификатом»

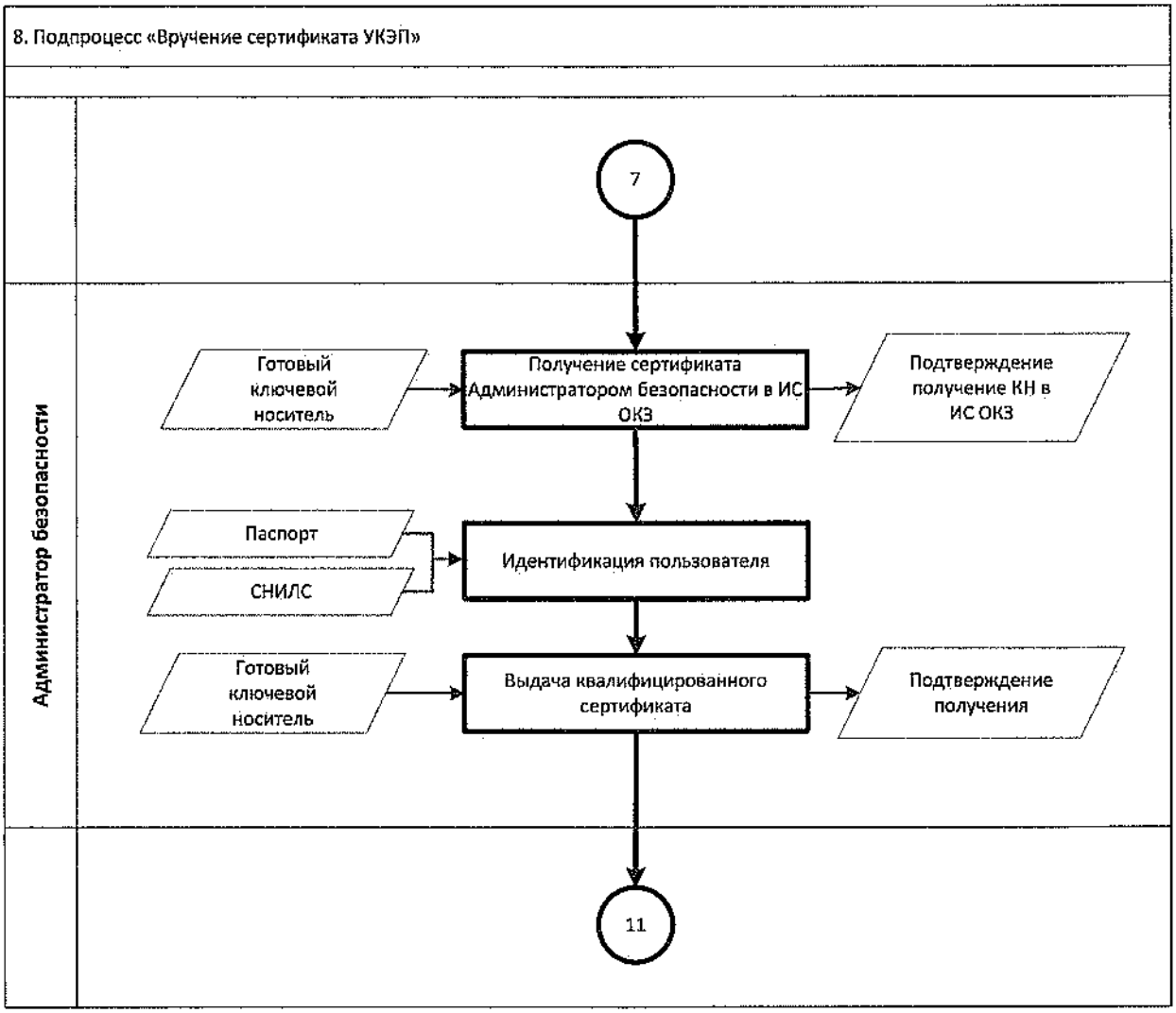


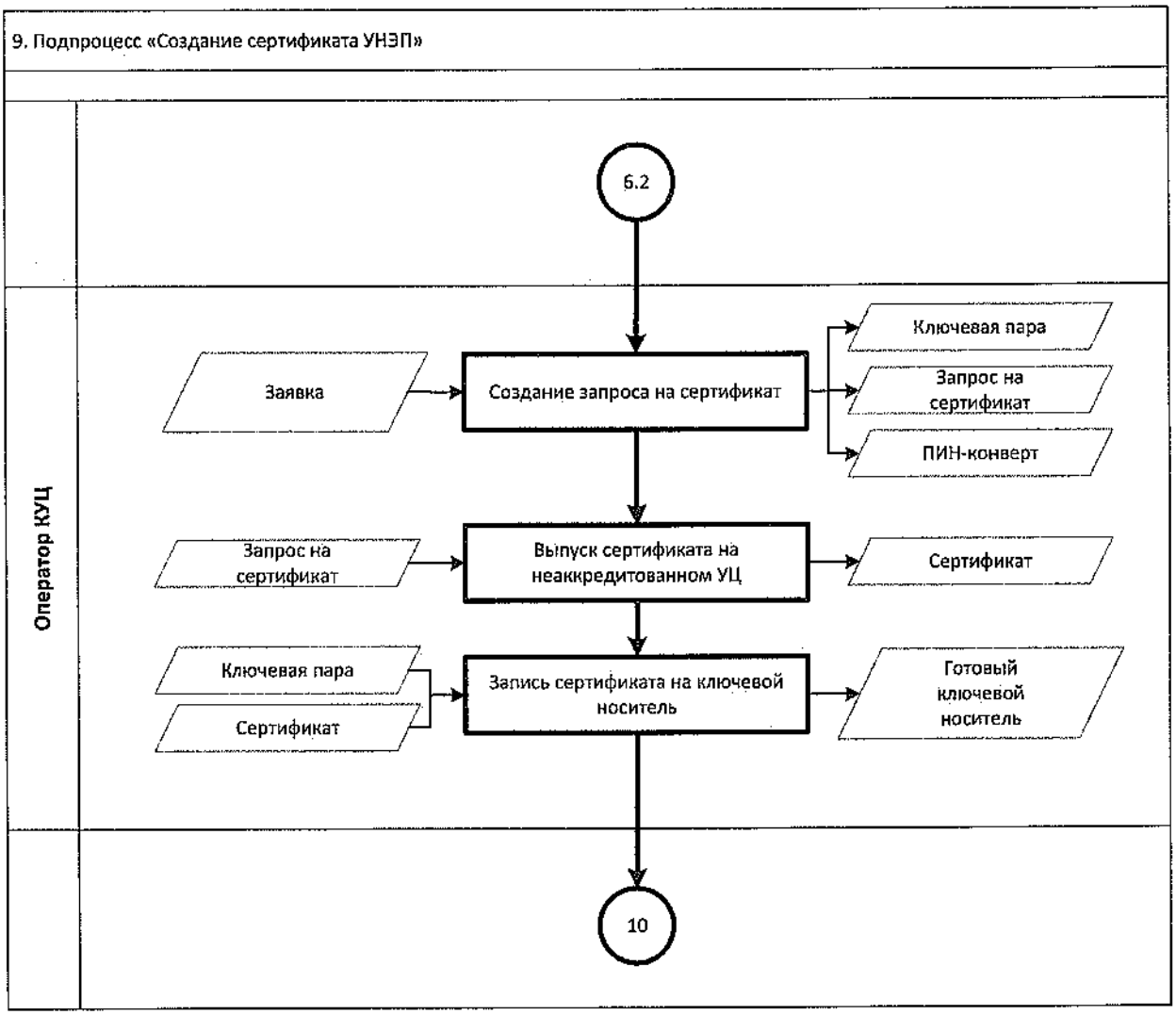

5. Подпроцесс «Перевыпуск сертификата»
АБ
1
Обращение в формализован ном виде
Заявка на выпуск сертификата в рамках подписки
Электронная заявка в ИС ОКЗ на перевыпуск сертификата
6

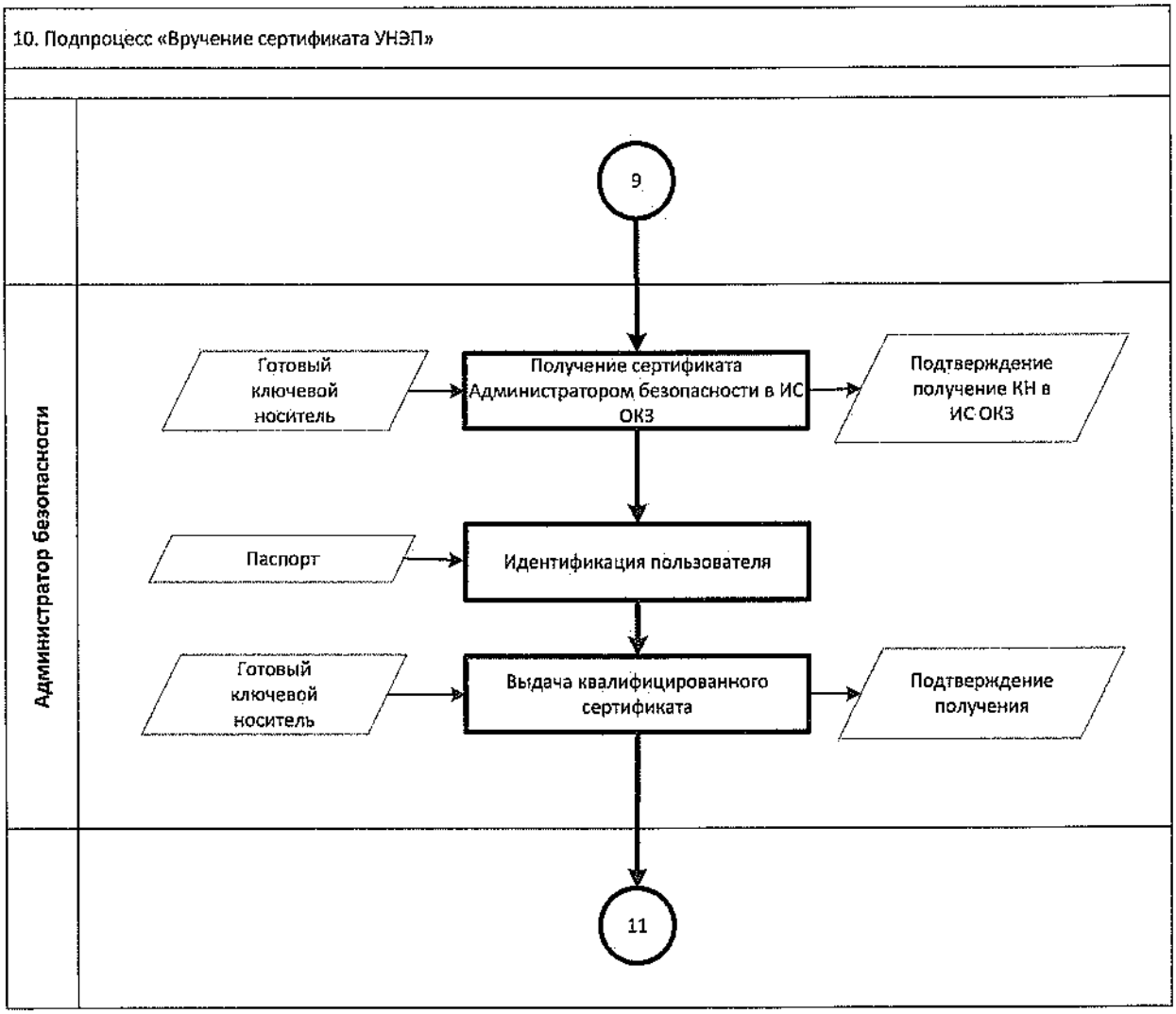

6. Подпроцесс «Аннулирование сертификата»
АБ
3
4
5
Обращение в формализован ном виде
Заявка на аннулирование сертификата
Электронная заявка в ИС ОКЗ на аннулирование сертификата
6.1

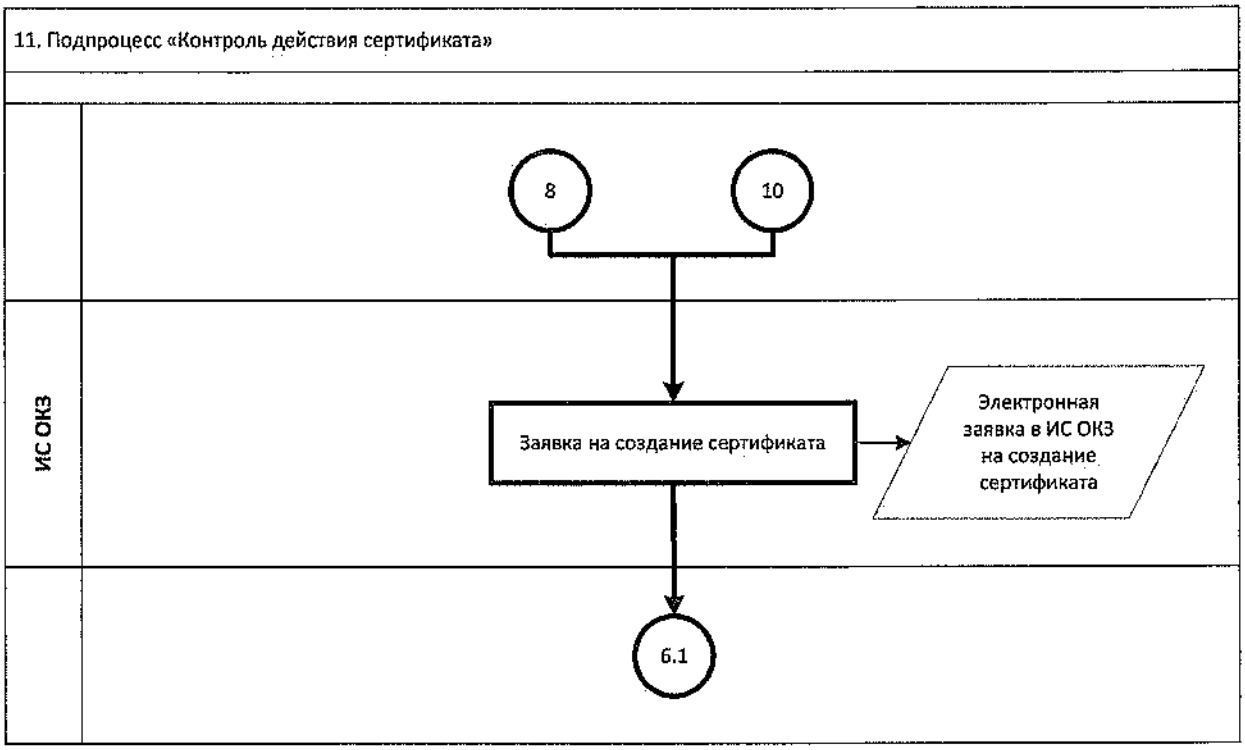
7. Подпроцесс «Создание сертификата УКЭП»




8. Подпроцесс «Вручение сертификата УКЭП»
Администратор безопасности
7
Готовый ключевой носитель
Получение сертификата Администратором безопасности в ИС ОКЗ
Подтверждение получение КН в ИС ОКЗ
Паспорт
СНИЛС
Идентификация пользователя
Готовый ключевой носитель
Выдача квалифицированного сертификата
Подтверждение получения
11


9. Подпроцесс «Создание сертификата УНЭП»
Оператор КУЦ
6.2
Заявка
Создание запроса на сертификат
Ключевая пара
Запрос на сертификат
ПИН-конверт
Запрос на сертификат
Выпуск сертификата на неаккредитованном УЦ
Сертификат
Ключевая пара
Сертификат
Запись сертификата на ключевой носитель
Готовый ключевой носитель
10


10. Подпроцесс «Вручение сертификата УНЭП»
Администратор безопасности
9
Готовый ключевой носитель
Получение сертификата Администратором безопасности в ИС ОКЗ
Подтверждение получение КН в ИС ОКЗ
Паспорт
Идентификация пользователя
Готовый ключевой носитель
Выдача квалифицированного сертификата
Подтверждение получения
11


11. Подпроцесс «Контроль действия сертификата»
ИС ОКЗ
8
10
Заявка на создание сертификата
Электронная заявка в ИС ОКЗ на создание сертификата
6.1

Приложение №2. Формат сертификатов ключа проверки электронной подписи

1. Формат квалифицированного 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 34.11/34.10-2012
Issuer	Издатель сертификата	1) commonName (общее имя). 2) countryName (наименование страны). 3) stateOrProvinceName (наименование штата или области). 4) localityName (наименование населенного пункта). 5) streetAddress (название улицы, номер дома). 6) organizationName (наименование организации). 7) organizationUnitName (подразделение организации). 8) title (должность). 9) OGRN (ОГРН). 10) 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 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с 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

2. Формат неквалифицированного 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 34.11/34.10-2012
Issuer	Издатель сертификата	1) commonName (общее имя). 2) countryName (наименование страны). 3) stateOrProvinceName (наименование штата или области). 4) localityName (наименование населенного пункта). 5) streetAddress (название улицы, номер дома). 6) organizationName (наименование организации). 7) organizationUnitName (подразделение организации). 8) title (должность). 9) OGRN (ОГРН). 10) 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) organizationName (наименование организации). 6) organizationUnitName (подразделение организации). 7) title (должность). 8) E = электронная почта
Public Key	Открытый ключ	Уникальный ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с 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 №3. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

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 №4. Шаблоны сертификатов ключей проверки электронной подписи

Шаблоны сертификатов ключей проверки электронной подписи

1. Квалифицированный сертификат Госкорпорации «Росатом»

Данные сертификаты ключа проверки электронной подписи предназначены для использования при участии в качестве заказчика на электронных торговых площадках, для использования в защищенной корпоративной почтовой системе Госкорпорации «Росатом», для аутентификации пользователей при доступе к корпоративным информационным системам ЦОД из сети Интернет.

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В сертификате указываются следующие объектные идентификаторы:

- 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)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

2. 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 объектные идентификаторы:

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)

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

3. Квалифицированный сертификат для Росреестра (требуется доп. доверенность)

Данные сертификаты ключа проверки электронной подписи предназначены для 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, для использования при участии в качестве заказчика на электронных торговых площадках, для использования в защищенной корпоративной почтовой системе Госкорпорации «Росатом», для аутентификации пользователей при доступе к корпоративным информационным системам ЦОД из сети Интернет.

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)
- Шифрующая файловая система (EFS) (1.3.6.1.4.1.311.10.3.4)
- Вход со смарт-картой (1.3.6.1.4.1.311.20.2.2)
- 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)

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

4. Аутентификация сервера

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

- Аутентификация веб-сервера.

В сертификате указываются следующие дополнительные поля:

В поле улучшенный ключ:

- Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

5. 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 ЗАО «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)

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

6. 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)

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

7. 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 объектные идентификаторы:

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)

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

Приложение № 9 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю
Директор по информационным технологиям
АО «Гринатом»

_____/ А.Н. Киселёв /

М.П.

ПОРЯДОК

организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну
с использованием информационной системы Органа криптографической защиты

Москва 2021 г.

Содержание

1. Назначение и область применения

Настоящий порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну с использованием информационной системы Органа криптографической защиты» (далее – Порядок), разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты (далее – ОКЗ).

Настоящий Порядок определяет условия предоставления и правила пользования услугами ОКЗ, основные организационно-технические мероприятия, направленные на обеспечение работы ОКЗ. Порядок имеет статус локального.

Требования настоящего Порядка распространяются на организации-обладатели конфиденциальной информации (далее - ООКИ), использующие автоматизированные и/или информационные системы, в которых хранится, обрабатывается и/или передается по каналам связи с использованием средств криптографической защиты информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну и обязательны для выполнения сотрудниками, исполняющими следующие функциональные роли:

1. Уполномоченное лицо предприятия;
2. Аналитик ОКЗ АО «Гринатом»;
3. Администратор безопасности ОКЗ АО «Гринатом»;
4. Пользователь

Настоящий Порядок использует ссылки на следующие документы, необходимые для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну с использованием информационной системы Органа криптографической защиты:

Документ	Статус	Тип документа	Ответствен-ный
Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686 Н 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	Действует	Лицензия	Волков С.П.

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 06.04.11 г. № 63-ФЗ "Об электронной подписи"	Действует	Федеральный закон	Волков С.П.
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	Волков С.П.
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	Волков С.П.
Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» (с	Действует	Требование	Волков С.П.

пометкой «Для служебного пользования»)			

и является основой для регламентации следующих подпроцессов и процедур:

Подпроцессы:
Подпроцесс «Обработка обращения»
Подпроцесс «Создание подписки»
Подпроцесс «Передача СКЗИ»
Подпроцесс «Проверка готовности»
Подпроцесс «Монтаж, установка (инсталляция) криптографических средств»
Подпроцесс «Учет СКЗИ»
Подпроцесс «Обеспечение функционирования»
Подпроцесс «Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки»

2. Термины, определения и сокращения

Термин	Определение
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока
Книга лицевых счетов	Книга регистрации применяющихся Пользователями средств криптографической защиты информации, эксплуатационной и технической документации
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

Средства криптографической защиты информации (СКЗИ)	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
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
Подписка	Заказ предприятия в ИС ОКЗ в соответствии с условиями договора присоединения на обеспечение сертификатами или средствами криптографической защиты и информации.

Сокращение	Расшифровка
АБ	Администратор безопасности ОКЗ АО «Гринатом»
ООКИ	Организация-обладатель конфиденциальной информации
КУЦ	Корпоративный Удостоверяющий центр Госкорпорации «Росатом»
ОКЗ	Орган криптографической защиты АО «Гринатом»
СКЗИ	Средство криптографической защиты информации
ЭП	Электронная подпись
ИС ОКЗ	Информационная система Органа криптографической защиты АО «Гринатом»
ЗКПС	Защищенная корпоративная почтовая система
ЕОСДО	Единая отраслевая система документооборота

3. Описание процесса

3.1. Цель процесса

Предоставление услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

3.2. Задачи процесса

- Создание и сокращение подписок предприятия в ИС ОКЗ;
- Передача СКЗИ;
- Разработка и утверждение схемы организации криптографической защиты информации;
- Обучение и допуск пользователей к самостоятельной эксплуатации СКЗИ;
- Проверка АРМ на соответствие требованиям к среде функционирования СКЗИ;
- Установка и настройка СКЗИ;
- Учет лицензий и АРМ с СКЗИ;
- Вывод из эксплуатации и уничтожение СКЗИ;

3.3. Участники группы процессов и их роли

№ п.п.	Участники	Основные роли
1	Уполномоченное лицо предприятия	• Согласовывает и подписывает электронные заявки в ИС ОКЗ на создание и сокращение подписок предприятия.
2	Аналитик ОКЗ АО «Гринатом» (далее – Аналитик)	• Согласовывает и подписывает электронные заявки в ИС ОКЗ на создание и сокращение подписок предприятий; • Разрабатывает и поддерживает в актуальном состоянии схему криптографической защиты информации в ИС ОКЗ; • Выделяет лицензии СКЗИ для предприятия в ИС ОКЗ; • Составляет заключение о возможности эксплуатации СКЗИ.
3	Администратор безопасности ОКЗ АО «Гринатом»	• Формирует обращения в ИС ОКЗ на создание, изменение и сокращение подписки предприятия; • Осуществляет проверку готовности СКЗИ к эксплуатации; • Выполняет монтаж, установку (инсталляцию) криптографических средств; • Учитывает СКЗИ в ИС ОКЗ; • Уничтожает выведенные из действия СКЗИ.
4	Пользователь	• Проходит обучение в ИС ОКЗ и сдает тестирование.

3.4. Описание подпроцессов

3.4.1. Подпроцесс «Обработка обращения»

АБ:

- Получает обращение от следующих возможных инициаторов:
  пользователь СКЗИ;
  АБ;
  уполномоченное лицо предприятия;
  аналитик ОКЗ,

  одним из следующих способов:
  заявка в ИС ОКЗ;

заявка через порталы АО «Гринатом» или «Страна Росатом»;
электронное письмо на п/я 1111@greenatom.ru;
звонок в центр поддержки пользователей АО «Гринатом»;

- Определяет наличие подписки у пользователя СКЗИ, указанного в обращении;
- Формализует обращение в зависимости от следующих условий:

В случае если подписка на пользователя, указанного в обращении, отсутствует и обращение не на создание подписки, то процесс «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 с использованием информационной системы Органа криптографической защиты» завершается.

В случае если подписка на пользователя, указанного в обращении, отсутствует и обращение на создание подписки, то исходящая информация поступает в подпроцесс «Создание подписки».

В случае если подписка на пользователя, указанного в обращении, есть, и обращение не на переустановку СКЗИ, а на сокращение подписки, то исходящая информация поступает в подпроцесс «Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки».

В случае если подписка на пользователя, указанного в обращении, есть, и обращение на переустановку СКЗИ, то исходящая информация поступает в подпроцесс «Проверка готовности».

В случае если подписка на пользователя, указанного в обращении, есть, и обращение не на переустановку СКЗИ, и не на сокращение подписки, то исходящая информация поступает в подпроцесс «Обеспечение функционирования».

3.4.2. Подпроцесс «Создание подписки»

Входящая информация поступает из подпроцесса «Обработка обращения».

АБ:

- Формирует электронную заявку на новую подписку в ИС ОКЗ;

Уполномоченное лицо предприятия:

- Получает электронную заявку на создание подписки в ИС ОКЗ;
- Подписывает заявку на создание подписки, *в случае если заявка им согласована.*

В случае если заявка не согласована, то процесс «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 с использованием информационной системы Органа криптографической защиты» завершается.

Аналитик:

- Получает подписанную уполномоченным лицом электронную заявку в ИС ОКЗ на создание подписки;
- Подписывает заявку на создание подписки, *в случае если заявка им согласована.*

Исходящая информация поступает в подпроцесс «Передача СКЗИ».

В случае если заявка не согласована, процесс «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 с использованием информационной системы Органа криптографической защиты» завершается.

3.4.3. Подпроцесс «Передача СКЗИ»

Входящая информация поступает из подпроцесса «Создание подписки».

Аналитик:
- Выделяет лицензию на СКЗИ согласно полученной заявке.

Лицензия на СКЗИ поступает АБ в ИС ОКЗ. Дистрибутив на СКЗИ и эксплуатационная техническая документация доступна для загрузки в ИС ОКЗ.

Исходящая информация поступает в подпроцесс «Проверка готовности».

3.4.4. Подпроцесс «Проверка готовности»

Входящая информация поступает из подпроцессов «Передача СКЗИ» и «Обработка обращения».

АБ:

- Осуществляет проверку готовности технических средств и вносит в ИС ОКЗ информацию по АРМ:

  Серийный/инвентарный номер АРМ;
  Адрес месторасположения АРМ;
  Вид обрабатываемой информации;
  Область использования СКЗИ;
  ФИО Пользователя СКЗИ;
  Реквизиты приказа о допуске пользователя к самостоятельной работе с СКЗИ;
  Номер опечатывающей пломбы;
  Версию и наименование операционной системы;
  Версию и наименование сертифицированного антивирусного средства;

Версию и наименование сертифицированного СЗИ от НСД;
О настройке СКЗИ в соответствии с ЕОМУ и документацией (ставит отметку).

- Формирует приказ о допуске пользователя к самостоятельной работе с СКЗИ.

Исходящая информация поступает в подпроцесс «Монтаж, установка (инсталляция) криптографических средств».

3.4.5. Подпроцесс «Монтаж, установка (инсталляция) криптографических средств»

Входящая информация поступает из подпроцесса «Проверка готовности».

АБ:

- Устанавливает и настраивает СКЗИ в соответствии с Инструкцией по установке СКЗИ (лицензия и дистрибутив для загрузки доступны в ИС ОКЗ);
- Устанавливает ПО «Агент ИС ОКЗ» (дистрибутив для загрузки доступен в ИС ОКЗ).

Исходящая информация поступает в подпроцесс «Обучение и допуск пользователя».

3.4.6. Подпроцесс «Обучение и допуск пользователя»

Входящая информация поступает из подпроцесса «Монтаж, установка (инсталляция) криптографических средств».

Пользователь:
- Получает по электронной почте уведомление о назначении ему в ИС ОКЗ курса обучения правилам работы с СКЗИ;
- Проходит обучение в ИС ОКЗ;
- Сдает тестирование по итогам обучения.

Активация СКЗИ не произойдет до тех пор, пока пользователь не пройдет назначенный ему курс обучения и не сдаст тестирование по пройденному материалу в ИС ОКЗ.

В случае получения положительного результата по итогам прохождения тестирования происходит активация СКЗИ, и исходящая информация поступает в подпроцесс «Учет СКЗИ».

В случае получения отрицательного результата по итогам прохождения тестирования, требуется повторно ознакомиться с учебными материалами и снова пройти тестирование.

3.4.7. Подпроцесс «Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки»

Входящая информация поступает из подпроцесса «Обработка обращения».

АБ:

- Формирует заявку на сокращение подписки в ИС ОКЗ;
- *В случае, если заявка на сокращение подписки согласована и подписана уполномоченным лицом в ИС ОКЗ,* изымает СКЗИ из аппаратных средств, с которыми они функционировали. При этом СКЗИ считается изъятым из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ, и он полностью отсоединен от аппаратных средств и уничтожает СКЗИ.
  Уничтожение путем физического уничтожения или путем стирания (разрушения), исключающего возможность их использования, а также восстановления. Непосредственные действия по уничтожению конкретного типа СКЗИ регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями ОКЗ АО «Гринатом».
  СКЗИ должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации. Если срок уничтожения эксплуатационной и технической документацией не установлен, то СКЗИ должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия).

Уполномоченное лицо предприятия:

- Получает электронную заявку на сокращение подписки в ИС ОКЗ;
- Подписывает заявку на сокращение подписки, *в случае если заявка им согласована.*

Исходящая информация поступает в подпроцесс «Учет СКЗИ».

3.4.8. Подпроцесс «Учет СКЗИ»

Входящая информация поступает из подпроцесса «Обучение и допуск пользователя» или из подпроцесса «Вывод из эксплуатации, уничтожение СКЗИ».

АБ (в случае если информация поступает из подпроцесса «Обучение и допуск пользователя»):

- Проверяет наличие приказа о допуске пользователя к самостоятельной работе с СКЗИ, вносит его реквизиты в ИС ОКЗ;

- Проверяет наличие у пользователя отметки об успешном прохождении обучения в ИС ОКЗ;
- Проверяет актуальность данных в ИС ОКЗ по АРМ, пользователю и установленным СКЗИ.
- Закрепляет полученную лицензию СКЗИ в ИС ОКЗ за АРМ и пользователем;

На основании заполненных АБ данных в ИС ОКЗ происходит актуализация схемы криптографической защиты информации.

Исходящая информация поступает в подпроцесс «Обеспечение функционирования»

АБ (в случае если информация поступает из подпроцесса «Вывод из эксплуатации, уничтожение СКЗИ»):

- Ставит отметку об уничтожении в ИС ОКЗ.

В случае если подписка сокращена, процесс «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 с использованием информационной системы Органа криптографической защиты» завершается.

3.4.9. Подпроцесс «Обеспечение функционирования»

Входящая информация поступает из подпроцессов «Учет СКЗИ» и «Обработка обращения».

Функционирование и безопасность применения СКЗИ обеспечивается в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам.

Оригиналы выданных сертификатов соответствия требованиям безопасности находятся в ОКЗ АО «Гринатом», копии находятся в ИС ОКЗ.

АБ (в случае если информация поступает из подпроцесса «Обработка обращения»):

- Получает в ИС ОКЗ заявку (не реже раза в год) на проведение проверки порядка использования СКЗИ в соответствии с эксплуатационной и технической документацией. В состав проверки входит:

  соответствие номеров СКЗИ данным в ИС ОКЗ;
  соответствие настроек системного ПО, СКЗИ и мер физической защиты СКЗИ требованиям документации к СКЗИ;
  наличие носителей ключевой информации и их соответствие данным, указанным в ИС ОКЗ;
  наличие актуального приказа о допуске пользователей к самостоятельной работе с СКЗИ.

- В случае необходимости актуализирует данные в ИС ОКЗ.

Аналитик (в случае если информация поступает из подпроцессов «Учет СКЗИ» или «Обработка обращения»):

- Формирует заключение о возможности эксплуатации СКЗИ. Заключение выдается сроком на 1 год, в случае сохранения доверенной среды функционирования СКЗИ, подтвержденной данными в ИС ОКЗ.

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.№15686 Н 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);
- Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» (с пометкой «Для служебного пользования»);

- 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).

5. Порядок внесения изменений

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

6. Контроль и ответственность

6.1 Порядок обязаны соблюдать все следующие участники процесса:

Уполномоченное лицо предприятия;
Аналитик ОКЗ АО «Гринатом»;
Администратор безопасности ОКЗ АО «Гринатом»;
Пользователь.

6.2. Ответственность работников за несоблюдение требований Порядка.

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

7. Перечень приложений

Приложение №1. Матрица ответственности.
Приложение №2. Схема процесса.

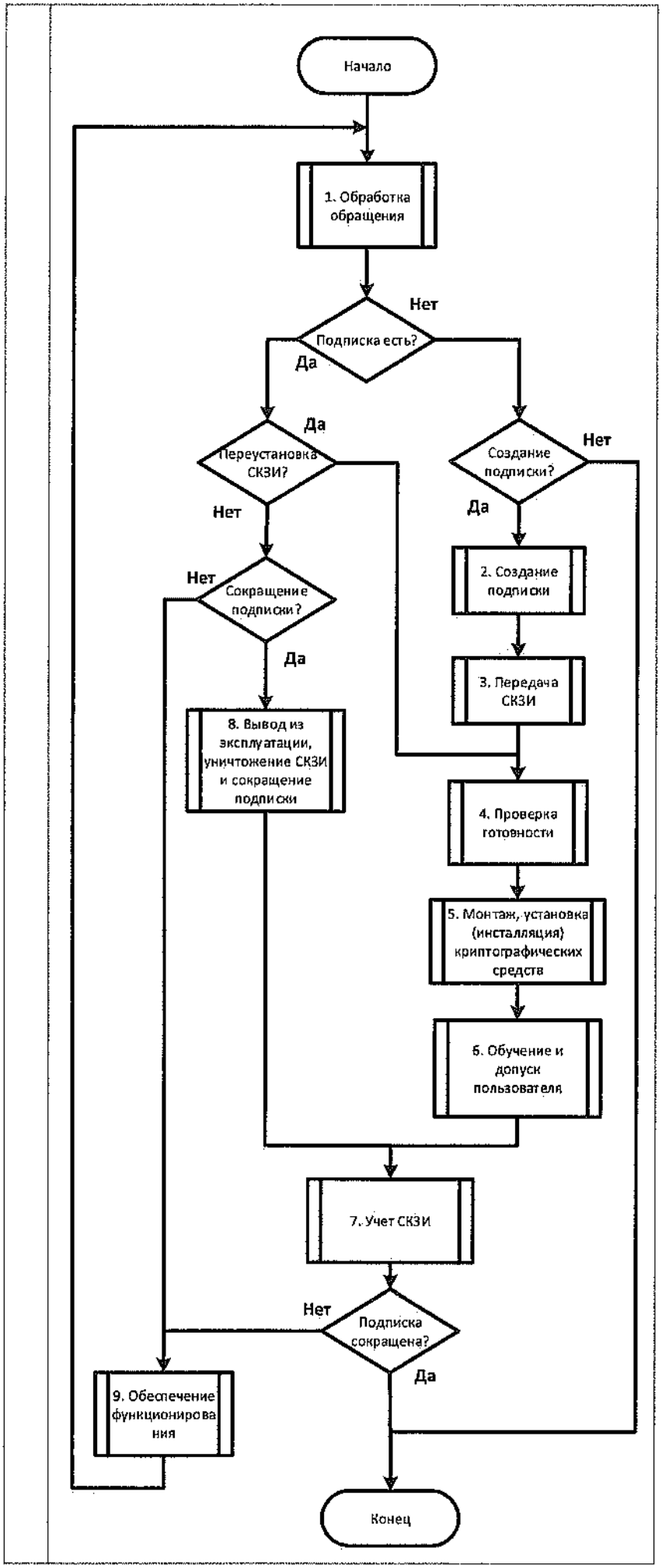
Приложение №1. Матрица ответственности

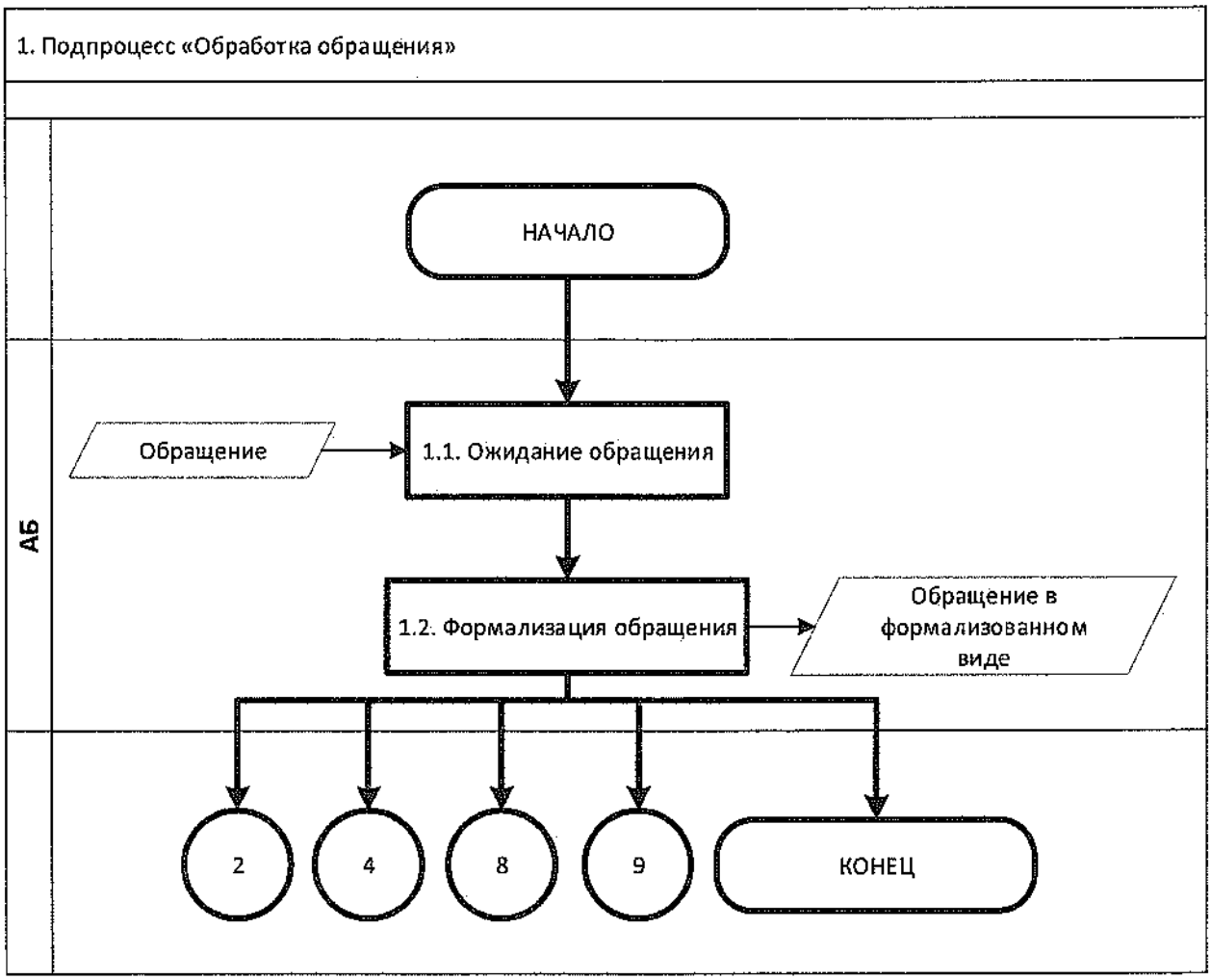
Подпроцессы в составе процесса	Участники процесса			
	Уполномоченное лицо предприятия	Аналитик	АБ	Пользователь
Подпроцесс «Обработка обращения»			О	
Подпроцесс «Создание подписки»	С	С	О	
Подпроцесс «Передача СКЗИ»	Инф.	О		Инф.
Подпроцесс «Проверка готовности»		Инф.	О	
Подпроцесс «Монтаж, установка (инсталляция) криптографических средств»		Инф.	О	
Подпроцесс «Обучение и допуск пользователя»			Инф.	О
Подпроцесс «Учет СКЗИ»		Инф.	О	
Подпроцесс «Обеспечение функционирования»			О	
Подпроцесс «Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки»	С	Инф.	О	

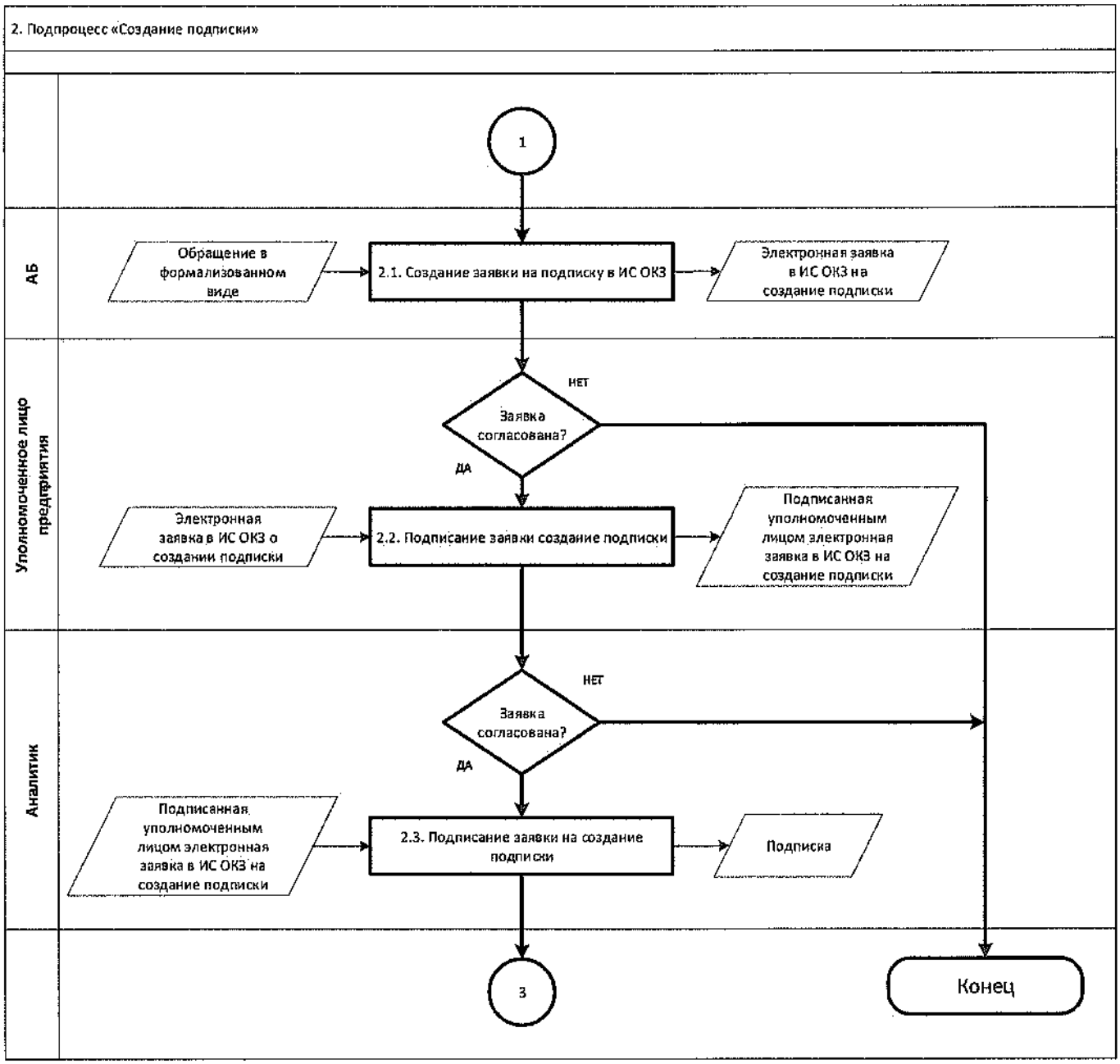
Сокращение	Название роли	Определение	Исполнитель Роли
М	Методолог	Формирует требования к организации деятельности в рамках подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации
И	Интегратор	Интегрирует результаты подпроцесса/процедуры и отвечает за организацию подпроцесса/процедуры, 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

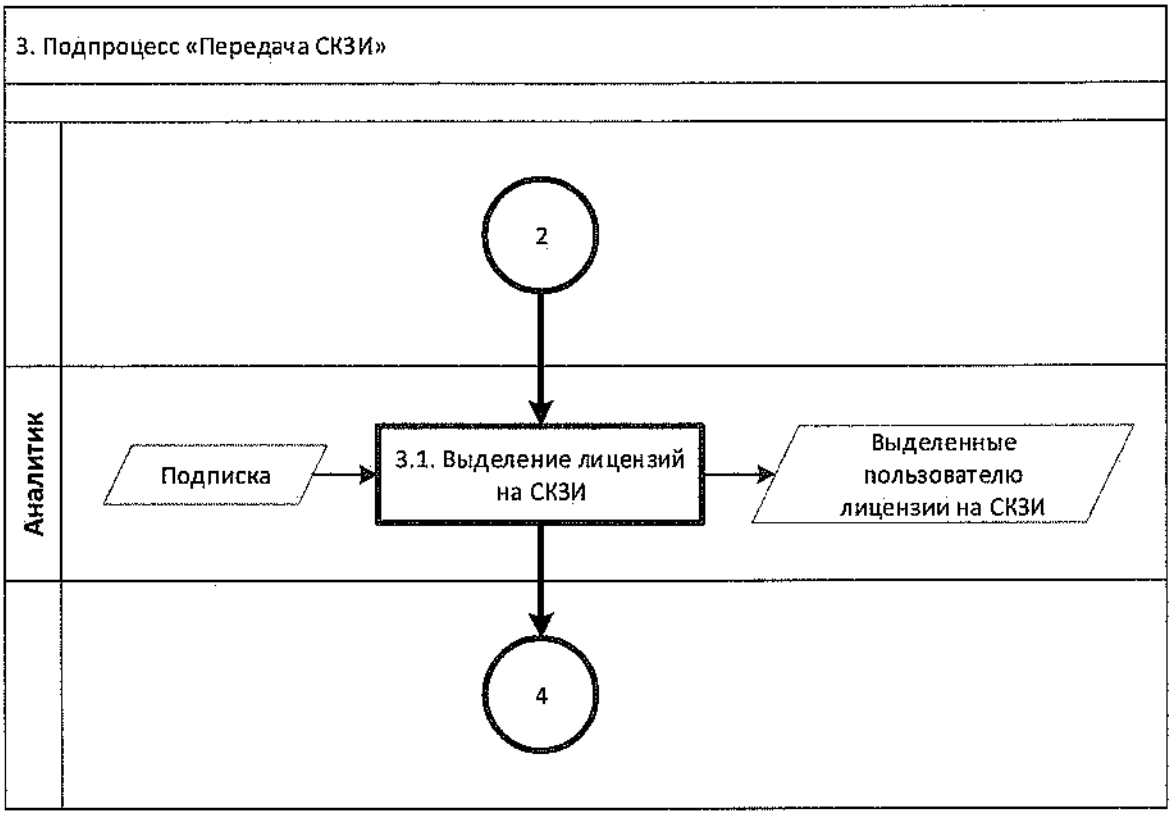
О	Ответственный	Несет ответственность за достижение результата по подпроцессу/процедуре в своей предметной области	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
Утв	Утверждающий	Утверждает - принимает окончательное решение по результату подпроцессу/процедуре	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

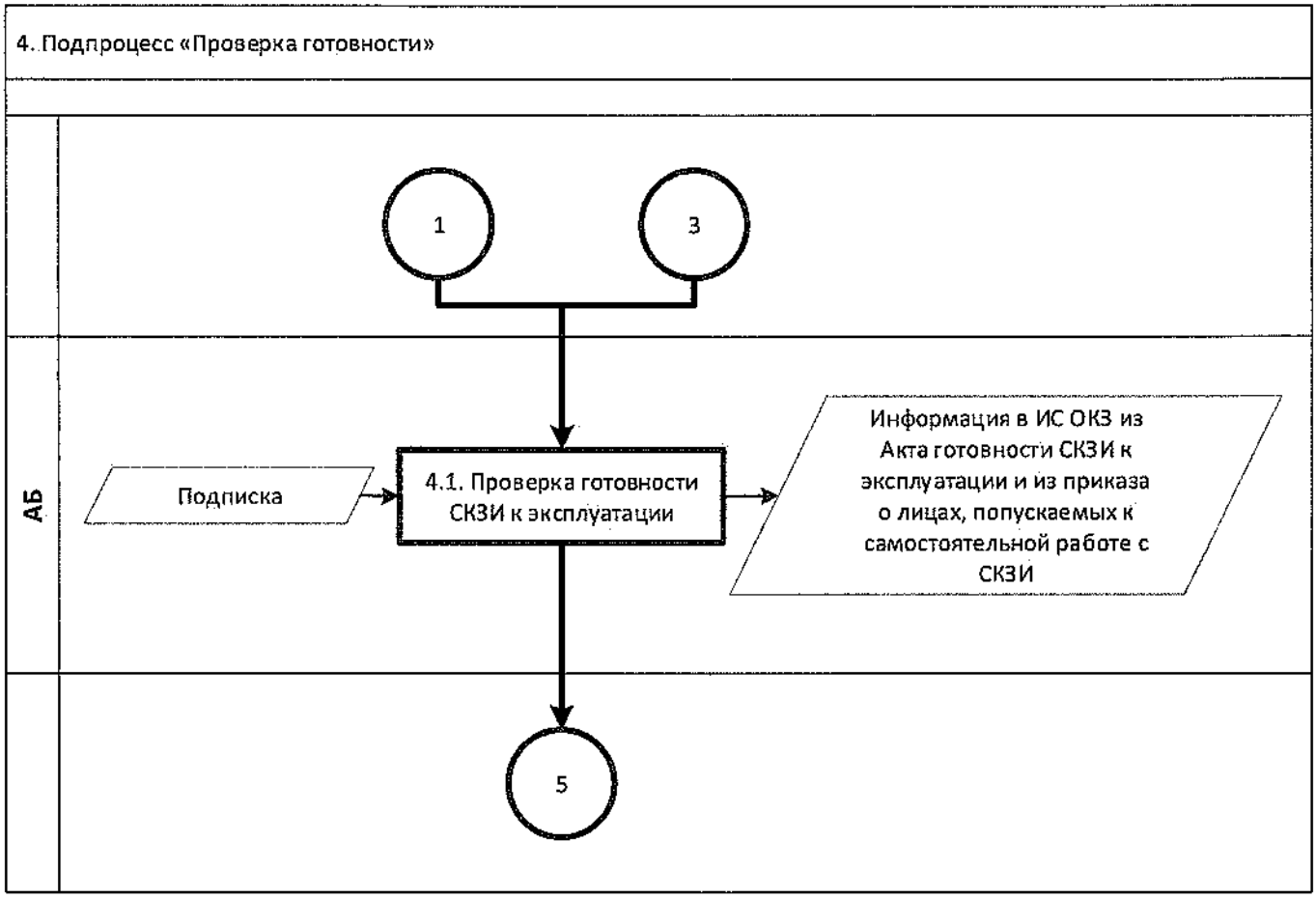
Приложение №2. Схема процесса

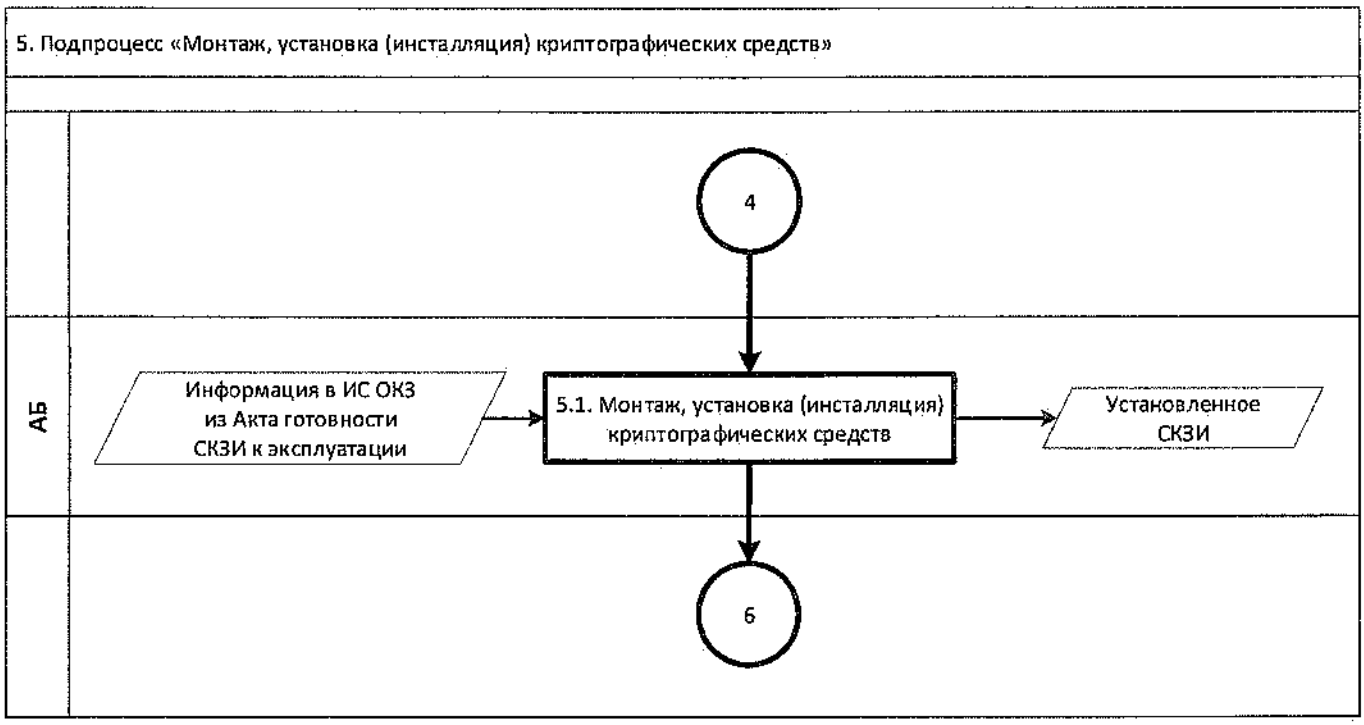

Начало
1. Обработка обращения
Подписка есть?
Нет
Да
Переустановка СКЗИ?
Да
Нет
Создание подписки?
Нет
Да
Сокращение подписки?
Нет
Да
2. Создание подписки
3. Передача СКЗИ
8. Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки
4. Проверка готовности
5. Монтаж, установка (инсталляция) криптографических средств
6. Обучение и допуск пользователя
7. Учет СКЗИ
Подписка сокращена?
Нет
Да
9. Обеспечение функционирования
Конец

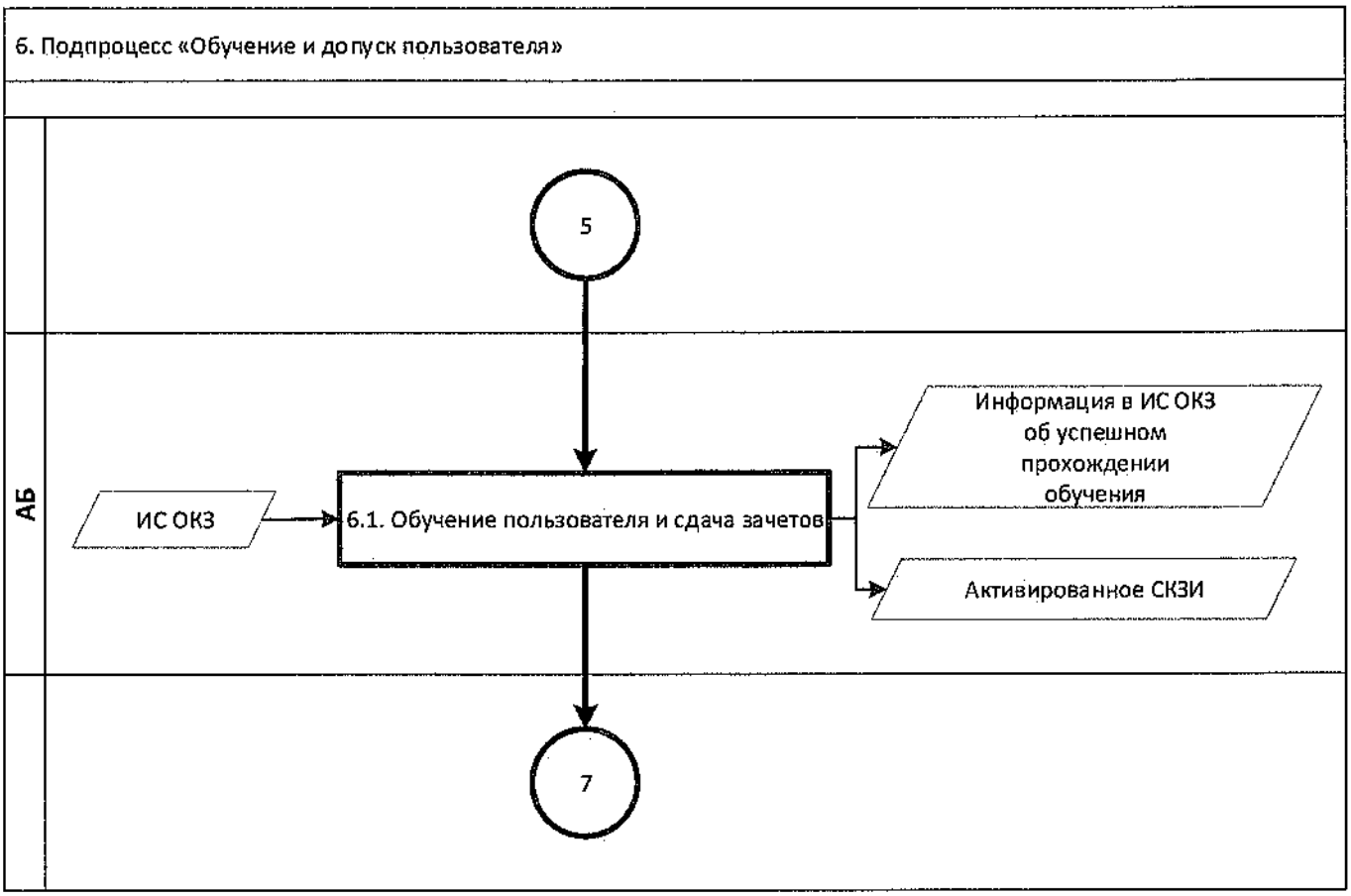

1. Подпроцесс «Обработка обращения»
АБ
НАЧАЛО
Обращение
1.1. Ожидание обращения
1.2. Формализация обращения
Обращение в формализованном виде
2
4
8
9
КОНЕЦ

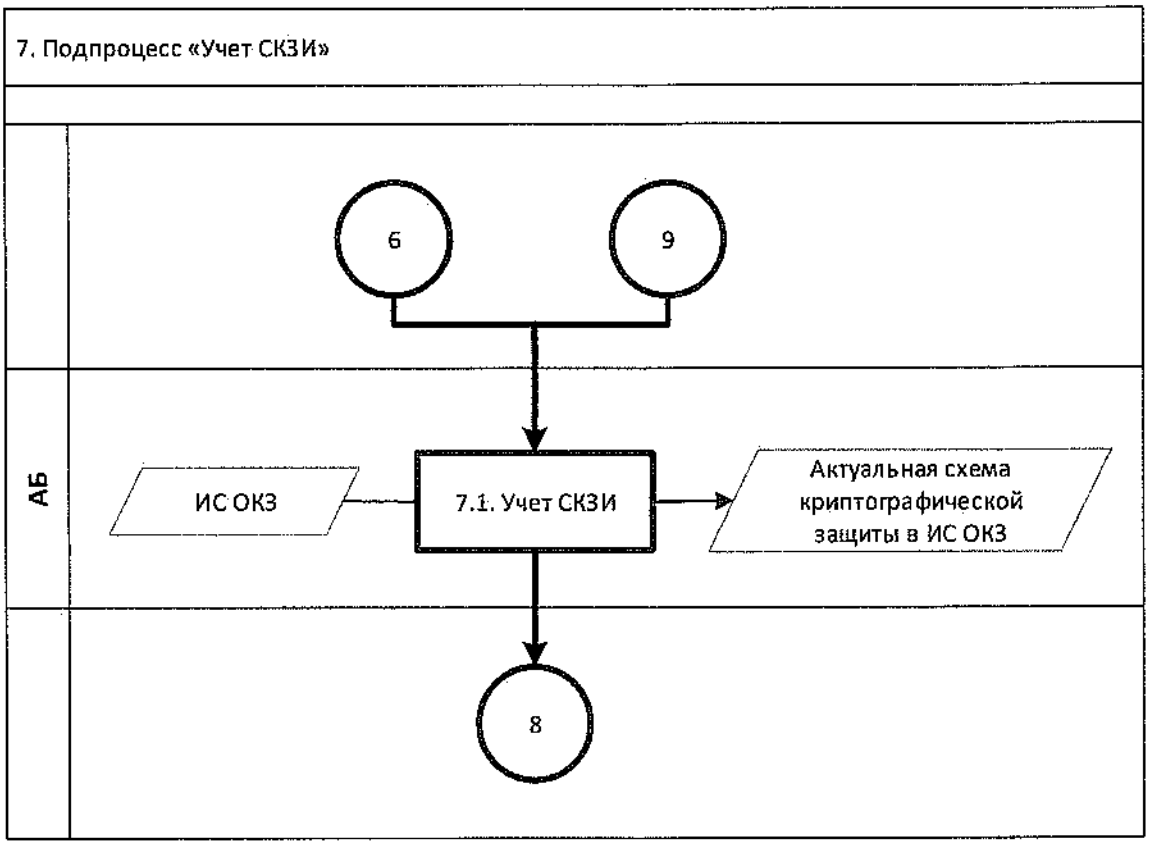

2. Подпроцесс «Создание подписки»
АБ
Уполномоченное лицо предприятия
Аналитик
1
Обращение в формализованном виде
2.1. Создание заявки на подписку в ИС ОКЗ
Электронная заявка в ИС ОКЗ на создание подписки
НЕТ
Заявка согласована?
ДА
Электронная заявка в ИС ОКЗ о создании подписки
2.2. Подписание заявки создание подписки
Подписанная уполномоченным лицом электронная заявка в ИС ОКЗ на создание подписки
НЕТ
Заявка согласована?
ДА
Подписанная уполномоченным лицом электронная заявка в ИС ОКЗ на создание подписки
2.3. Подписание заявки на создание подписки
Подписка
3
Конец

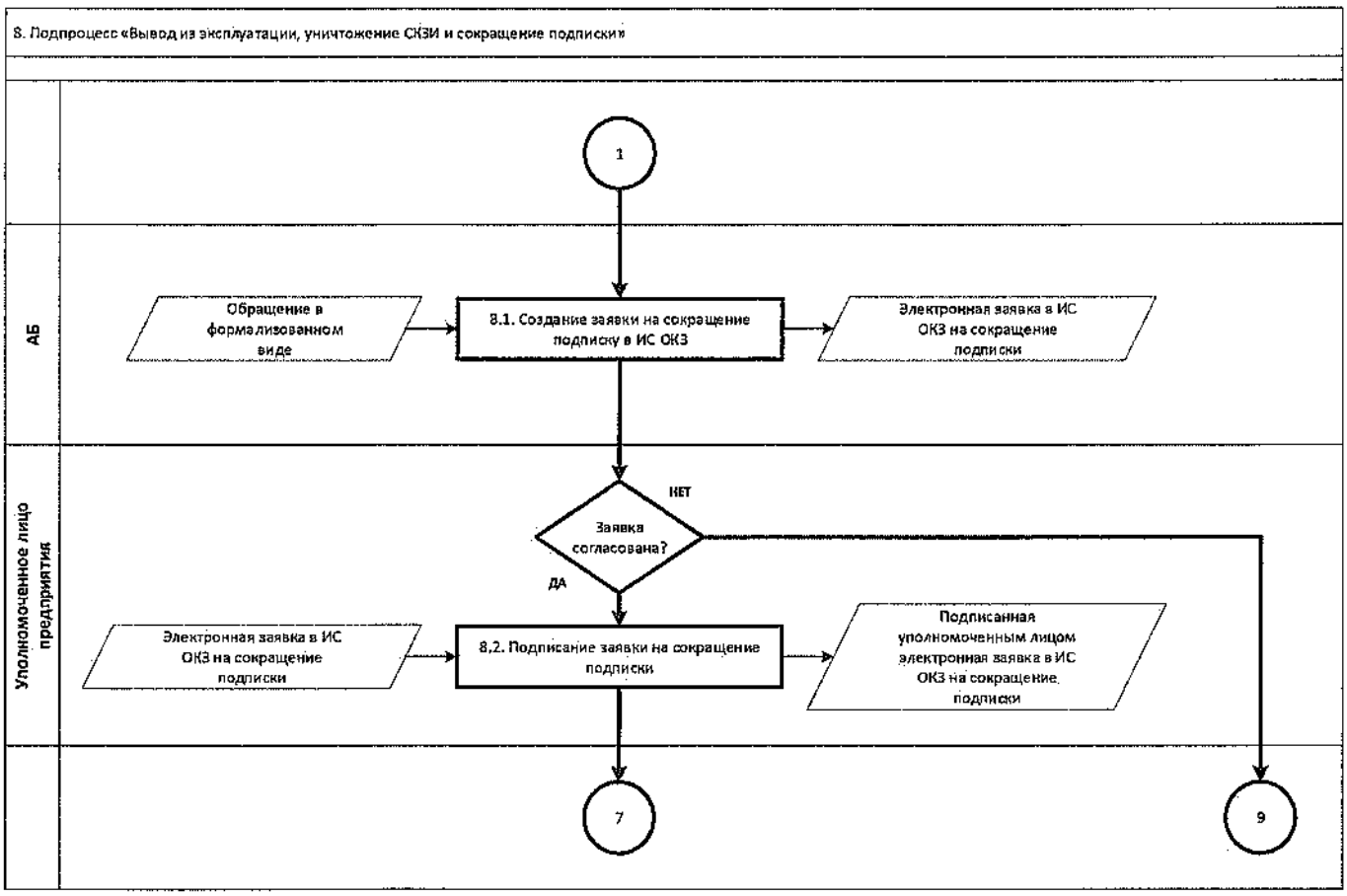

3. Подпроцесс «Передача СКЗИ»
Аналитик
2
Подписка
3.1. Выделение лицензий на СКЗИ
Выделенные пользователю лицензии на СКЗИ
4

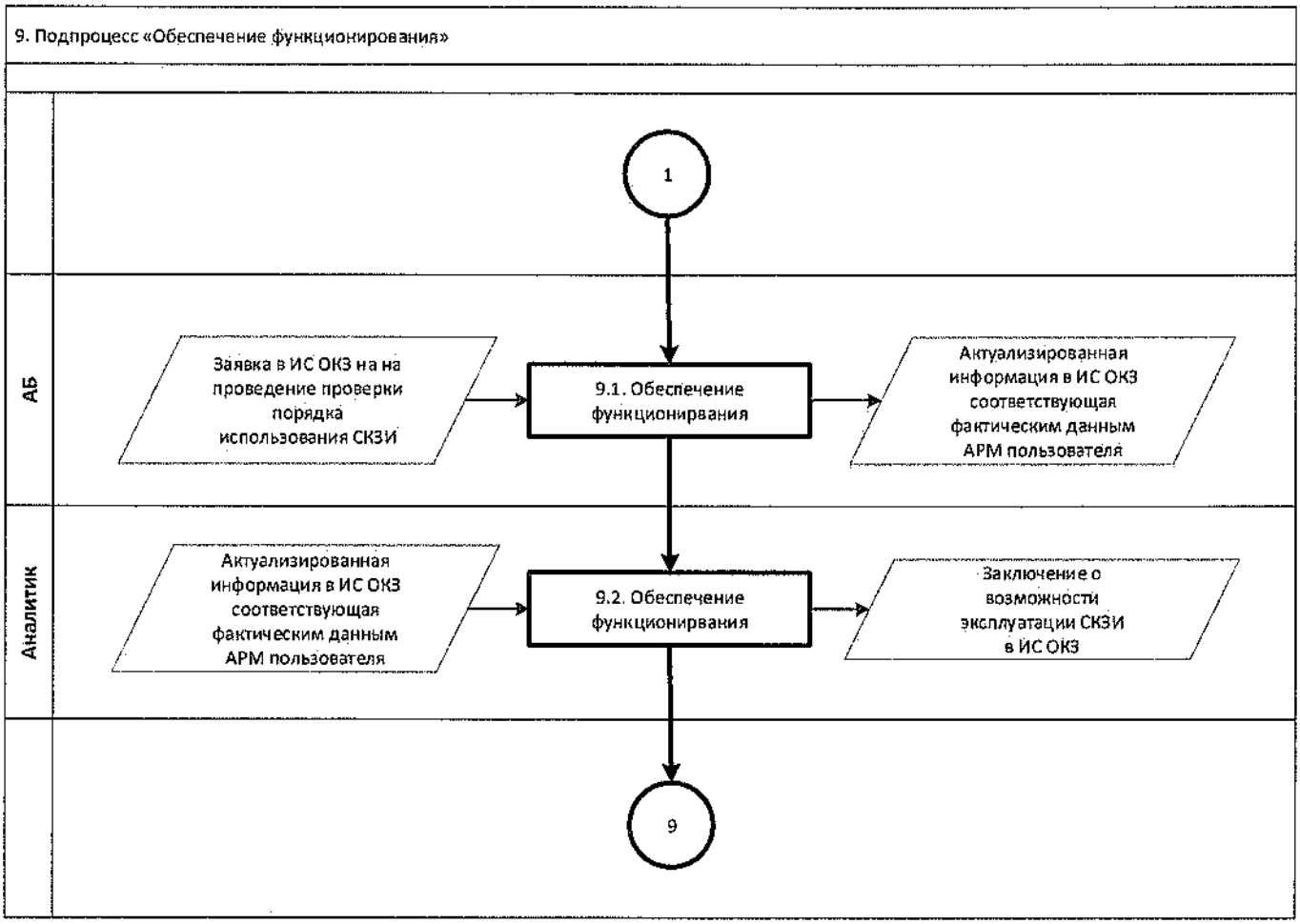

4. Подпроцесс «Проверка готовности»
АБ
1
3
Подписка
4.1. Проверка готовности СКЗИ к эксплуатации
Информация в ИС ОКЗ из Акта готовности СКЗИ к эксплуатации и из приказа о лицах, допускаемых к самостоятельной работе с СКЗИ
5


5. Подпроцесс «Монтаж, установка (инсталляция) криптографических средств»
АБ
4
Информация в ИС ОКЗ
из Акта готовности
СКЗИ к эксплуатации
5.1. Монтаж, установка (инсталляция)
криптографических средств
Установленное
СКЗИ
6


6. Подпроцесс «Обучение и допуск пользователя»
АБ
5
ИС ОКЗ
6.1. Обучение пользователя и сдача зачетов
Информация в ИС ОКЗ об успешном прохождении обучения
Активированное СКЗИ
7


7. Подпроцесс «Учет СКЗИ»
АБ
6
9
ИС ОКЗ
7.1. Учет СКЗИ
Актуальная схема криптографической защиты в ИС ОКЗ
8


8. Подпроцесс «Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки»
АБ
Уполномоченное лицо предприятия
1
Обращение в формализованном виде
8.1. Создание заявки на сокращение подписку в ИС ОКЗ
Электронная заявка в ИС ОКЗ на сокращение подписки
НЕТ
Заявка согласована?
ДА
Электронная заявка в ИС ОКЗ на сокращение подписки
8.2. Подписание заявки на сокращение подписки
Подписанная уполномоченным лицом электронная заявка в ИС ОКЗ на сокращение подписки
7
9


9. Подпроцесс «Обеспечение функционирования»
АБ
Аналитик
1
Заявка в ИС ОКЗ на на проведение проверки порядка использования СКЗИ
9.1. Обеспечение функционирования
Актуализированная информация в ИС ОКЗ соответствующая фактическим данным АРМ пользователя
Актуализированная информация в ИС ОКЗ соответствующая фактическим данным АРМ пользователя
9.2. Обеспечение функционирования
Заключение о возможности эксплуатации СКЗИ в ИС ОКЗ
9

Приложение № 10
к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю
Директор по информационным технологиям

_____ / А.Н. Киселёв /

М.П.

Соглашение
о применении простой и усиленной неквалифицированной электронных подписей
в информационной системе органа криптографической защиты
АО «Гринатом»

Москва 2020 г.

Оглавление

1. Термины и сокращения

В настоящем Соглашении о применении простой и усиленной неквалифицированной электронных подписей в информационной системе органа криптографической защиты АО «Гринатом» (далее – Соглашение) используются следующие термины и сокращения:

Термин	Определение
Участники информационной системы органа криптографической защиты АО «Гринатом»	Юридические и физические лица. Предприятия/ организации Госкорпорации «Росатом». Предприятия/организации зарегистрированные на территории Российской Федерации.
Оператор информационной системы органа криптографической защиты АО «Гринатом»	Многофункциональный общий центр обслуживания Госкорпорации «Росатом»

Сокращение	Расшифровка
АО «Гринатом»	Акционерное общество «Гринатом»
Оператор системы	Оператор информационной системы органа криптографической защиты АО «Гринатом»
Система	Информационная система органа криптографической защиты АО «Гринатом»
Участники системы	Участники информационной системы органа криптографической защиты АО «Гринатом»
Электронный документ	Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

2. Предмет Соглашения

Участники системы соглашаются принимать к исполнению электронные документы, изготовленные при помощи средств вычислительной техники Системы и подписанные простой или усиленной неквалифицированной электронными подписями при соблюдении условий, предусмотренных настоящим Соглашением. Участники системы соглашаются принимать к сведению и исполнению подписанные простой и усиленной неквалифицированной электронными подписями электронные документы в Системе.

3. Общие положения

Участники системы понимают термины, применяемые в настоящем Соглашении, строго в контексте общего смысла Соглашения.

Участники системы принимают, что настоящее Соглашение детализирует положения действующего законодательства Российской Федерации по применению простой и усиленной неквалифицированной электронных подписей.

Настоящее Соглашение регулируется Федеральным законом от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи".

Участники системы принимают, что простая и усиленная неквалифицированная электронные подписи в электронных документах, сформированные владельцем ключей простой и усиленной неквалифицированной электронных подписей, являются равнозначными собственноручной подписи владельца ключей простой и усиленной неквалифицированной электронных подписей Участника системы при выполнении условий, определенных настоящим Соглашением.

Использование в рамках настоящего Соглашения электронных документов, подписанных простой и усиленной неквалифицированной электронными подписями, не изменяет содержания установленных прав и обязанностей Участников системы, содержания документов и правил заполнения их реквизитов.

Участники системы признают, что электронные документы, подписанные простой и усиленной неквалифицированной электронными подписями, в соответствии с условиями настоящего Соглашения являются необходимым и достаточным условием, позволяющим установить, что электронный документ исходит от стороны, его отправившей.

Риск неправомерного подписания электронного документа простой и усиленной неквалифицированной электронными подписями несет Участник системы, уполномоченным лицом которого является владелец соответствующего ключа простой и усиленной неквалифицированной электронных подписей.

Использование электронных документов между Участниками системы при осуществлении взаимоотношений не отменяет использование иных способов связи для обмена документами и сообщениями между Участниками системы. **Ключи простой и неквалифицированной электронных подписей**

Ключом простой электронной подписи является сочетание 2 элементов - идентификатора и пароля ключа. Участники системы принимают, что идентификатор ключа простой электронной подписи является уникальным логином владельца ключа в Системе и однозначно идентифицирует владельца ключа простой электронной подписи, а пароль ключа аутентифицирует его в Системе.

Ключами усиленной неквалифицированной электронной подписи являются ключ электронной подписи и ключ проверки электронной подписи в терминах Федерального закона от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи".

3.1.Средства простой и усиленной неквалифицированной электронных подписей

Участники системы принимают в качестве средства простой электронной подписи программно-технические средства Системы при выполнении функций создания и проверки простой электронной подписи в электронном документе.

Участники системы принимают в качестве средства усиленной неквалифицированной электронной подписи средство криптографической защиты информации, к которому обращается Система при выполнении функций создания и проверки усиленной неквалифицированной электронной подписи в электронном документе.

Электронный документ считается подписанным простой электронной подписью или усиленной неквалифицированной электронной подписью, если ключи простой электронной подписи или усиленной неквалифицированной электронной подписи применяются в соответствии с правилами, установленными Оператором системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

3.2.Условия равнозначности простой и усиленной неквалифицированной электронных подписей собственноручной

Информация в электронной форме, подписанная простой или усиленной неквалифицированной электронными подписями, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Простая электронная подпись в электронном документе равнозначна собственноручной подписи владельца ключа простой электронной подписи при одновременном соблюдении следующих условий:

лицо, подписывающее электронный документ, идентифицировано по идентификатору ключа простой электронной подписи;

обеспечена конфиденциальность ключа простой электронной подписи лица, использующего ключ простой электронной подписи.

Усиленная неквалифицированная электронная подпись в электронном документе равнозначна собственноручной подписи владельца ключа усиленной неквалифицированной электронной подписи если обеспечена конфиденциальность ключа усиленной неквалифицированной электронной подписи лица, использующего ключ усиленной неквалифицированной электронной подписи.

Проверка усиленной неквалифицированной электронной подписи осуществляется средствами сервиса проверки усиленной неквалифицированной электронной подписи. Для проверки Участник системы через ресурс http://ndss.rosatom.local/svs отправляет запрос на проверку электронной подписи в электронном документе.

4. Обязанности владельцев ключей простой и усиленной неквалифицированной электронных подписей

Владелец ключа простой и усиленной неквалифицированной электронных подписей обязан:

обеспечивать конфиденциальность ключей простой и усиленной неквалифицированной электронных подписей;

немедленно информировать Оператора системы о факте компрометации ключей простой и усиленной неквалифицированной электронных подписей;

немедленно прекратить использование ключей простой и усиленной неквалифицированной электронных подписей в случае их компрометации;

соблюдать правила работы в Системе;

содержать в исправном состоянии программно-технические средства, которые подключены к Системе, принимать меры для предотвращения несанкционированного доступа к данным компьютерам, а также в помещения, в которых они установлены.

5. Ответственность Участников системы

За невыполнение или ненадлежащее выполнение обязательств по настоящему Соглашению Участники системы несут ответственность в соответствии с действующим законодательством Российской Федерации.

6. Форс-мажор

Участники системы освобождаются от ответственности за частичное или полное неисполнение принятых на себя обязательств вследствие возникновения обстоятельств непреодолимой силы.

Под обстоятельствами непреодолимой силы понимаются обстоятельства, которые возникли после присоединения к настоящему соглашению в результате непредвиденных и неотвратимых стороной событий чрезвычайного характера, к числу которых относятся: пожар, стихийное бедствие, война, какие бы то ни было военные действия, блокады, запрещение определенных коммерческих операций, а также в случае появления акта государственного органа, в результате издания которого исполнение обязательств Участников системы становится невозможным полностью или частично.

При наступлении обстоятельств непреодолимой силы срок исполнения обязательств отодвигается соразмерно времени, в течение которого будут действовать такие обстоятельства и их последствия.

Если эти обстоятельства и их последствия будут продолжаться свыше 30 (тридцати) дней, то каждый из Участников системы будет иметь право отказаться от дальнейшего исполнения обязательств по настоящему Соглашению, и в этом случае ни один из Участников системы не будет иметь права на возмещение другими Участниками системы возможных убытков.

7. Разрешение споров

Все споры, разногласия, требования, возникающие из данного Соглашения или касающиеся его нарушения, прекращения, недействительности, подлежат разрешению в рамках согласительной комиссии, действующей в соответствии с порядком, определенным настоящим Соглашением.

Участники системы обязуются способствовать работе комиссии и не допускать отказа от предоставления необходимых документов.

8. Порядок заключения Соглашения

Участник системы заключает настоящее Соглашение не иначе как путем присоединения к Соглашению в целом.

Присоединение к настоящему Соглашению осуществляется путем подписания и предоставления Участником системы в адрес АО «Гринатом» двух экземпляров заявления о присоединении к Соглашению по форме, определенной в приложении к настоящему Соглашению. АО «Гринатом» регистрирует Участника системы в реестре и направляет один экземпляр заявления с отметкой о регистрации в адрес

Участника системы. АО «Гринатом» вправе отказать любому Участнику системы в регистрации заявления о присоединении к Соглашению путем возврата заявления о присоединении в адрес Участника системы с отметкой «Отказано в регистрации».

С момента регистрации заявления о присоединении к Соглашению сторона, подавшая заявление, считается присоединившейся к Соглашению.

Факт присоединения Участника системы к Соглашению является полным принятием им условий настоящего Соглашения и всех его приложений в редакции, действующей на момент регистрации заявления о присоединении в реестре АО «Гринатом». Сторона, присоединившаяся к Соглашению, принимает дальнейшие изменения (дополнения), вносимые в Соглашение и его приложения, в соответствии с условиями настоящего Соглашения.

8.1.Срок действия соглашения

После присоединения в установленном порядке Участники системы вступают в соответствующие договорные отношения на неопределенный срок.

Участник системы имеет право отказаться от Соглашения, письменно уведомив об этом Оператора системы за один месяц до принятия решения об отказе от Соглашения.

Отказ от Соглашения не освобождает Участника системы от исполнения обязательств, возникших до указанного прекращения, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

8.2.Изменение условий соглашения

Внесение изменений (дополнений) в Соглашение, в том числе в приложения к нему, производится АО «Гринатом» и утверждается приказом.

Уведомление Участников системы о внесении изменений (дополнений) в Соглашение осуществляется путем размещения указанных изменений (дополнений) на сайте https://crypto.rosatom.ru.

Все изменения (дополнения), вносимые в Соглашение и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными для Участников системы по истечении 30 (тридцати) календарных дней с даты уведомления Участников системы.

Любые изменения и дополнения в Соглашении с момента вступления в силу равно распространяются на всех Участников системы, присоединившихся к Соглашению, в том числе присоединившихся к Соглашению ранее даты вступления изменений (дополнений) в силу.

9. Дополнительные условия

Все приложения к настоящему соглашению, оформленные надлежащим образом, являются его неотъемлемой частью.

Участники системы обязаны незамедлительно извещать Оператора системы и друг друга об изменении почтовых, платежных, отгрузочных и иных, необходимых для исполнения настоящего соглашения реквизитов. Все риски, связанные с этим, лежат на не уведомившем Участнике системы.

Участники системы не вправе передавать права и обязанности по данному соглашению третьим лицам без согласия Оператора системы.

Во всем остальном, что не предусмотрено настоящим соглашением, Участники системы руководствуются действующим законодательством Российской Федерации.

10. Юридический адрес АО «Гринатом»

Полное наименование: Акционерное общество «Гринатом»
Краткое наименование: АО «Гринатом»
Место нахождения: 119017, Россия, г. Москва, ул. Большая Ордынка, дом 24
Почтовый адрес: 115114, Россия, г. Москва, 1-й Нагатинский проезд, дом 10, стр. 1
ОГРН: 1097746819720
ИНН: 7706729736
КПП: 770601001
Расчетный счет: 40702810038110013312
Банк: Московский банк Сбербанка России ПАО
Корреспондентский счет: 30101810400000000225 в ПЕРУ Московского ГТУ Банка России
БИК: 044525225
ОКПО: 64509942
ОКАТО: 45286596000
ОКТМО: 45384000
Телефон: + 7 (499) 949-49-19
Адрес электронной почты: dogovor@greenatom.ru

Директор по информационным технологиям _____ / А.Н. Киселёв /

М.П.

Приложение №1 к Соглашению,
утв. Приказом АО «Гринатом» от __.__.____ № _____

ЗАЯВЛЕНИЕ
о присоединении к соглашению о применении простой и усиленной неквалифицированной электронных подписей в информационной системе органа криптографической защиты АО «Гринатом»

_____
(наименование организации, включая организационно-правовую форму)

в лице_____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании_____

полностью и безусловно присоединяется к Соглашению о применении простой и усиленной неквалифицированной электронных подписей в информационной системе органа криптографической защиты АО «Гринатом», условия которого определены АО «Гринатом» и опубликованы на сайте по адресу https://crypto.rosatom.ru

Уполномоченное должностное лицо

_____ _____ / _____ /
(подпись) (ФИО)

М.П.

Реквизиты организации:
Полное наименование:
Место нахождения:
Почтовый адрес:
ОГРН:
ИНН:
КПП:
Расчетный счет:
Банк:
Кор. счет:
БИК:
ОКПО:
ОКАТО:
Телефон/факс:
e-mail:

Данное Заявление о присоединении к Соглашению о применении простой и усиленной неквалифицированной электронных подписей в информационной системе органа криптографической защиты АО «Гринатом» зарегистрировано в реестре АО «Гринатом». Заявление о присоединении к соглашению подается в АО «Гринатом» в двух экземплярах. После регистрации Заявления в АО «Гринатом» один экземпляр предоставляется заявителю.

Регистрационный № _____ от «_____» _____ 20___ г.

_____ _____/_____/
Должность М.П.

Приложение №2 к Соглашению,
утв. Приказом АО «Гринатом» от __.__.____ № _____

Порядок рассмотрения конфликтных ситуаций, связанных с подлинностью электронных документов в информационной системе органа криптографической защиты АО «Гринатом»

1. Общие положения.

В данном документе описан порядок разрешения конфликтных ситуаций между Участниками системы, присоединившимися к Соглашению о применении простой и усиленной неквалифицированной электронных подписей в информационной системе органа криптографической защиты АО «Гринатом».

Рассматриваются конфликтные ситуации двух типов:

отказ Стороны от авторства электронного документа (Сторона утверждает, что она не подписывала принятый другой Стороной электронный документ, а другая Сторона утверждает обратное);

отказ Стороны от факта получения электронного документа (Сторона утверждает, что посланный ею электронный документ был принят другой Стороной, а другая Сторона это отрицает).

1.1. Сторона – инициатор рассмотрения конфликтной ситуации (далее – Заявитель) должна подготовить и направить другой Стороне (далее – Ответчик) документ (заявление), подписанный уполномоченным должностным лицом с изложением обстоятельств случившегося. До подачи заявления Заявителю рекомендуется убедиться в отсутствии несанкционированных действий со стороны персонала. В заявлении должно быть указано:

наименование организации;

дата и номер оспариваемого электронного документа;

тип и характер претензии.

1.2. На основании заявления Ответчик в течение 5 (пяти) рабочих дней рассматривает заявление и либо удовлетворяет претензию Заявителя, либо передает Заявителю письменный отказ в удовлетворении претензии с обоснованием причины отказа.

1.3. В случае несогласия с отказом Заявитель направляет Ответчику письменное заявление о своем несогласии и требованием формирования согласительной комиссии для рассмотрения конфликтной ситуации.

1.4. На основании данного заявления не позднее 15 (пятнадцати) календарных дней с момента его получения совместным решением Сторон создается согласительная комиссия для рассмотрения возникшей конфликтной ситуации. Представителями в согласительной комиссии от Заявителя, Ответчика и Оператора системы могут быть лица как из числа сотрудников этих организаций (в равном количестве от каждой Стороны), так и иных компетентных организаций. В последнем случае их полномочия определяются доверенностями. Состав согласительной комиссии согласовывается Сторонами и утверждается двусторонним актом.

1.5. Рекомендуется следующий состав экспертной комиссии:

абоненты, участвовавшие в обмене электронными документами, со стороны Заявителя и Ответчика;

представители подразделений безопасности и технических подразделений Заявителя и Ответчика.

Кроме того, в случае необходимости могут привлекаться Оператор системы, независимые эксперты и технические специалисты, в том числе из организаций-изготовителей программного обеспечения.

1.6. В течение 5 (пяти) рабочих дней с момента формирования согласительной комиссии Стороны предоставляют согласительной комиссии следующие материалы:

заверенные копии Заявлений о присоединении к соглашению о применении простой и усиленной неквалифицированной электронных подписей в информационной системе органа криптографической защиты АО «Гринатом»;

заявление Заявителя с изложением сути претензии;

письменный отказ Ответчика в удовлетворении претензии Заявителя;

реквизиты оспариваемых электронных документов в Системе, подписанных простой или усиленной неквалифицированной электронной подписью.

1.7 Стороны обязаны способствовать работе согласительной комиссии и своевременно предоставлять все необходимые материалы.

1.8 Согласительная комиссия делает запрос Оператору системы на предоставление технического заключения о корректности работы Системы в промежуток времени возникновения конфликтной ситуации и корректности действий пользователей и администраторов Системы с электронным документом (далее – Заключение). К запросу Оператору системы на предоставление Заключения согласительная комиссия прикладывает документы, указанные в п. 1.6.

1.9 В течение 5 (пяти) рабочих дней с момента получения запроса и документов, указанных в п. 1.6, с помощью средств Системы Оператор системы предоставляет согласительной комиссии Заключение (порядок предоставления Заключения указан в п.2).

1.10 Согласительная комиссия не позднее 10 (десяти) рабочих дней с момента получения Заключения Оператора системы большинством голосов членов принимает решение о виновности той или иной Стороны и оформляет его в виде акта, который оформляется на бумаге и подписывается всеми членами согласительной комиссии.

1.8. Акт согласительной комиссии является окончательным и пересмотру не подлежит. Предписываемые данным актом действия обязательны для Сторон.

1.9. Акт согласительной комиссии является основанием для предъявления претензий к лицам, виновным в возникновении конфликта.

1.10. В случае невозможности принятия решения согласительной комиссией, а также в случае несогласия одной из Сторон с принятым согласительной комиссией решением, уклонения одной из Сторон от формирования согласительной комиссии, препятствования участию второй Стороны в работе согласительной комиссии, Стороны вправе разрешать спор путем арбитража, администрируемого Российским арбитражным центром при автономной некоммерческой организации «Российский институт современного арбитража» в соответствии с Правилами Отделения Российского арбитражного центра при автономной некоммерческой организации

«Российский институт современного арбитража» по разрешению споров в атомной отрасли.

Стороны соглашаются, что для целей направления письменных заявлений, сообщений и иных письменных документов будут использоваться следующие адреса электронной почты:

Исполнитель: адрес, указанный в ст. 10 Соглашения.

Заказчик: адрес, указанный в Приложении №1 к Соглашению.

В случае изменения указанного выше адреса электронной почты Сторона обязуется незамедлительно сообщить о таком изменении другой Стороне, а в случае, если арбитраж уже начат, также Отделению Российского арбитражного центра при автономной некоммерческой организации «Российский институт современного арбитража» по разрешению споров в атомной отрасли. В ином случае Сторона несет все негативные последствия направления письменных заявлений, сообщений и иных письменных документов по неактуальному адресу электронной почты.

Стороны принимают на себя обязанность добровольно исполнять арбитражное решение.

Стороны прямо соглашаются, что в случае, если заявление об отводе арбитра не было удовлетворено Президиумом Российского арбитражного центра в соответствии с Правилами Отделения Российского арбитражного центра при автономной некоммерческой организации «Российский институт современного арбитража» по разрешению споров в атомной отрасли, Сторона, заявляющая отвод, не вправе подавать в компетентный суд заявление об удовлетворении отвода.

Стороны прямо соглашаются, что в случае, если Состав арбитража выносит постановление о наличии у него компетенции в качестве вопроса предварительного характера, Стороны не вправе подавать в компетентный суд заявление об отсутствии у Состава арбитража компетенции.

Стороны прямо соглашаются, что арбитражное решение является окончательным для Сторон и отмене не подлежит.

В случаях, предусмотренных статьёй 25 Правил Отделения Российского арбитражного центра при автономной некоммерческой организации «Российский институт современного арбитража» по разрешению споров в атомной отрасли, Сторонами может быть заключено соглашение о рассмотрении спора в рамках ускоренной процедуры арбитража передать спор на рассмотрение в Третейский суд Госкорпорации «Росатом».

2. Порядок предоставления Заключения Оператором системы

2.1. Порядок предоставления Заключения Оператором Системы в связи с конфликтной ситуацией, связанной с отказом Стороны от факта направления/подписания электронного документа/порядок предоставления Заключения Оператором системы в связи с конфликтной ситуацией, связанной с отказом Стороны от факта получения электронного документа.

2.1.1. Средствами Системы проверяется корректность работы Системы в промежуток времени возникновения конфликтной ситуации и корректность действий пользователей и администраторов Системы с данным электронным документом по журналам аудита событий.

2.1.2. По результатам рассмотрения предоставленных документов, указанных в п. 1.6, и с помощью средств Системы Оператор системы предоставляет согласительной комиссии Заключение.

Приложение № 1
к Договору присоединения № 22/2143-Д от 6 июля 2018 г.
УТВЕРЖДАЮ
Директор по информационным технологиям
АО «Гринатом»
_____ / А.Н. Киселев /
М.П.

Предоставление/отключение доступа/изменение прав доступа пользователей к информационному ресурсу

В соответствии с Приказом ГК Росатом 1/1517-П от 30.12.2019 года заявка на массовое подключение оформляется в случае подключения 5 (пяти) и более пользователей.

Наименование информационного ресурса (полное наименование)	Срок (период), на который предоставляется доступ	Согласование владельца ресурса		Согласование администратора информационной безопасности ИС	
		Расшифровка подписи и дата подписания	Подпись	Расшифровка подписи и дата подписания	Подпись
Информационная система Органа криптографической защиты/ Платформа доверенных сервисов Госкорпорации "Росатом"	Бессрочно	Волков С.П. Дата		Тихонов А.В. Дата	

	Фамилия Имя Отчество - полностью	Табельный номер	Должность	Организация (полное наименование)	Подразделение	Гражданство (РФ или иное)	Login	e-mail	Месторасположение	Контактный телефон	Действие	Название роли	Техническое имя
1												Пользователь	
2													
3													
4													
5													
6													
7													
8													
9													
10													

В соответствии с п. 3.8.5 Единых отраслевых методических указаний по предоставлению доступа пользователей к централизованным информационным системам ГК Росатом и организаций ГК Росатом, утвержденным Приказом ГК Росатом № 1/577-П от 27.06.2017 года, ответственность за ознакомление и соблюдение требований данных Методических указаний пользователями, перечисленными в заявке на массовое подключение, возлагается на руководителя организации пользователей.

Специалист отдела кадров организации (ПЕЧАТЬ)	Подпись	Расшифровка подписи и дата подписания / М.П. организации
Руководитель пользователей /Руководитель организации	Подпись	Расшифровка подписи и дата подписания
Согласование АБ ОКЗ организации/АБ ОКЗ (GEN.23)	Подпись	Расшифровка подписи и дата подписания
Согласование ДЗГТИ ГК Росатом для пользователей, не являющихся гражданами Российской Федерации	Подпись	Расшифровка подписи и дата подписания

Отсутствие проставленных подписей, их расшифровок и может являться основанием для отклонения заявки на предоставление доступа к ИС

Примечания:

Все строки подлежат обязательному заполнению, если не указано иное. Все сведения, кроме подписей, расшифровок и дат, вносятся машинописным способом, внесение изменений и исправлений не допускается

Приложение № 12 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю

Директор по информационным технологиям

АО «Гринатом»

_____ / А.Н. Киселёв /

М.П.

ПОРЯДОК

предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом»

Москва 2020 г.

Содержание

1. Назначение и область применения

1.1. Настоящий Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (далее - Порядок) разработан для установления последовательности действий по процессу группы процессов управления информационными технологиями с целями установления правил и условий предоставления и пользования услугами Корпоративного удостоверяющего центра Госкорпорации «Росатом» по созданию, выдаче и управлению квалифицированными сертификатами ключей проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом».

Информация о Корпоративном удостоверяющем центре Госкорпорации «Росатом» размещена на официальном сайте https://crypto.rosatom.ru.

1.2. Соблюдение Порядка является обязательным для предприятий/ организаций, использующих автоматизированные информационные системы, в которых применяются сертификаты ключей проверки электронных подписей, создаваемые Корпоративным удостоверяющим центром Госкорпорации «Росатом».

Требования Порядка обязательны для сотрудников, выполняющих следующие функциональные роли:

1. Подписчик.
2. Куратор от организации.
3. Уполномоченное лицо от организации.
4. Администратор безопасности ОКЗ.
5. Оператор УЦ от ПУСК ПДС.

1.3. Ответственным за актуализацию Порядка и контроль его исполнения в соответствии с требованиями Положения о системе регламентирующих документов Госкорпорации «Росатом» является директор Департамента по информационным технологиям Блока по ИТ АО «Гринатом».

1.4. Актуальная версия Порядка размещена по адресу: https://crypto.rosatom.ru.

2. Термины, сокращения и аббревиатуры

2.1. Термины и определения

Термин	Определение
Администратор безопасности ОКЗ	Уполномоченный работник АО «Гринатом» (по договору) или уполномоченный работник организации-заказчика, наделенный полномочиями по вручению сертификатов ключей проверки электронных подписей от имени удостоверяющего центра.
Аккредитация удостоверяющего центра	Признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

Владелец сертификата ключа проверки электронной подписи	Лицо, которому в соответствии настоящим Порядком, с учетом Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», создан квалифицированный или неквалифицированный сертификат ключа проверки 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 Федеральным законом №63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным центром сертификации.
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.
Ключевой носитель	Отчуждаемый носитель информации, предназначенный для хранения ключа электронной подписи и ключа проверки электронной подписи.
Корпоративный удостоверяющий центр Госкорпорации «Росатом»	Удостоверяющий центр АО «Гринатом».
Куратор от организации	Сотрудник организации-заказчика, который дополняет заявки на создание подписки, на обеспечение Сертификата кадровыми данными Подписчика.
Оператор Удостоверяющего центра от подсистемы управления сервисами и коннекторами Платформы доверенных сервисов Госкорпорации «Росатом»	Сотрудник Корпоративного удостоверяющего центра Госкорпорации «Росатом», который создает Сертификаты.
Подписка	Заказ предприятия в ПДС в соответствии с условиями договора присоединения на обеспечение сертификатами или средствами криптографической защиты и информации. Подписка подразумевает владение Подписчиком одним действующим сертификатом выбранного шаблона.
Подписчик	Физическое лицо, для которого оформлена подписка на обеспечение сертификатом и (или) лицензией на средство криптографической защиты информации (обладает учётной записью в домене GK/inter, создаёт обращения, получает Сертификаты).
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.
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.
Уполномоченное лицо от организации	Работник юридического лица, указанный в ЕГРЮЛ и имеющий возможность обращаться в Удостоверяющий центр от имени юридического лица, либо работник имеющий право действовать от имени юридического лица на основании доверенности (согласовывает и подписывает электронные заявки в ПДС на создание и сокращение подписки организации).
Участники электронного взаимодействия	Государственные органы, органы местного самоуправления, организации, а также граждане осуществляющие обмен информацией в электронной форме.
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.

В Порядке используются термины, установленные Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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

Термин	Определение
ЕГРЮЛ	Единый государственный реестр юридических лиц
ЕСИА	Единая система идентификации и аутентификации
ИАСУП	Информационная автоматизированная система управления персоналом Госкорпорации «Росатом»
КУЦ	Корпоративный удостоверяющий центр Госкорпорации «Росатом»
МВД	Министерство внутренних дел Российской Федерации
ПДС	Платформа доверенных сервисов Госкорпорации «Росатом»
ПУСК ПДС	Подсистема управления сервисами и коннекторами Платформы доверенных сервисов Госкорпорации «Росатом»
ПФР	Пенсионный фонд России
Сертификат	Квалифицированный сертификат ключа проверки электронной подписи
СМЭВ	Система межведомственного электронного взаимодействия
СНИЛС	Страховой номер индивидуального лицевого счёта
СУ ИТ	Система управления информационными технологиями
УЦ	Удостоверяющий центр
ФНС	Федеральная налоговая служба
ЭП	Электронная подпись

3. Описание процесса

Описание процесса предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки ЭП с использованием Платформы доверенных сервисов Госкорпорации «Росатом».

3.1. Описание подпроцессов

3.1.1. Подпроцесс «Обработка обращения»

Инициаторами обращения могут быть:

Подписчик, либо от него контактное лицо;

Администратор безопасности ОКЗ;

Куратор от организации.

одним из следующих способов:

заявка в ПДС или заявка через автоматизированную информационную систему, подключенную к ПДС (далее – заявка в ПДС);

заявка через СУ ИТ;

электронное письмо на п/я 1111@greenatom.ru (Центр поддержки пользователей);

электронное письмо на п/я ca@rosatom.ru (КУЦ);

звонок в центр поддержки пользователей АО «Гринатом» (+7 499 949 49 19, доб. 1111).

Если заявка получена в неформализованном виде, то Администратор безопасности ОКЗ:

– определяет наличие подписки и учётной записи в домене GK/inter у Подписчиков, указанных в обращении;

– формализует обращение в соответствии с правилами формализации, изложенными на официальном сайте КУЦ https://crypto.rosatom.ru в зависимости от следующих условий:

- в случае если Подписка отсутствует и обращение является обращением на создание Подписки, то информация поступает в подпроцесс «Создание подписки» в соответствии с выбранным шаблоном. Администратор безопасности ОКЗ должен определить шаблон для выпуска Сертификата на основании неформализованного обращения Подписчика;
- в случае если подписка на обеспечение Сертификатом у Подписчика, указанного в обращении, есть и обращение связано с компрометацией ключевой информации, подозрением на компрометацию, или изменением кадровых данных Подписчика,

то исходящая информация поступает в подпроцесс «Обеспечение Сертификатом»;

- в случае если Подписка на обеспечение Сертификатом у Подписчика, указанного в обращении, есть и обращение является обращением на сокращение Подписки, то исходящая информация поступает в подпроцесс «Сокращение подписки и аннулирование сертификата».

Исходящая информация поступает в подпроцесс «Создание подписки», «Сокращение подписки и аннулирование Сертификата», или «Обеспечение Сертификатом».

Если обращение содержит иные данные, процесс завершается.

3.1.2. Подпроцесс «Создание подписки»

Входящая информация поступает из подпроцесса «Обработка обращения».

Если заявку в ПДС на создание Подписки завел Подписчик, то Администратор безопасности ОКЗ:

- получает электронное уведомление о заведении Подписчиком заявки;
- согласовывает или не согласовывает заявку:
  если заявка отклонена, то процесс завершается. Подписчику отправляется уведомление об отклонении заявки Администратором безопасности ОКЗ.
  если заявка не отклонена, то он выбирает шаблон для выпуска Сертификата и согласовывает заявку. Заявка поступает на рассмотрение Куратору от организации.

Если заявку в ПДС на создание Подписки завел Администратор безопасности ОКЗ, то он выбирает шаблон для выпуска Сертификата и заявка поступает на рассмотрение Куратору от организации.

Куратор от организации:

- получает заявку, проверяет корректность информации о Подписчике, вносит информацию о Подписчике, в объеме, необходимом для выпуска Сертификата и регистрации его в ЕСИА (данный шаг может быть произведён автоматически, при наличии данных о Подписчике в ИАСУП).

Для выпуска Сертификата ПДС с использованием инфраструктуры осуществляет проверку достоверности документов и сведений: производится проверка СНИЛС в сервисе ПФР, получение выписки из ЕГРЮЛ в сервисе ФНС, проверка паспортных данных в сервисе МВД. В случае неполучения ответа от любого сервиса СМЭВ процесс возвращается на повторное направление заявки на проверку в СМЭВ Администратором безопасности ОКЗ. В случае получения от СМЭВ отрицательного результата проверки, заявка поступает Куратору от организации на рассмотрение, который либо

внесет изменения в ИАСУП, либо актуализирует информацию о сотруднике в заявке на подписку в случае отсутствия ИАСУП.

Уполномоченное лицо от организации:

– получает электронное уведомление о поступившей заявке на создание Подписки на подписание.

Если заявка отклонена, то процесс завершается.

Если заявка одобрена, то Уполномоченное лицо от организации:

– подписывает PDF-документ (печатный аналог электронной заявки) и подтверждает правомочия обращаться за получением квалифицированного сертификата с использованием сервиса усиленной квалифицированной электронной подписи.

Оператору УЦ от ПУСК ПДС формируется и отправляется электронное уведомление.

Оператор УЦ от ПУСК ПДС определяется автоматически в соответствии с настройками ПДС согласно принадлежности Подписчика к той или иной организации.

Исходящая информация поступает в подпроцесс «Создание Сертификата».

3.1.3. Подпроцесс «Обеспечение Сертификатом»

Входящая информация поступает из подпроцесса «Обработка обращения».

Если данные о Подписчике в ИАСУП изменились, то заявка на обеспечение Сертификатом создается автоматически в ПДС (при этом данные направляются на проверку в СМЭВ и в случае если возвращаются ошибки, то Куратор от организации корректирует данные в ИАСУП, из ПДС запрашивает обновление данных по Подписчику из ИАСУП, после получения обновленных данных снова отправляет заявку на этап проверки в СМЭВ для получения положительного ответа; в случае неполучения ответа от любого сервиса СМЭВ процесс возвращается на повторное направление заявки на проверку в СМЭВ Администратором безопасности ОКЗ). В случае положительного ответа от СМЭВ исходящая информация поступает в подпроцессы «Сокращение Подписки и аннулирование Сертификата» и «Создание Сертификата».

Если данные о Подписчике не содержатся в ИАСУП и информация актуализирована в ПДС Куратором от организации, то далее заявка направляется на проверку в СМЭВ и в случае если возвращаются ошибки, то Куратор от организации корректирует данные в ПДС; в случае неполучения ответа от любого сервиса СМЭВ процесс возвращается на повторное направление заявки на проверку в СМЭВ Администратором безопасности ОКЗ. В случае положительного ответа от СМЭВ исходящая информация

поступает в подпроцессы «Сокращение Подписки и аннулирование Сертификата» и «Создание Сертификата».

Если заявка на обеспечение Сертификатом создана в ПДС Подписчиком (по причине компрометации Сертификата), то:

Куратор от организации:

– проверяет корректность информации о Подписчике, вносит информацию о Подписчике, в объеме, необходимом для обеспечения Сертификатом и регистрации его в ЕСИА (данный шаг может быть произведён автоматически, при наличии данных о Подписчике в ИАСУП).

Далее данные направляются на проверку в СМЭВ и в случае если возвращаются ошибки, то Куратор от организации корректирует данные в ИАСУП, из ПДС запрашивает обновление данных по Подписчику из ИАСУП, после получения обновленных данных снова отправляет заявку на этап проверки в СМЭВ для получения положительного ответа (если нет ИАСУП, то заявка направляется на проверку в СМЭВ и в случае если возвращаются ошибки, то Куратор от организации корректирует данные в ПДС). В случае неполучения ответа от любого сервиса СМЭВ процесс возвращается на повторное направление заявки на проверку в СМЭВ Администратором безопасности ОКЗ. В случае положительного ответа от СМЭВ исходящая информация поступает в подпроцессы «Сокращение Подписки и аннулирование Сертификата» и «Создание Сертификата».

Если заявка на обеспечение Сертификатом создана не в ПДС, то Администратор безопасности ОКЗ:

– создает заявку в ПДС на обеспечение Сертификатом.

Куратор от организации:

– проверяет корректность информации о Подписчике, вносит информацию о Подписчике, в объеме, необходимом для обеспечения Сертификатом и регистрации его в ЕСИА (данный шаг может быть произведён автоматически, при наличии данных о Подписчике в ИАСУП).

Далее данные направляются на проверку в СМЭВ и в случае если возвращаются ошибки, то Куратор от организации корректирует данные в ИАСУП, из ПДС запрашивает обновление данных по Подписчику из ИАСУП, после получения обновленных данных снова отправляет заявку на этап проверки в СМЭВ для получения положительного ответа (если нет ИАСУП, то заявка направляется на проверку в СМЭВ и в случае если возвращаются ошибки, то Куратор от организации корректирует данные в ПДС). В случае неполучения ответа от любого сервиса СМЭВ процесс возвращается на повторное направление заявки на проверку в СМЭВ Администратором безопасности ОКЗ. В случае положительного ответа от СМЭВ исходящая информация поступает в подпроцессы «Сокращение Подписки и аннулирование Сертификата» и «Создание Сертификата».

3.1.4. Подпроцесс «Сокращение Подписки и аннулирование Сертификата»

Входящая информация поступает из подпроцессов «Обработка обращения», «Обеспечение Сертификатом», «Вручение Сертификата».

Если входящая информация поступает из подпроцесса «Обработка обращения»:

Если заявку на сокращение Подписки создал Подписчик, то Администратор безопасности ОКЗ:

- получает электронное уведомление о заведении Подписчиком заявки на сокращение Подписки;
- согласовывает или не согласовывает заявку на сокращение Подписки:
  если заявка на сокращение Подписки не согласована, то процесс завершается. Подписчику отправляется уведомление об отклонении заявки Администратором безопасности ОКЗ;
  если заявка на сокращение Подписки не отклонена, то он согласовывает заявку.

Если заявку на сокращение Подписки создает не Подписчик, то такая возможность есть у Администратора безопасности ОКЗ или Куратора от организации:

- создает заявку на сокращение Подписки в ПДС.

Уполномоченное лицо от организации:

- получает электронное уведомление о поступившей заявке на сокращение Подписки на подписание.

Если заявка отклонена, то процесс завершается.

Если заявка согласована, то:

- подписывает PDF-документ (печатный аналог электронной заявки) с использованием сервиса усиленной квалифицированной электронной подписи.

ПДС автоматически создает запрос на отзыв Сертификата.

От ПУСК ПДС приходит уведомление Подписчику об отзыве Сертификата и процесс завершается.

Если входящая информация поступает из подпроцессов «Обеспечение Сертификатом» и «Вручение Сертификата», то происходит автоматическое аннулирование Сертификата в ПДС и процесс завершается.

3.1.5. Подпроцесс «Создание Сертификата»

Входящая информация поступает из подпроцессов «Создание Подписки» и «Обеспечение Сертификатом».

Оператор УЦ от ПУСК ПДС:

- получает подписанную уполномоченным лицом от организации электронную заявку в ПДС на создание Подписки или электронную заявку в ПДС на Обеспечение Сертификатом, подключает ключевой носитель (при необходимости использования ключевого носителя) к рабочему месту Оператора УЦ от ПУСК ПДС;
- выбирает параметры ключевого контейнера, создает ключевой контейнер и запрос на Сертификат (в случае облачного Сертификата это происходит автоматически ПДС, созданный запрос на выпуск Сертификата Оператор УЦ от ПУСК ПДС переносит на квалифицированный УЦ и выполняет выпуск Сертификата);
- устанавливает выпущенный Сертификат на ключевой носитель (в случае облачного Сертификата Сертификат передается в DSS для установки в контейнер);
- создаёт пакет для передачи выпущенного Сертификата на ключевом носителе Администратору безопасности ОКЗ лично или Службой специальной связи. Если создан облачный Сертификат, то исходящая информация сразу поступает в подпроцесс «Вручение Сертификата».

Исходящая информация поступает в подпроцесс «Вручение сертификата».

3.1.6. Подпроцесс «Вручение Сертификата»

Входящая информация поступает из подпроцесса «Создание Сертификата».

Если создан Сертификат на ключевом носителе, то Администратору безопасности ОКЗ формируется и отправляется электронное уведомление о необходимости получения ключевого носителя.

Если передается Сертификат на ключевом носителе, Оператор УЦ от ПУСК ПДС:

- передает пакет с Сертификатом Администратору безопасности ОКЗ лично в руки или Спецсвязью.

Администратор безопасности ОКЗ:

- подтверждает получение Сертификата в ПДС. Подписчику формируется и отправляется электронное уведомление о выпуске Сертификата от ПДС;
- верифицирует Подписчика. При вручении Сертификата Администратор безопасности ОКЗ обязан установить личность Подписчика (устанавливает личность Подписчика при личном присутствии Подписчика);

  если верификация прошла успешно, то передает пакет с Сертификатом;

если верификация не пройдена, то вносит данные в заявку на создание Подписки о причинах отказа в верификации, заявка закрывается с ошибкой выдачи Сертификата. Исходящая информация поступает в подпроцесс «Сокращение Подписки и аннулирование Сертификата», Подписка в этом случае не начинает действовать.

Подписчик:

- получает пакет с ключевым носителем с выпущенным Сертификатом;
- просматривает информацию на бумажном носителе, содержащуюся в Сертификате:
  если информация на бумажном носителе, содержащаяся в Сертификате верна, то подписывает ее собственноручной подписью.

Администратор безопасности ОКЗ:
- загружает в ПДС скан-копию подписанной информации на бумажном носителе, сод. в Сертификате.

Исходящая информация поступает в подпроцесс «Контроль срока действия Сертификата».

если информация на бумажном носителе, содержащаяся в Сертификате не верна, то:

Администратор безопасности ОКЗ:
- вносит данные в заявку на создание Подписки о причинах отказа в выдаче/получении Сертификата.

Исходящая информация поступает в подпроцесс «Сокращение Подписки и аннулирование Сертификата»

Если создан облачный Сертификат и у Подписчика есть действующий Сертификат, то Подписчик:

- просматривает информацию в ПДС, содержащуюся в Сертификате:
  если информация, содержащаяся в Сертификате в ПДС верна, то подписывает его усиленной квалифицированной электронной подписью. При этом исходящая информация поступает в подпроцесс «Контроль срока действия Сертификата»;
  если информация, содержащаяся в Сертификате в ПДС не верна, то вносит в заявку на создание Подписки данные о причине отказа в получении Сертификата. При этом исходящая информация поступает в подпроцесс «Сокращение Подписки и аннулирование Сертификата».
  Личность Подписчика устанавливается посредством идентификации заявителя без его личного присутствия с использованием усиленной квалифицированной электронной подписи.

Если создан облачный Сертификат и у Подписчика нет действующего Сертификата, то верификация осуществляется Администратором безопасности так же, как и в случае с Сертификатом на ключевом носителе, при этом Подписчик:

– просматривает информацию на бумажном носителе, содержащуюся в Сертификате:
если информация на бумажном носителе, содержащаяся в Сертификате верна, то подписывает ее собственноручной подписью.

Администратор безопасности ОКЗ:
– загружает в ПДС скан-копию подписанной информации на бумажном носителе, сод. в Сертификате.

Исходящая информация поступает в подпроцесс «Контроль срока действия Сертификата».

если информация на бумажном носителе, содержащаяся в Сертификате не верна, то:

Администратор безопасности ОКЗ:
– вносит данные в заявку на создание Подписки о причинах отказа в выдаче/получении Сертификата.

Исходящая информация поступает в подпроцесс «Сокращение Подписки и аннулирование Сертификата»

ПДС автоматически направляет в ЕСИА сведения о лице, получившем Сертификат, в объеме, необходимом для регистрации в ЕСИА, и о полученном им Сертификате (уникальный номер Сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра) после того как Подписчик был идентифицирован и подтвердил сведения в выпущенном сертификате. После получения от СМЭВ ответа об успешной публикации сертификата, подписчику в ЛК ПДС становится доступен:

– если облачный Сертификат, то либо пин-код от контейнера, либо QR-код для подключения myDSS;
– если Сертификат на ключевом носителе, то пин-код от контейнера.

Исходящая информация поступает в подпроцесс «Контроль действия Сертификата».

При выдаче Сертификата аккредитованный удостоверяющий центр по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию указанного лица в ЕСИА.

3.1.7. Подпроцесс «Контроль срока действия Сертификата»

Входящая информация поступает из подпроцесса «Вручение Сертификата».

Контроль срока действия Сертификата инициируется автоматически за 90 дней до окончания срока действия Сертификата.

Куратор от организации:

– получает заявку, проверяет корректность информации о Подписчике, вносит информацию о Подписчике, в объеме, необходимом для выпуска Сертификата и регистрации его в ЕСИА. Данный шаг может быть произведён автоматически, при наличии данных о Подписчике в ИАСУП.

Для выпуска Сертификата ПДС с использованием инфраструктуры осуществляет проверку достоверности документов и сведений: производится проверка СНИЛС в сервисе ПФР, получение выписки из ЕГРЮЛ в сервисе ФНС, проверка паспортных данных в сервисе МВД. В случае неполучения ответа от любого сервиса СМЭВ процесс возвращается на повторное направление заявки на проверку в СМЭВ Администратором безопасности ОКЗ. В случае получения от СМЭВ отрицательного результата проверки, заявка уйдет Куратору от организации на рассмотрение, который либо внесет изменения в ИАСУП, либо актуализирует информацию о сотруднике в заявке на Подписку в случае отсутствия ИАСУП.

Исходящая информация поступает в подпроцесс «Создание Сертификата».

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".

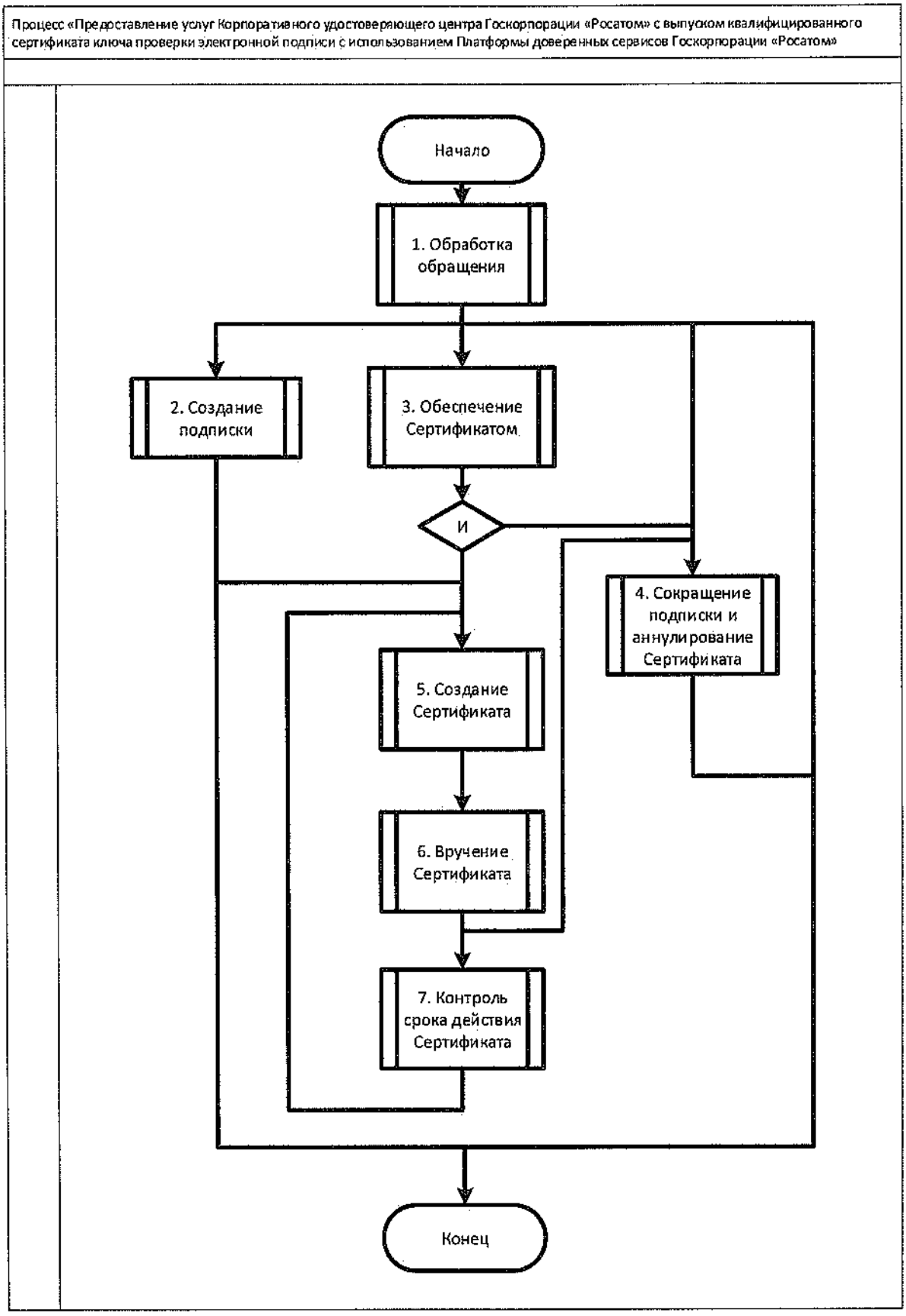
Приказ Министерства связи и массовых коммуникаций РФ от 23 ноября 2011 г. № 320 “Об аккредитации удостоверяющих центров”.

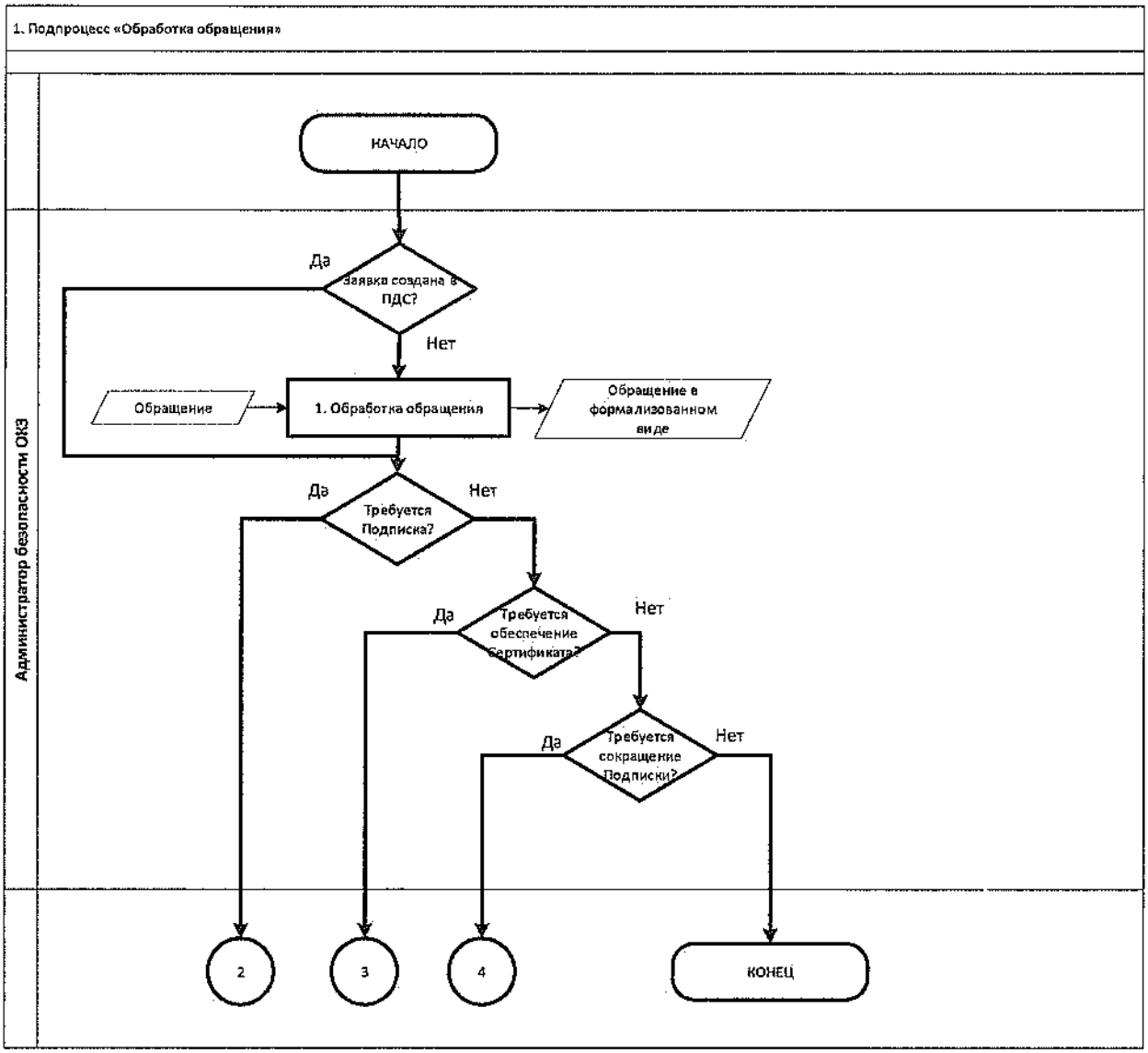
Приказ Госкорпорации «Росатом» от 04.12.2015 № 1/1176-П (с учётом изменений, внесённых приказом Госкорпорации «Росатом» от 26.07.2019 № 1/764-П).

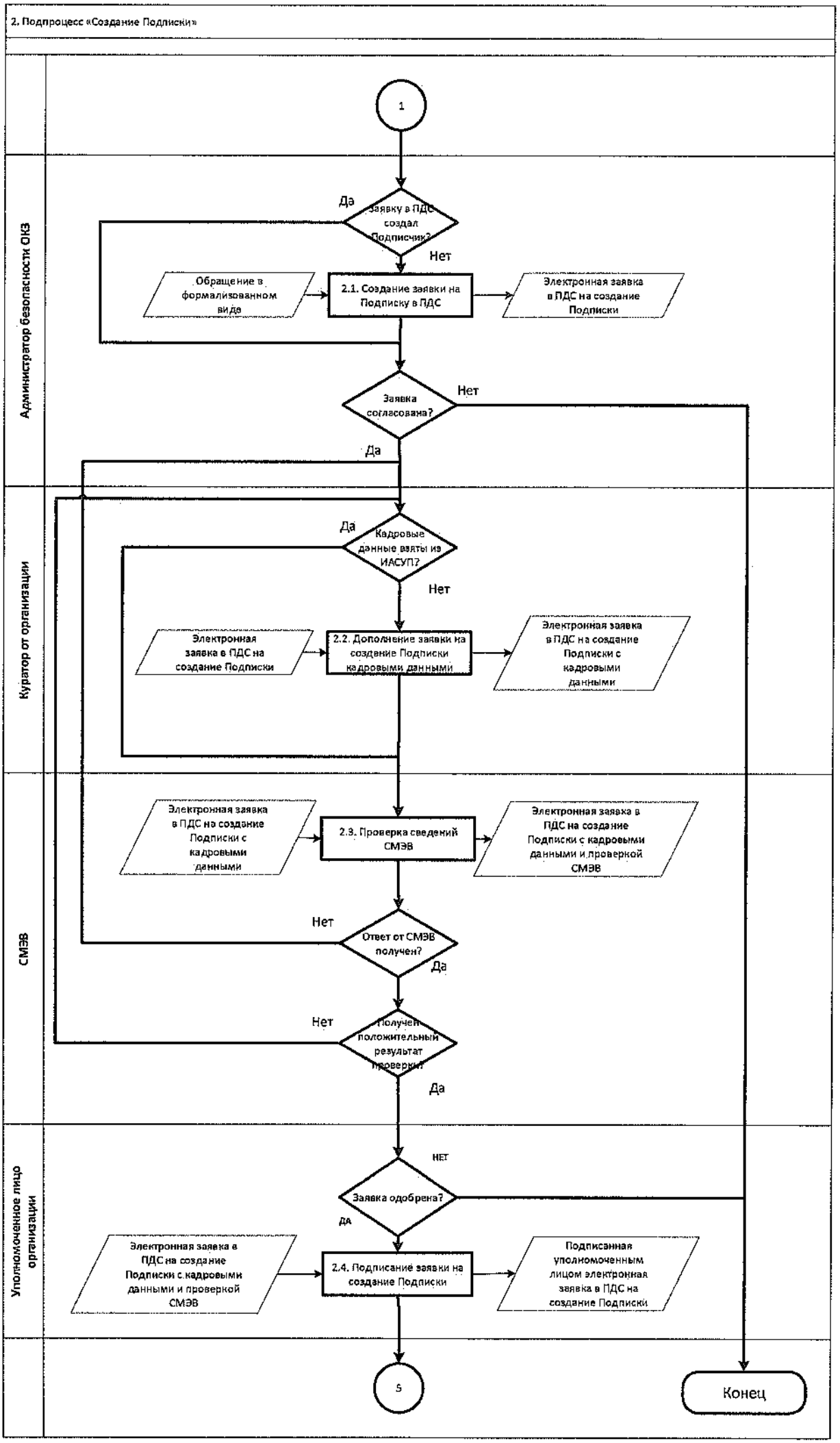
5. Перечень приложений

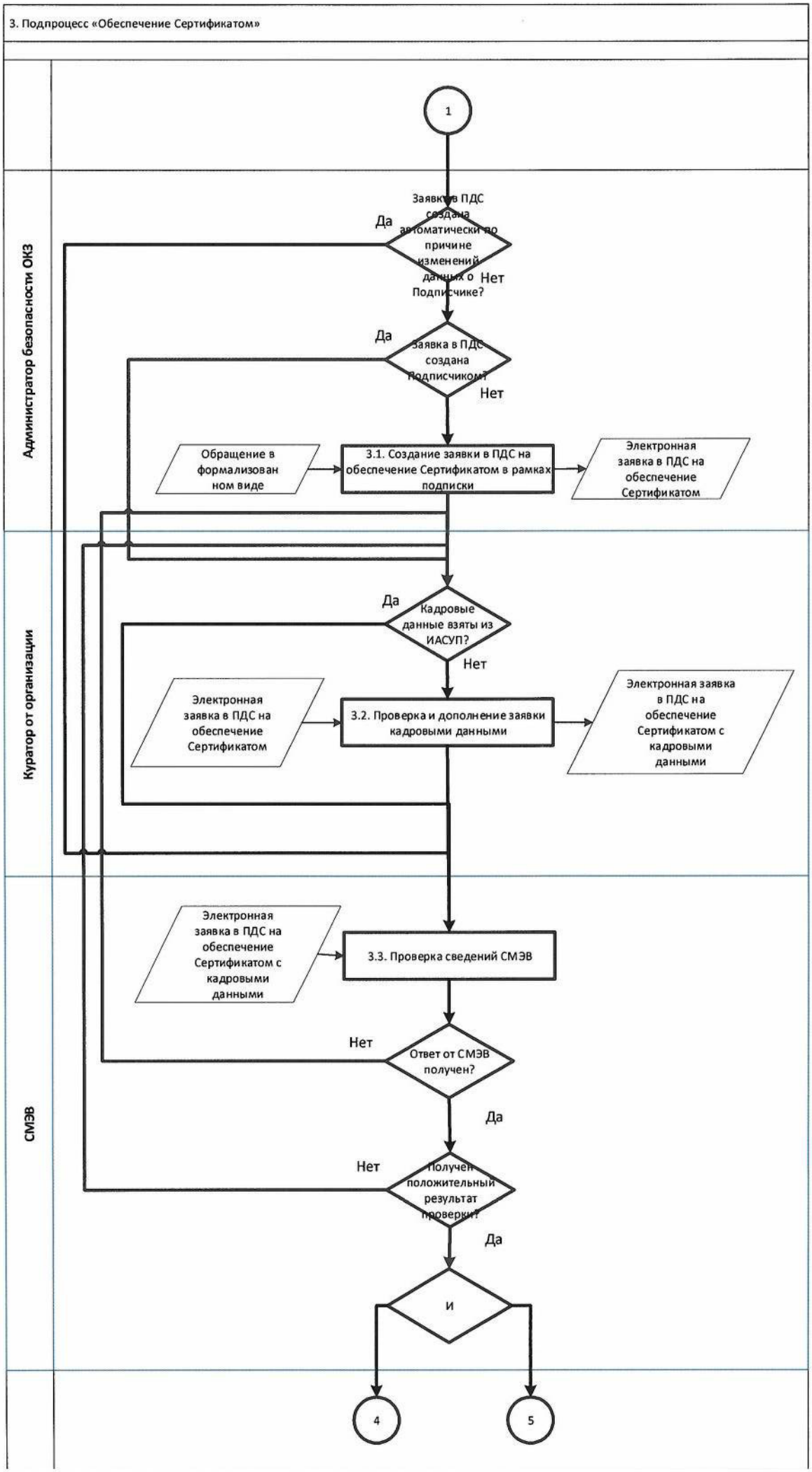
Приложение №1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом».

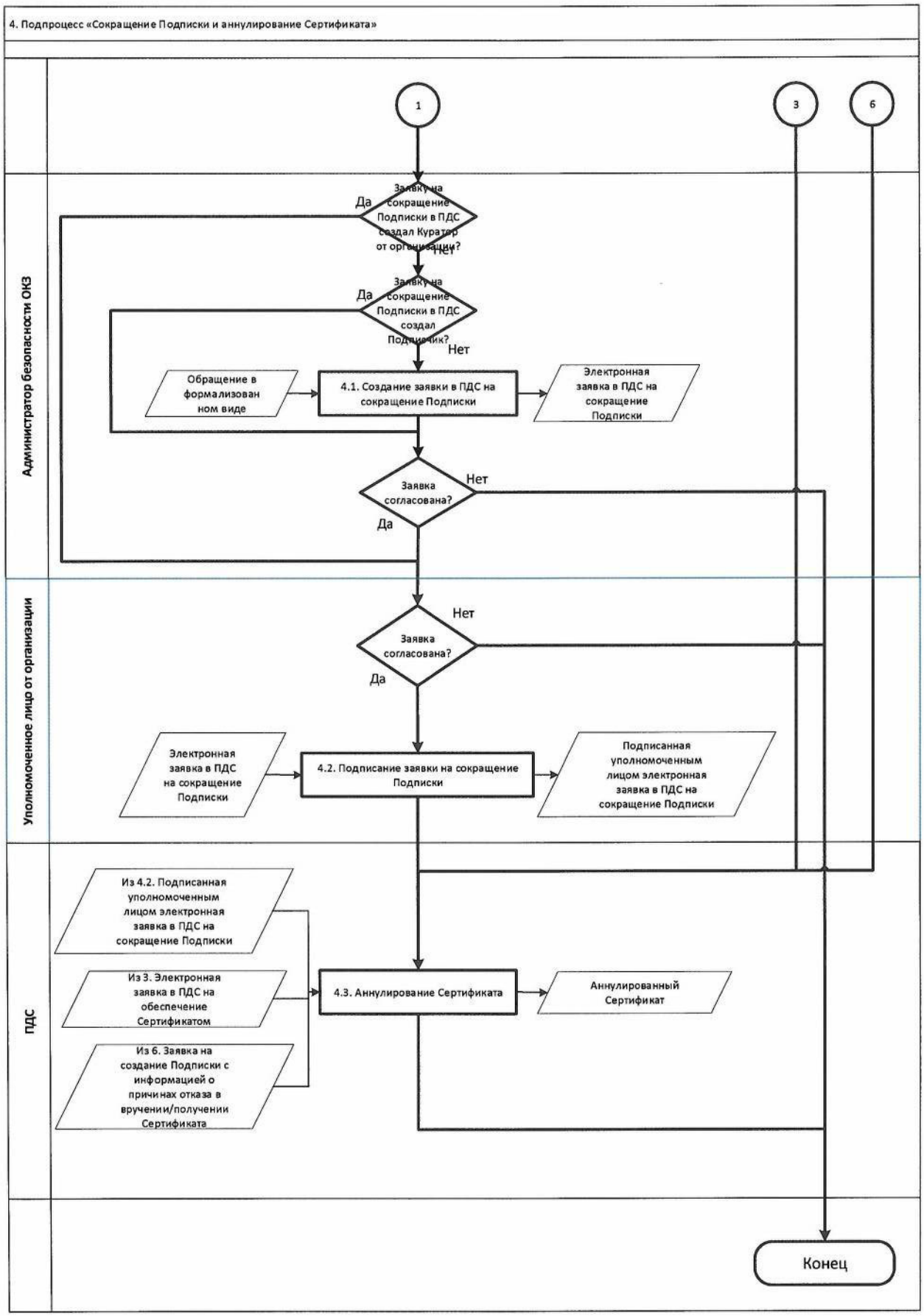
Приложение №1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом»

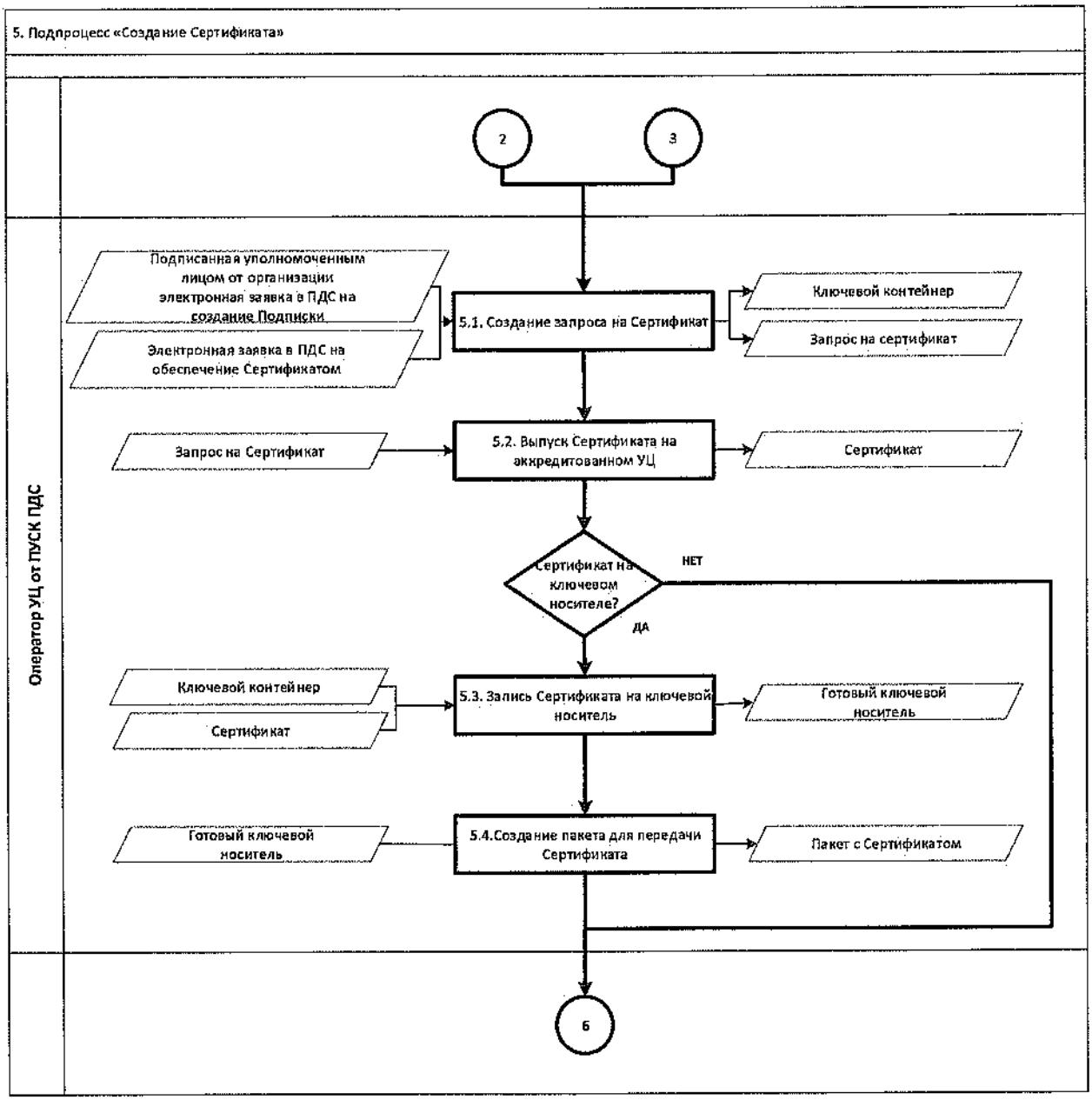


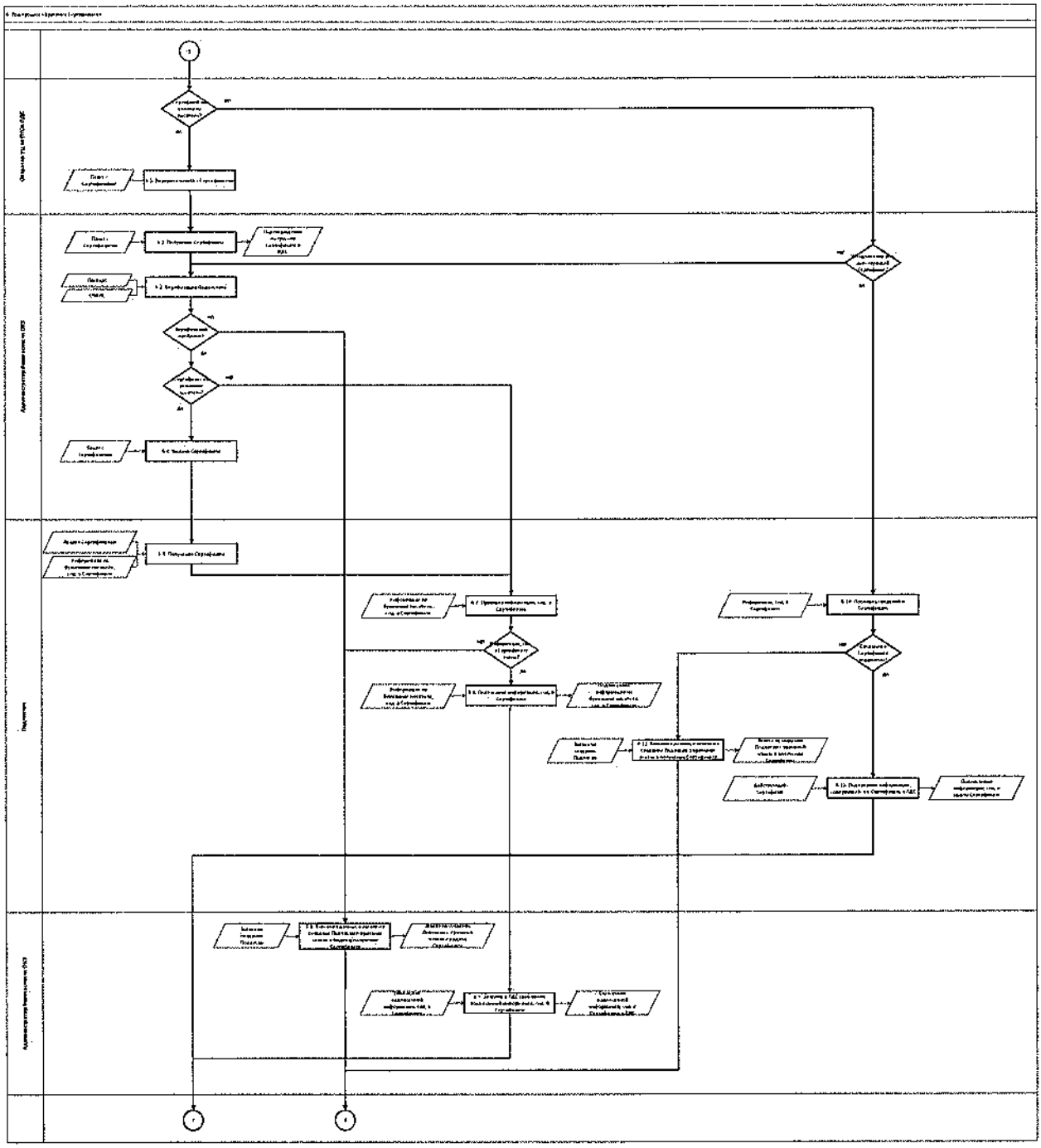

1. Подпроцесс «Обработка обращения»
Администратор безопасности ОКЗ
НАЧАЛО
Да
Заявка создана в ПДС?
Нет
Обращение
1. Обработка обращения
Обращение в формализованном виде
Да
Требуется Подписка?
Нет
Да
Требуется обеспечение сертификата?
Нет
Да
Требуется сокращение Подписки?
Нет
2
3
4
КОНЕЦ

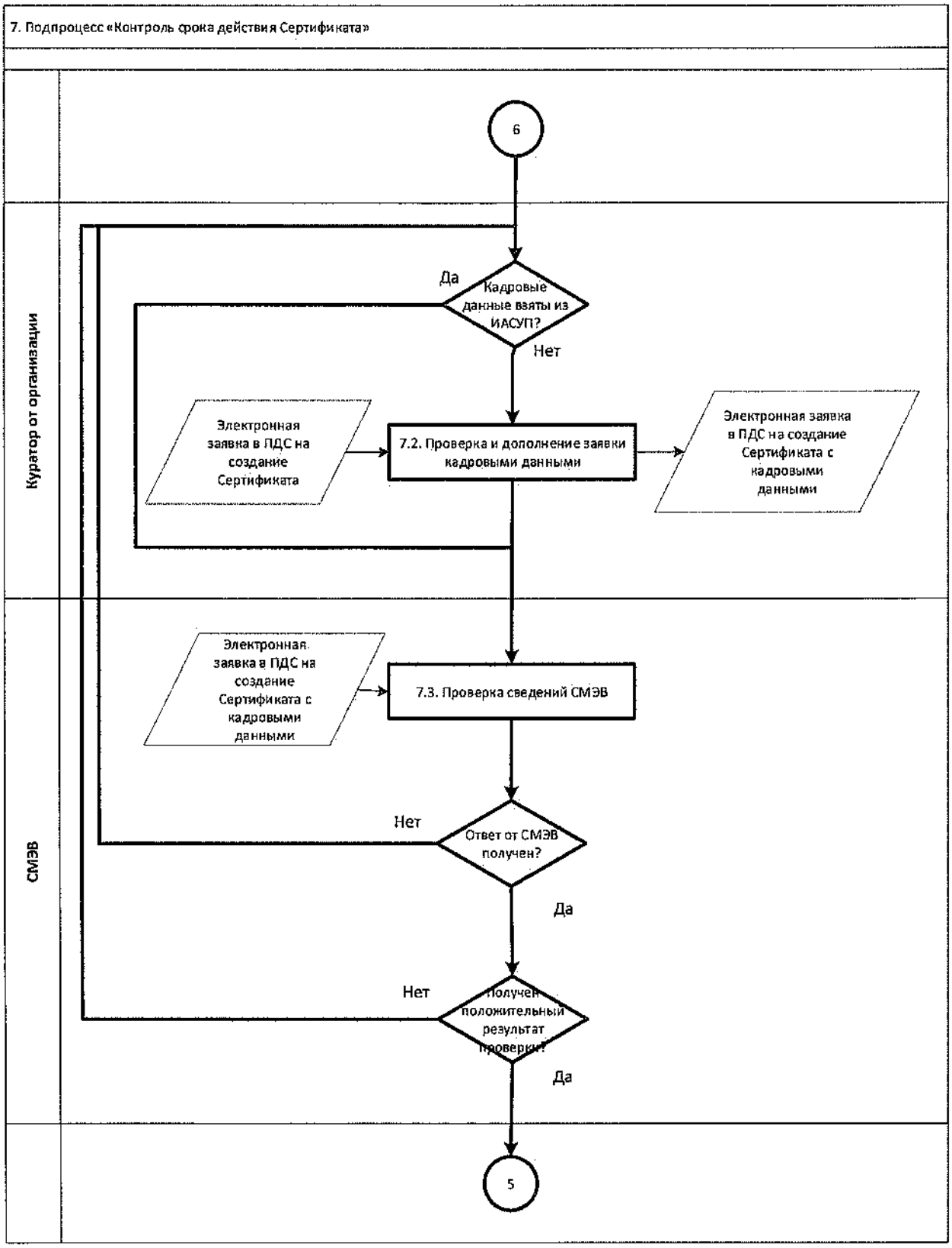

2. Подпроцесс «Создание Подписки»
Администратор безопасности ОКЗ
Куратор от организации
СМЭВ
Уполномоченное лицо организации
1
Заявку в ПДС создал Подписчик?
Да
Нет
Обращение в формализованном виде
2.1. Создание заявки на Подписку в ПДС
Электронная заявка в ПДС на создание Подписки
Заявка согласована?
Нет
Да
Кадровые данные взяты из ИАСУП?
Да
Нет
Электронная заявка в ПДС на создание Подписки
2.2. Дополнение заявки на создание Подписки кадровыми данными
Электронная заявка в ПДС на создание Подписки с кадровыми данными
Электронная заявка в ПДС на создание Подписки с кадровыми данными
2.3. Проверка сведений СМЭВ
Электронная заявка в ПДС на создание Подписки с кадровыми данными и проверкой СМЭВ
Ответ от СМЭВ получен?
Нет
Да
Получен положительный результат проверки?
Нет
Да
Заявка одобрена?
НЕТ
ДА
Электронная заявка в ПДС на создание Подписки с кадровыми данными и проверкой СМЭВ
2.4. Подписание заявки на создание Подписки
Подписанная уполномоченным лицом электронная заявка в ПДС на создание Подписки
5
Конец


3. Подпроцесс «Обеспечение Сертификатом»
Администратор безопасности ОКЗ
Куратор от организации
СМЭВ
1
Заявка в ПДС создана автоматически по причине изменений данных о Подписчике?
Да
Нет
Заявка в ПДС создана Подписчиком?
Да
Нет
Обращение в формализованном виде
3.1. Создание заявки в ПДС на обеспечение Сертификатом в рамках подписки
Электронная заявка в ПДС на обеспечение Сертификатом
Кадровые данные взяты из ИАСУП?
Да
Нет
Электронная заявка в ПДС на обеспечение Сертификатом
3.2. Проверка и дополнение заявки кадровыми данными
Электронная заявка в ПДС на обеспечение Сертификатом с кадровыми данными
Электронная заявка в ПДС на обеспечение Сертификатом с кадровыми данными
3.3. Проверка сведений СМЭВ
Ответ от СМЭВ получен?
Нет
Да
Получен положительный результат проверки?
Нет
Да
И
4
5


4. Подпроцесс «Сокращение Подписки и аннулирование Сертификата»
Администратор безопасности ОКЗ
Уполномоченное лицо от организации
ПДС
1
3
6
Заявку на сокращение Подписки в ПДС создал Куратор от организации?
Да
Нет
Заявку на сокращение Подписки в ПДС создал Подписчик?
Да
Нет
Обращение в формализованном виде
4.1. Создание заявки в ПДС на сокращение Подписки
Электронная заявка в ПДС на сокращение Подписки
Заявка согласована?
Нет
Да
Заявка согласована?
Нет
Да
Электронная заявка в ПДС на сокращение Подписки
4.2. Подписание заявки на сокращение Подписки
Подписанная уполномоченным лицом электронная заявка в ПДС на сокращение Подписки
Из 4.2. Подписанная уполномоченным лицом электронная заявка в ПДС на сокращение Подписки
Из 3. Электронная заявка в ПДС на обеспечение Сертификатом
Из 6. Заявка на создание Подписки с информацией о причинах отказа в вручении/получении Сертификата
4.3. Аннулирование Сертификата
Аннулированный Сертификат
Конец


5. Подпроцесс «Создание Сертификата»
Оператор УЦ от ПУСК ПДС
2
3
Подписанная уполномоченным лицом от организации электронная заявка в ПДС на создание Подписки
Электронная заявка в ПДС на обеспечение Сертификатом
5.1. Создание запроса на Сертификат
Ключевой контейнер
Запрос на сертификат
Запрос на Сертификат
5.2. Выпуск Сертификата на аккредитованном УЦ
Сертификат
Сертификат на ключевом носителе?
НЕТ
ДА
Ключевой контейнер
Сертификат
5.3. Запись Сертификата на ключевой носитель
Готовый ключевой носитель
Готовый ключевой носитель
5.4.Создание пакета для передачи Сертификата
Пакет с Сертификатом
6




7. Подпроцесс «Контроль срока действия Сертификата»
Куратор от организации
СМЭВ
6
Да
Кадровые данные взяты из ИАСУП?
Нет
Электронная заявка в ПДС на создание Сертификата
7.2. Проверка и дополнение заявки кадровыми данными
Электронная заявка в ПДС на создание Сертификата с кадровыми данными
Электронная заявка в ПДС на создание Сертификата с кадровыми данными
7.3. Проверка сведений СМЭВ
Нет
Ответ от СМЭВ получен?
Да
Нет
Получен положительный результат проверки?
Да
5

Приложение №13 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю

Директор по информационным технологиям

АО «Гринатом»

_____ / А.Н. Киселёв /

М.П.

ПОРЯДОК

предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом»

Москва 2020 г.

Содержание

1. Назначение и область применения

1.1. Настоящий Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (далее - Порядок) разработан для установления последовательности действий по процессу группы процессов управления информационными технологиями с целями установления правил и условий предоставления и пользования услугами Корпоративного удостоверяющего центра Госкорпорации «Росатом» по созданию, выдаче и управлению неквалифицированными сертификатами ключей проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом».

Информация о Корпоративном удостоверяющем центре Госкорпорации «Росатом» размещена на официальном сайте https://crypto.rosatom.ru.

1.2. Соблюдение Порядка является обязательным для предприятий/ организаций, использующих автоматизированные информационные системы, в которых применяются сертификаты ключей проверки электронных подписей, создаваемые Корпоративным удостоверяющим центром Госкорпорации «Росатом».

Требования Порядка обязательны для сотрудников, выполняющих следующие функциональные роли:

1. Подписчик.
2. Куратор от организации.
3. Уполномоченное лицо от организации.
4. Администратор безопасности ОКЗ.
5. Куратор ПДС.
6. Оператор УЦ от ПУСК ПДС.

1.3. Ответственным за актуализацию Порядка и контроль его исполнения в соответствии с требованиями Положения о системе регламентирующих документов Госкорпорации «Росатом» является директор Департамента по информационным технологиям Блока по ИТ АО «Гринатом».

1.4. Актуальная версия Порядка размещена по адресу: https://crypto.rosatom.ru.

2. Термины, сокращения и аббревиатуры

2.1. Термины и определения

Термин	Определение
Администратор безопасности ОКЗ	Уполномоченный работник АО «Гринатом» (по договору) или уполномоченный работник организации-заказчика, наделенный полномочиями по вручению сертификатов ключей проверки электронных подписей от имени удостоверяющего центра.
Аккредитация удостоверяющего центра	Признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

Владелец сертификата ключа проверки электронной подписи	Лицо, которому в соответствии настоящим Порядком, с учетом Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», создан неквалифицированный сертификат ключа проверки электронной подписи.
Вручение сертификата ключа проверки электронной подписи	Передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.
Неквалифицированный сертификат ключа проверки электронной подписи	Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом №63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный неаккредитованным центром сертификации.
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
Ключевой носитель	Отчуждаемый носитель информации, предназначенный для хранения ключа электронной подписи и ключа проверки электронной подписи.
Корпоративный удостоверяющий центр Госкорпорации «Росатом»	Удостоверяющий центр АО «Гринатом».
Куратор от организации	Сотрудник организации-заказчика, который дополняет заявки на создание Подписки, на перевыпуск Сертификата кадровыми данными Подписчика.
Оператор Удостоверяющего центра от подсистемы управления сервисами и коннекторами Платформы доверенных сервисов Госкорпорации «Росатом»	Сотрудник Корпоративного удостоверяющего центра Госкорпорации «Росатом», который создает Сертификаты.
Подписка	Заказ предприятия в ПДС в соответствии с условиями договора присоединения на обеспечение сертификатами или средствами криптографической защиты и информации. Подписка подразумевает владение Подписчиком одним действующим сертификатом выбранного шаблона.
Подписчик	Физическое лицо, для которого оформлена подписка на обеспечение сертификатом и (или) лицензией на средство криптографической защиты информации (обладает учётной записью в домене GK/inter, создаёт обращения, получает Сертификаты).
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.
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.
Уполномоченное лицо от организации	Работник юридического лица, указанный в ЕГРЮЛ и имеющий возможность обращаться в Удостоверяющий центр от имени юридического лица, либо работник имеющий право действовать от имени юридического лица на основании доверенности
Участники электронного взаимодействия	Государственные органы, органы местного самоуправления, организации, а также граждане осуществляющие обмен информацией в электронной форме.
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.

В Порядке используются термины, установленные Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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

Термин	Определение
ИАСУП	Информационная автоматизированная система управления персоналом Госкорпорации «Росатом»
КИС	Корпоративная информационная система
КУЦ	Корпоративный удостоверяющий центр Госкорпорации «Росатом»
ЛИС	Локальная информационная система
ПДС	Платформа доверенных сервисов Госкорпорации «Росатом»
ПУСК ПДС	Подсистема управления сервисами и коннекторами Платформы доверенных сервисов Госкорпорации «Росатом»
Сертификат	Неквалифицированный сертификат ключа проверки электронной подписи
СУ ИТ	Система управления информационными технологиями
УНЭП	Усиленная неквалифицированная электронная подпись
УЦ	Удостоверяющий центр
ЭП	Электронная подпись

3. Описание процесса

Описание процесса предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки ЭП с использованием Платформы доверенных сервисов Госкорпорации «Росатом».

До начала процесса организация-заказчик должна направить в орган криптографической защиты АО «Гринатом» оригинал заявления на предоставление услуги по форме Приложения №2, подписанное Уполномоченным лицом от организации.

3.1. Описание подпроцессов

3.1.1. Подпроцесс «Заведение информации в ПДС об объеме Подписки»

Куратор ПДС:

– заводит информацию в ПДС об объеме Подписки организации-заказчика, согласно полученному заявлению на предоставление услуги (Приложение №2).

3.1.2. Подпроцесс «Обработка обращения»

Инициаторами обращения могут быть:

Подписчик, либо от него контактное лицо;

Администратор безопасности ОКЗ.

одним из следующих способов:

информация из ИАСУП о том, что Подписчик согласился/отказался использовать УНЭП (облачный Сертификат). В этом случае Сертификат Подписчику создается/аннулируется автоматически;

заявка в ПДС или заявка через автоматизированную информационную систему, подключенную к ПДС (далее – заявка в ПДС);

заявка через СУ ИТ;

электронное письмо на п/я 1111@greenatom.ru (Центр поддержки пользователей);

электронное письмо на п/я ca@rosatom.ru (КУЦ);

звонок в центр поддержки пользователей АО «Гринатом» (+7 499 949 49 19, доб. 1111).

В случае если поступает неформализованное обращение, то Администратор безопасности ОКЗ:

– определяет наличие Подписки и учётной записи в домене GK/inter у Подписчиков, указанных в обращении;

– формализует обращение в соответствии с правилами формализации, изложенными на официальном сайте КУЦ https://crypto.rosatom.ru в зависимости от следующих условий:

- в случае если Подписка отсутствует и обращение является обращением на создание Подписки, то информация поступает

в подпроцесс «Создание подписки» в соответствии с выбранным шаблоном. Администратор безопасности ОКЗ должен определить шаблон для выпуска Сертификата на основании неформализованного обращения Подписчика;

- в случае если Подписка на Подписчика, указанного в обращении, есть и обращение связано с компрометацией ключевой информации, подозрением на компрометацию или изменением кадровых данных о подписчике, то исходящая информация поступает в подпроцесс «Перевыпуск сертификата»;
- в случае если Подписка на сотрудника организации, указанного в обращении, есть и обращение является обращением на сокращение Подписки, то исходящая информация поступает в подпроцесс «Сокращение подписки и аннулирование Сертификата»;

Исходящая информация поступает в подпроцесс «Создание подписки», «Сокращение подписки и аннулирование Сертификата», либо «Перевыпуск Сертификата».

Если обращение содержит иные данные, процесс завершается.

Если заявка была создана в ПДС, то процесс начинается с подпроцессов «Создание подписки», «Перевыпуск сертификата» или «Сокращение подписки и аннулирование Сертификата», в зависимости от типа заявки.

3.1.3. Подпроцесс «Создание Подписки»

Входящая информация поступает из подпроцесса «Обработка обращения».

Если заявка на создание Подписки создана автоматически в ПДС по причине согласия Подписчика в ИАСУП на использование облачного Сертификата, то исходящая информация поступает в подпроцесс «Создание Сертификата».

Если заявку на создание Подписки в ПДС создал Подписчик или Администратор безопасности ОКЗ (если заявка создана Администратором безопасности ОКЗ, то Подписчику отправляется уведомление о создании заявки), то Куратор от организации:

– получает в ПДС заявку на создание Подписки, проверяет корректность информации о Подписчике, вносит информацию о Подписчике, в объеме, необходимом для выпуска Сертификата.

Если заявка на создание Подписки на Сертификат на ключевом носителе, то она переходит на рассмотрение Уполномоченному лицу от организации.

Если заявка на создание Подписки на облачный Сертификат, то исходящая информация сразу поступает в подпроцесс «Создание Сертификата».

Уполномоченное лицо от организации:

– получает электронное уведомление о поступившей заявке на создание Подписки на Сертификат на ключевом носителе на подписание.

Если заявка отклонена, то процесс завершается и Подписчику отправляется уведомление об отклонении заявки.

Если заявка согласована, то:

– подписывает PDF-документ (печатный аналог электронной заявки) с использованием сервиса усиленной квалифицированной/неквалифицированной электронной подписи.

Исходящая информация поступает в подпроцесс «Создание сертификата».

3.1.4. Подпроцесс «Перевыпуск Сертификата»

Входящая информация поступает из подпроцесса «Обработка обращения».

Если информация о Подписчике в ИАСУП изменилась, и она не связана с увольнением Подписчика или кадровые данные о Подписчике в ПДС изменил Куратор от организации, то ПДС автоматически создает заявку на перевыпуск Сертификата, при этом Подписчику отправляется уведомление о создании заявки на перевыпуск Сертификата.

Исходящая информация сразу поступает в подпроцесс «Сокращение подписки и аннулирование Сертификата» и «Создание Сертификата».

Если заявку на перевыпуск создал Подписчик, то Куратор от организации:

– получает в ПДС заявку на перевыпуск Сертификата, проверяет корректность информации о Подписчике, вносит информацию о Подписчике, в объеме, необходимом для выпуска Сертификата (данный шаг может быть произведён автоматически, при наличии данных о Подписчике в ИАСУП).

Исходящая информация поступает в подпроцесс «Сокращение подписки и аннулирование сертификата» и «Создание Сертификата».

Если заявка на перевыпуск получена через обращение, то Администратор безопасности ОКЗ:

– создает заявку в ПДС на перевыпуск Сертификата.

Куратор от организации:

– получает в ПДС заявку на перевыпуск Сертификата, проверяет корректность информации о Подписчике, вносит информацию о Подписчике, в объеме, необходимом для выпуска Сертификата (данный шаг может быть произведён автоматически, при наличии данных о Подписчике в ИАСУП).

Если перевыпуск Сертификата связан с изменением кадровых данных о Подписчике, то сначала создается новый Сертификат, а потом аннулируется ранее выпущенный.

Если перевыпуск Сертификата связан с компрометацией, то сначала аннулируется действующий Сертификат и только потом выпускается новый.

Исходящая информация поступает в подпроцесс «Сокращение подписки и аннулирование Сертификата» и «Создание Сертификата».

3.1.5. Подпроцесс «Сокращение подписки и аннулирование Сертификата»

Входящая информация поступает из подпроцессов «Обработка обращения», «Перевыпуск Сертификата», «Вручение Сертификата».

Если в ИАСУП или Куратором от организации в ПДС была внесена информация об увольнении Подписчика, то процесс аннулирования Сертификата происходит в автоматическом режиме и процесс завершается. Подписчику отправляется уведомление о сокращении Подписки и аннулировании Сертификата. При этом если Сертификат на ключевом носителе, то Администратору безопасности также отправляется уведомление о сокращении Подписки и аннулировании Сертификата Подписчика и он изымает ключевой носитель у Подписчика, уничтожает его и ставит отметку в ПДС об уничтожении.

Если входящая информация поступает из подпроцесса «Обработка обращения»:

Если заявку на сокращение Подписки на облачный Сертификат в ПДС создал Подписчик или Администратор безопасности, то ПДС отправляет запрос в УЦ на аннулирование Сертификата и процесс завершается. В случае если заявку на сокращение Подписки создал Администратор безопасности ОКЗ, то Подписчику отправляется уведомление о создании заявки на сокращение Подписки.

Если заявку на сокращение Подписки на Сертификат на ключевом носителе в ПДС создал Подписчик или Администратор безопасности, подпроцесс переходит к Уполномоченному лицу организации. В случае если заявку на сокращение Подписки создал Администратор безопасности ОКЗ, то Подписчику отправляется уведомление о создании заявки на сокращение Подписки.

Уполномоченное лицо от организации:

– получает электронное уведомление о поступившей заявке на сокращение Подписки на подписание.

Если заявка отклонена, то процесс завершается (при этом Подписчику и Администратору безопасности ОКЗ отправляется уведомление об отклонении заявки).

Если заявка согласована, то:

– подписывает PDF-документ (печатный аналог электронной заявки) с использованием сервиса усиленной квалифицированной/неквалифицированной электронной подписи.

ПДС отправляет запрос в УЦ на аннулирование Сертификата.

От ПУСК ПДС приходит уведомление Подписчику и Администратору безопасности ОКЗ об аннулировании Сертификата и процесс завершается.

Если входящая информация поступает из подпроцесса «Перевыпуск Сертификата»:

Сертификат аннулируется автоматически, при этом Подписчику и Администратору безопасности ОКЗ приходит уведомление об аннулировании Сертификата и о создании заявки на новый Сертификат, и процесс завершается.

Если входящая информация поступает из подпроцесса «Вручение Сертификата»:

Сертификат аннулируется автоматически, при этом Подписчику и Администратору безопасности ОКЗ приходит уведомление об аннулировании Сертификата, Подписка не начинает действовать.

3.1.6. Подпроцесс «Создание Сертификата»

Входящая информация поступает из подпроцессов «Создание Подписки», «Перевыпуск Сертификата» и «Контроль срока действия Сертификата».

Если получена заявка на выпуск облачного Сертификата, то создание Сертификата происходит автоматически в ПДС и исходящая информация поступает в подпроцесс «Контроль срока действия Сертификата». При этом Подписчик не получает ПИН-код в личном кабинете ПУСК ПДС. В качестве второго фактора для подтверждения операций используется одноразовый пароль (one time password).

Если получена заявка на выпуск Сертификата на ключевом носителе, то Оператор УЦ от ПУСК ПДС:

– подключает ключевой носитель к своему рабочему месту;

– форматирует ключевой носитель, запускает генерацию ключевой пары;

- ПДС автоматически создаёт запрос на Сертификат и выпускает Сертификат на неаккредитованном УЦ;
- устанавливает выпущенный Сертификат на ключевой носитель;
- создаёт пакет для передачи выпущенного Сертификата Администратору безопасности ОКЗ лично или Службой специальной связи. Пакет содержит готовый ключевой носитель с содержащейся на нем ключевой информацией и Сертификатом. При этом ПИН-код от ключевого контейнера Подписчик получит в личном кабинете ПУСК ПДС после того, как подтвердит получение ключевого носителя.

Исходящая информация поступает в подпроцесс «Вручение Сертификата».

3.1.7. Подпроцесс «Вручение Сертификата»

Входящая информация поступает из подпроцесса «Создание Сертификата».

Администратору безопасности ОКЗ формируется и отправляется электронное уведомление о необходимости получения пакета с Сертификатом.

Оператор УЦ от ПУСК ПДС:

- передает пакет с Сертификатом Администратору безопасности ОКЗ.

Администратор безопасности ОКЗ:

- подтверждает получение Сертификата в ПДС. Подписчику формируется и отправляется электронное уведомление о получении Сертификата Администратором безопасности ОКЗ;
- верифицирует Подписчика. Вручает Подписчику пакет с Сертификатом. При вручении Сертификата Администратор безопасности ОКЗ обязан установить личность Подписчика (если верификация не пройдена, то вносит данные в заявку на создание Подписки о причинах отказа в верификации, заявка закрывается с ошибкой выдачи Сертификата. Исходящая информация поступает в подпроцесс «Сокращение Подписки и аннулирование Сертификата», Подписка в этом случае не начинает действовать).

Подписчик:

- получает пакет с Сертификатом.
- аутентифицируется в личном кабинете ПДС (в присутствии Администратора безопасности ОКЗ), где ознакамливается с информацией, содержащейся в Сертификате и нажимает кнопку «Сертификат получен» (если информация, содержащаяся в Сертификате в ПДС не верна, то вносит в заявку на создание

Подписки данные о причине отказа в получении Сертификата. При этом исходящая информация поступает в подпроцесс «Сокращение Подписки и аннулирование Сертификата»).

Исходящая информация поступает в подпроцесс «Контроль действия Сертификата».

3.1.8. Подпроцесс «Контроль срока действия Сертификата»

Входящая информация поступает из подпроцессов «Создание Сертификата» и «Вручение Сертификата».

ПДС в автоматическом режиме контролирует сроки действия Сертификатов и инициирует процесс выпуска нового Сертификата для Подписчика за 90 дней до окончания срока действия старого Сертификата.

Исходящая информация поступает в подпроцесс «Создание Сертификата».

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 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”.

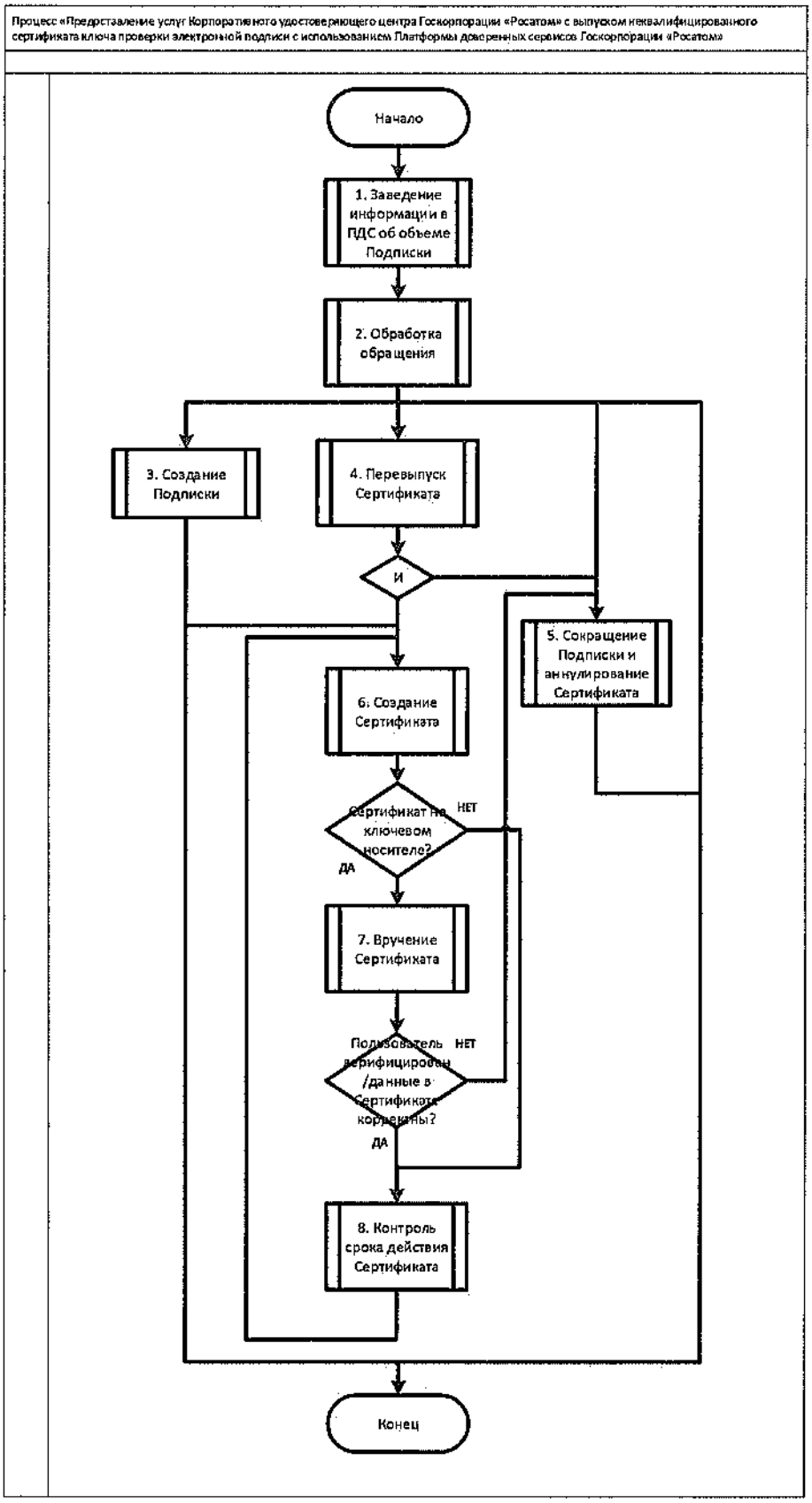
Приказ Госкорпорации «Росатом» от 04.12.2015 № 1/1176-П (с учётом изменений, внесённых приказом Госкорпорации «Росатом» от 26.07.2019 № 1/764-П).

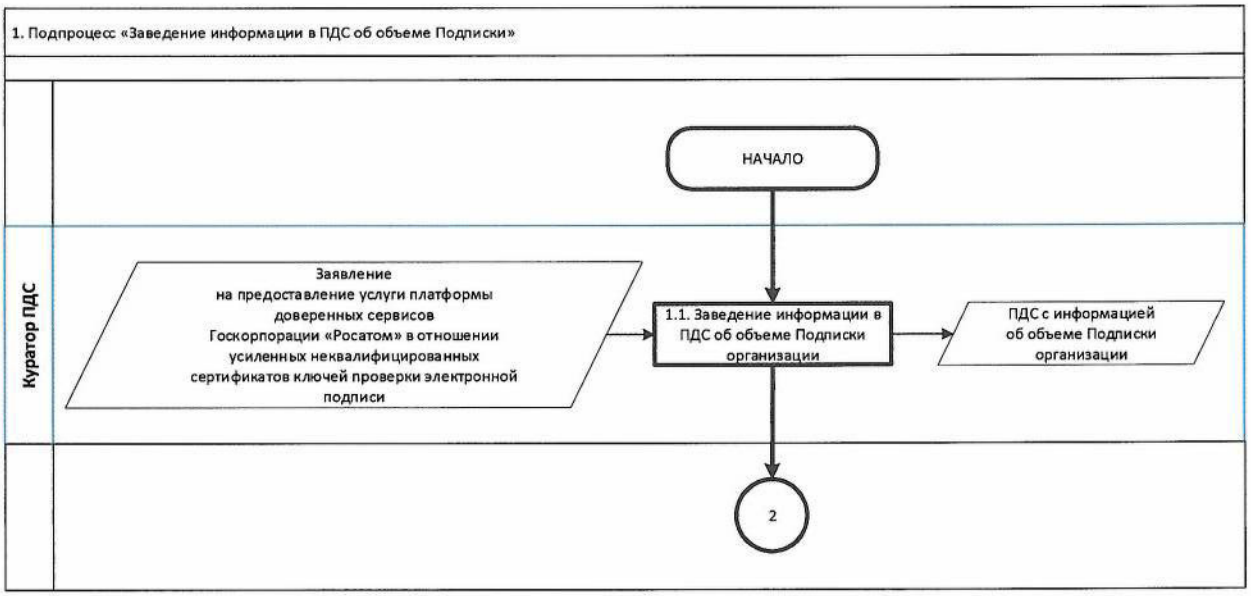
5. Перечень приложений

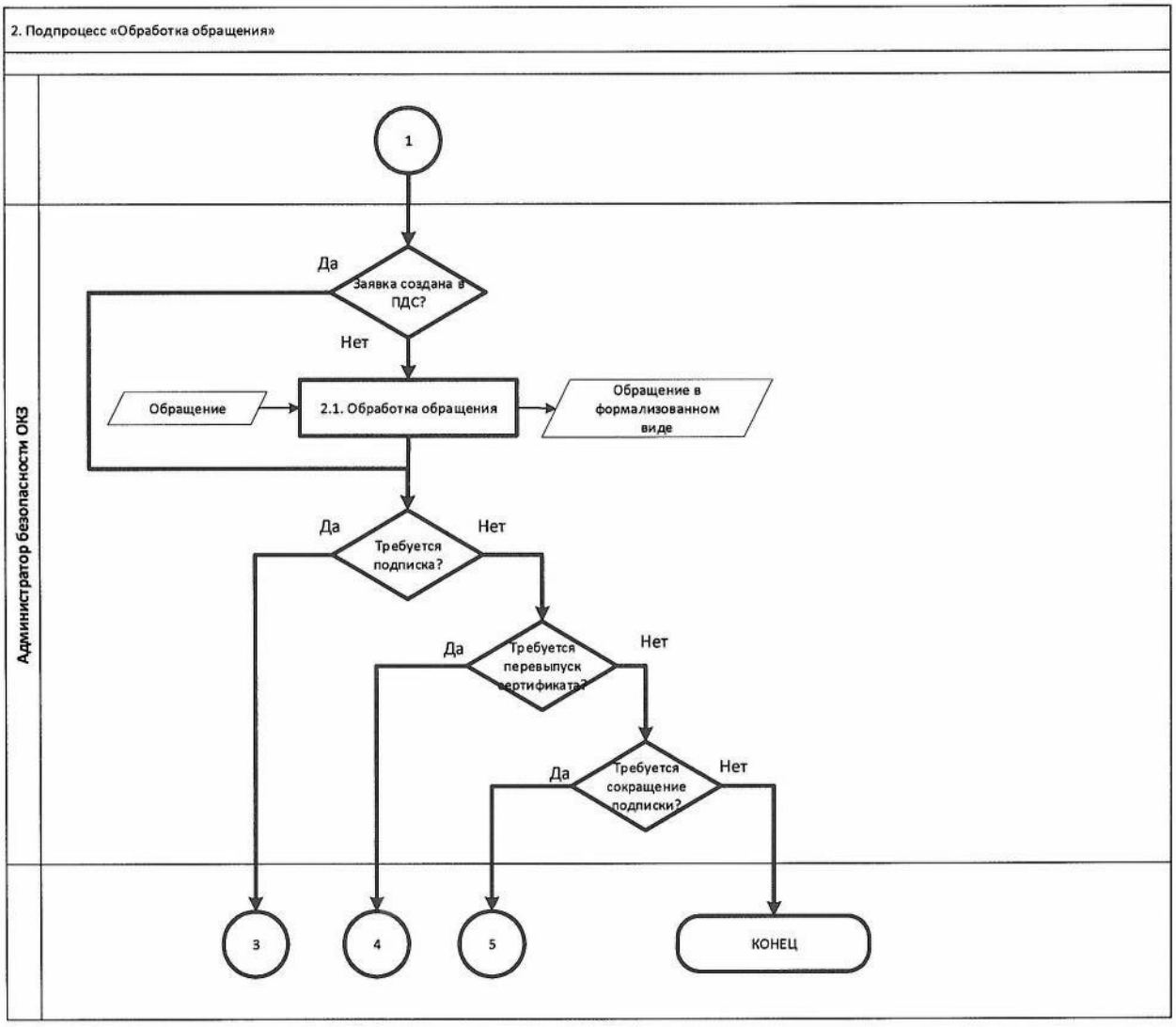
Приложение №1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом».

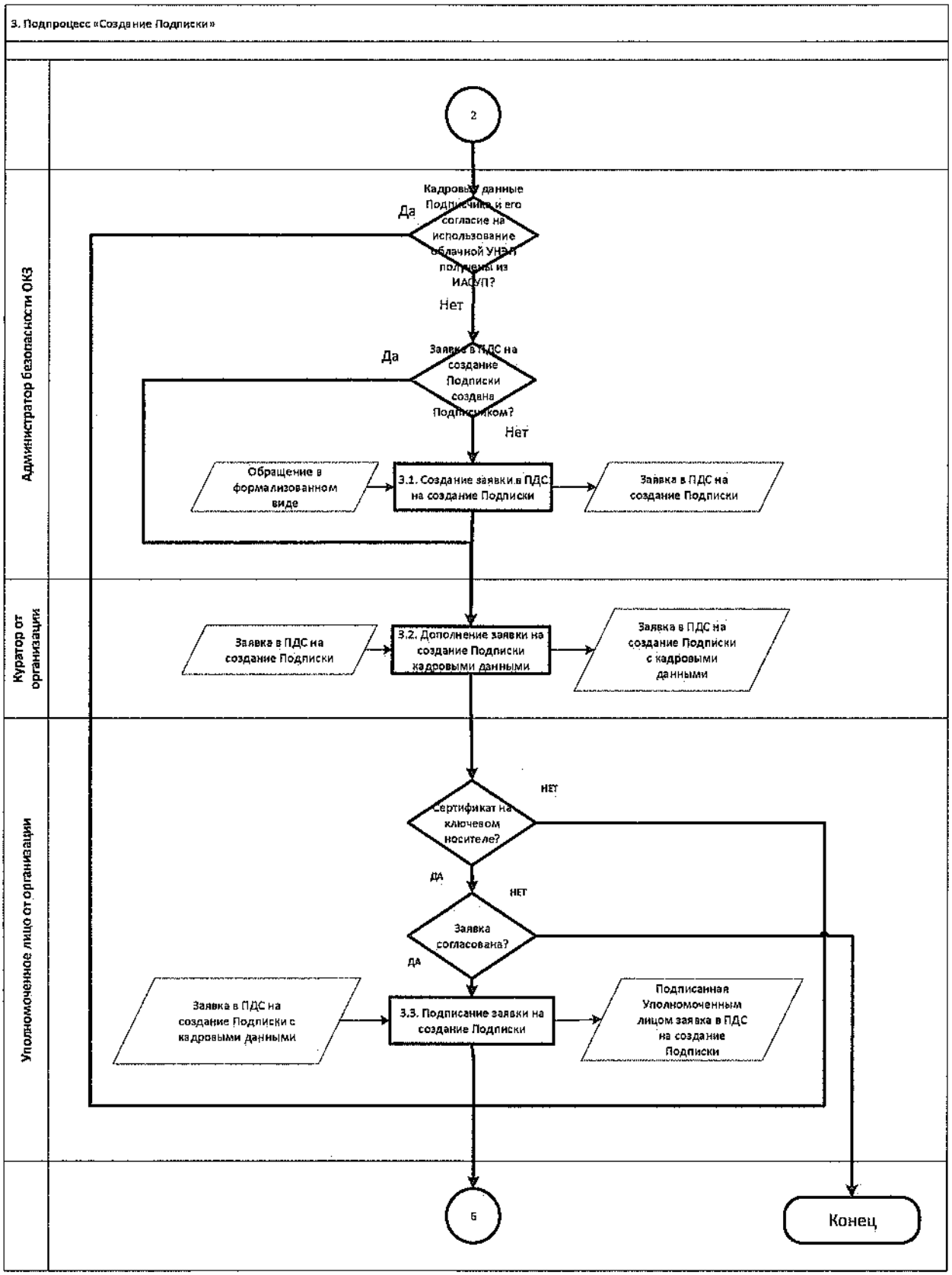
Приложение №2. Заявление на предоставление услуги.

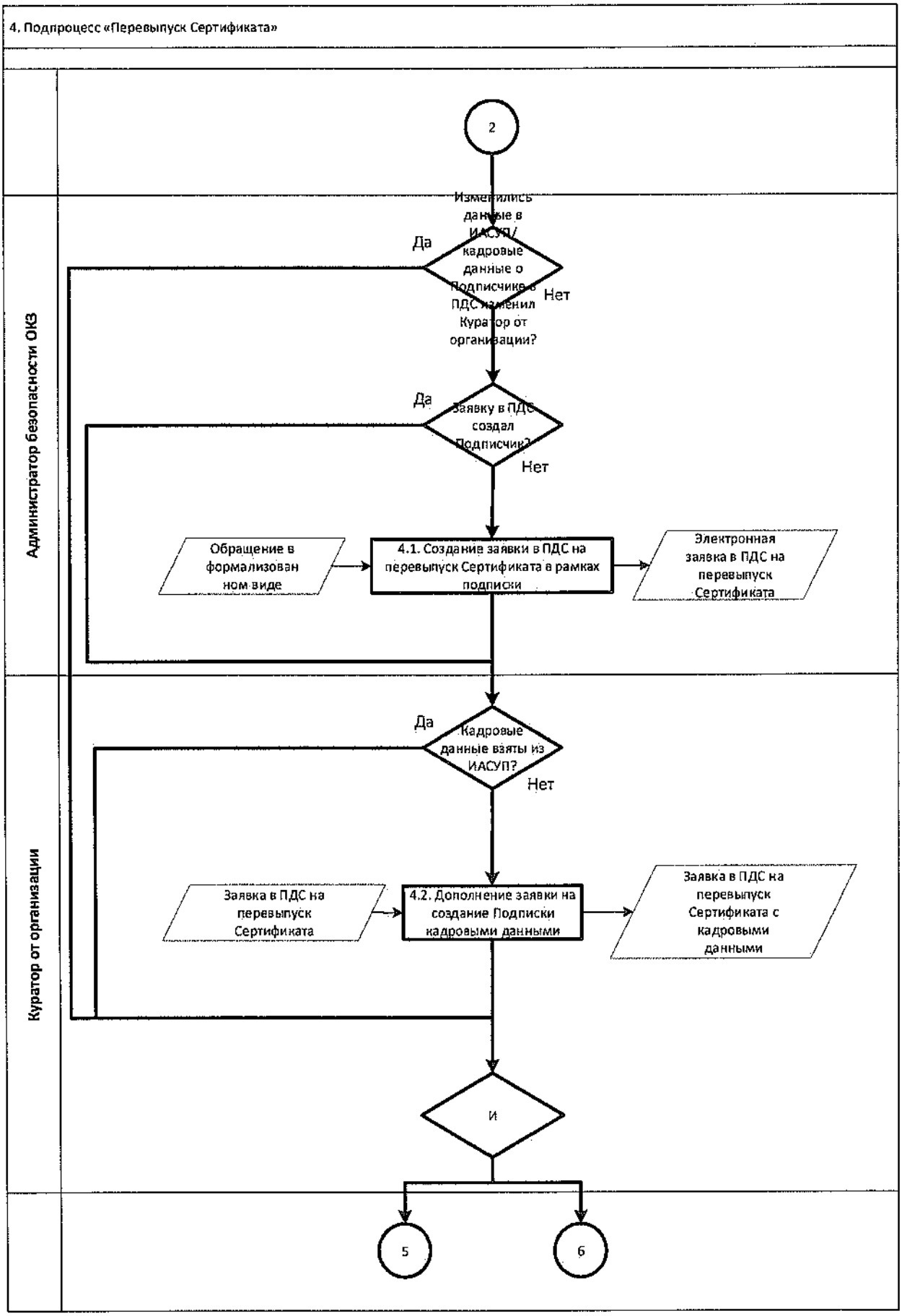
Приложение №1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом»

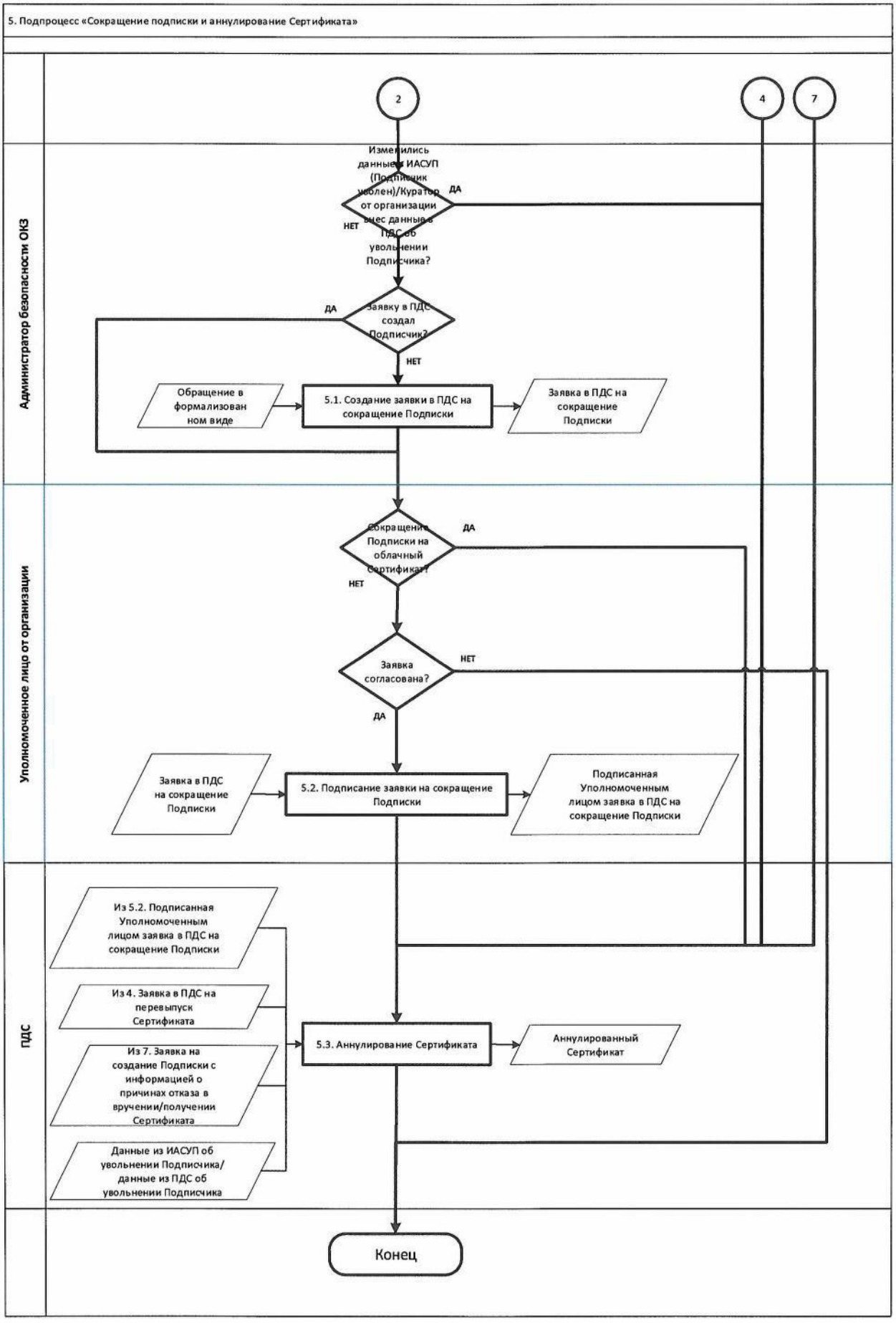


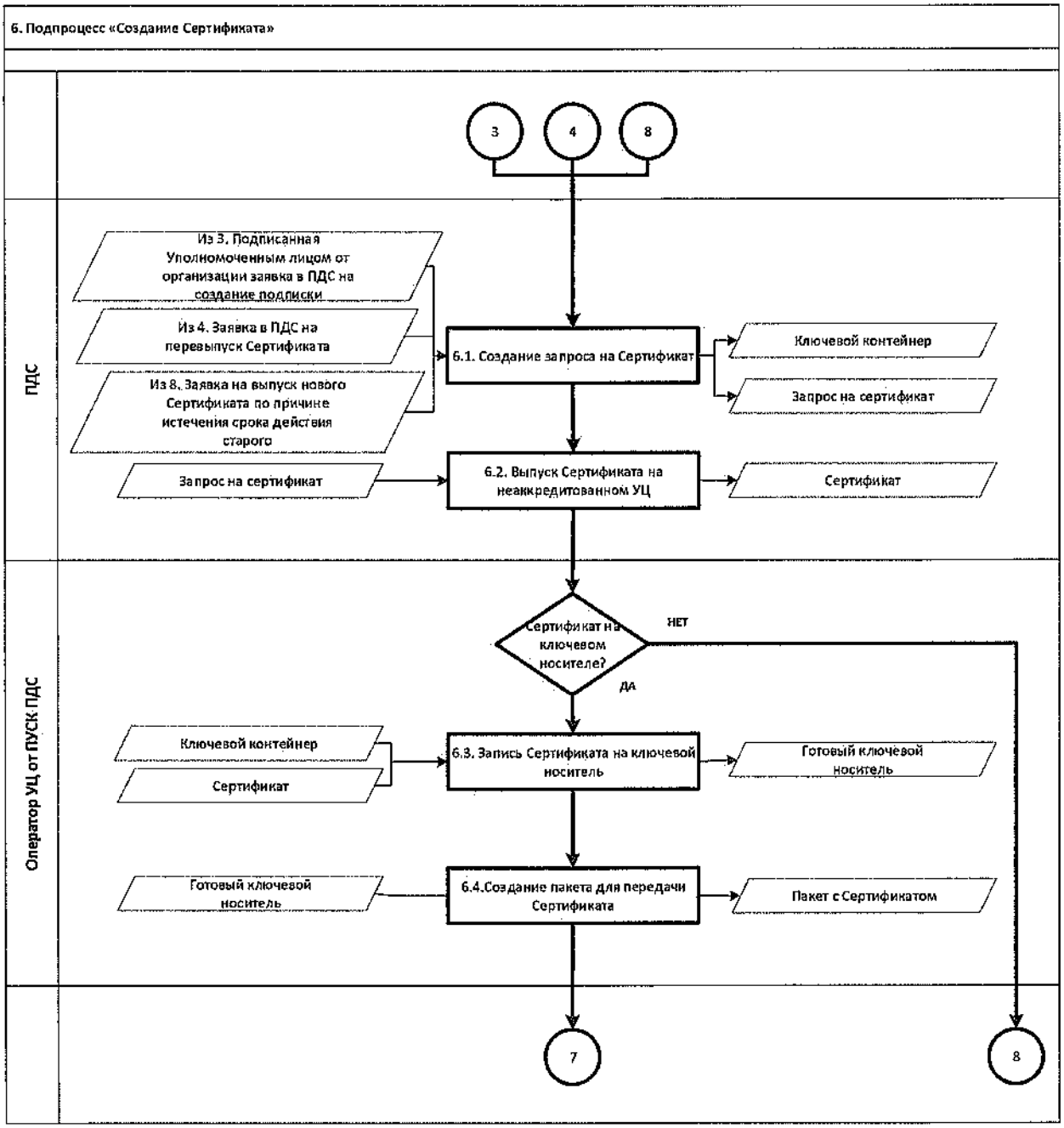

1. Подпроцесс «Заведение информации в ПДС об объеме Подписки»
Куратор ПДС
НАЧАЛО
Заявление на предоставление услуги платформы доверенных сервисов Госкорпорации «Росатом» в отношении усиленных неквалифицированных сертификатов ключей проверки электронной подписи
1.1. Заведение информации в ПДС об объеме Подписки организации
ПДС с информацией об объеме Подписки организации
2

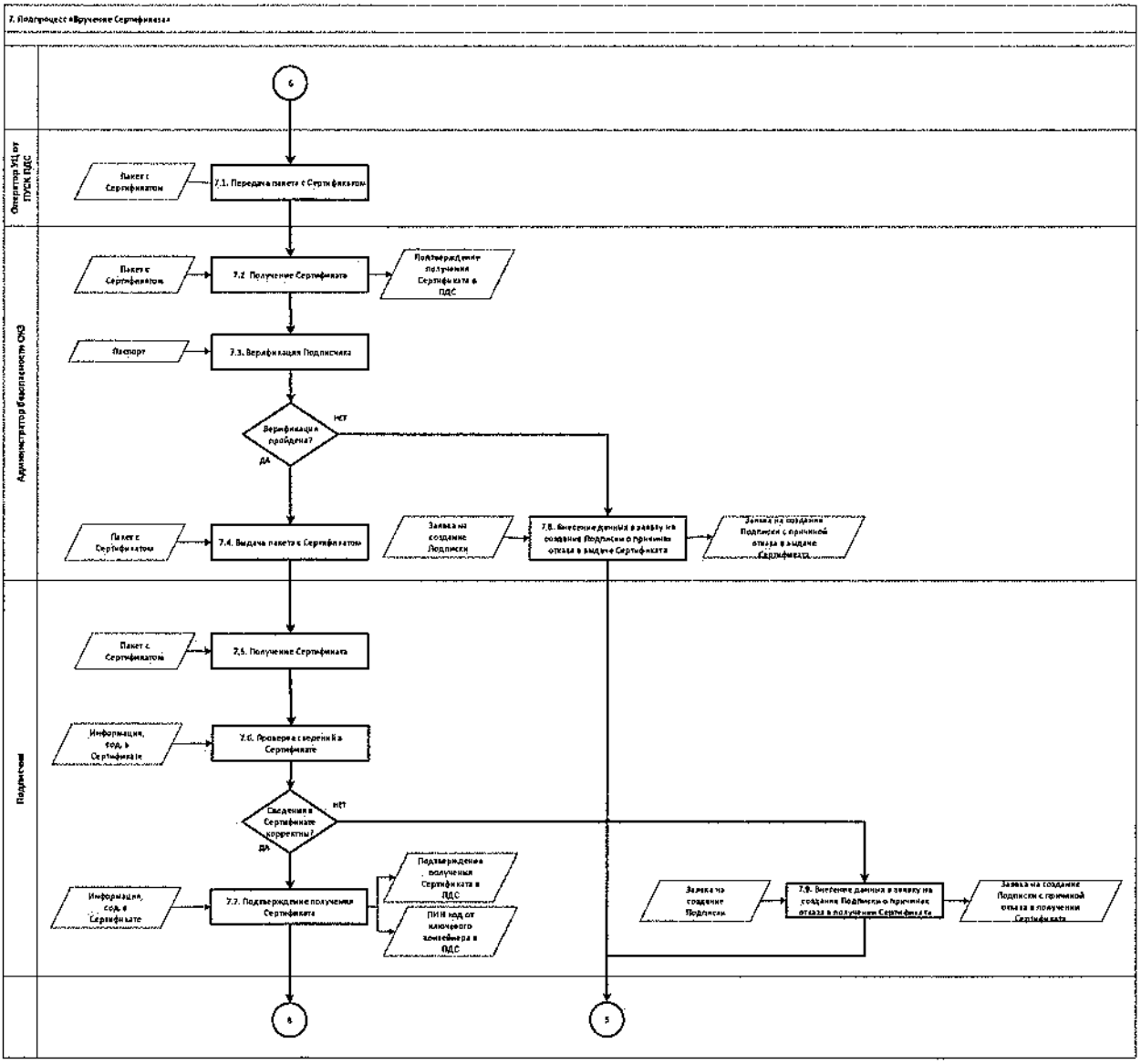

2. Подпроцесс «Обработка обращения»
Администратор безопасности ОКЗ
1
Да
Заявка создана в ПДС?
Нет
Обращение
2.1. Обработка обращения
Обращение в формализованном виде
Да
Требуется подписка?
Нет
Да
Требуется перевыпуск сертификата?
Нет
Да
Требуется сокращение подписки?
Нет
3
4
5
КОНЕЦ

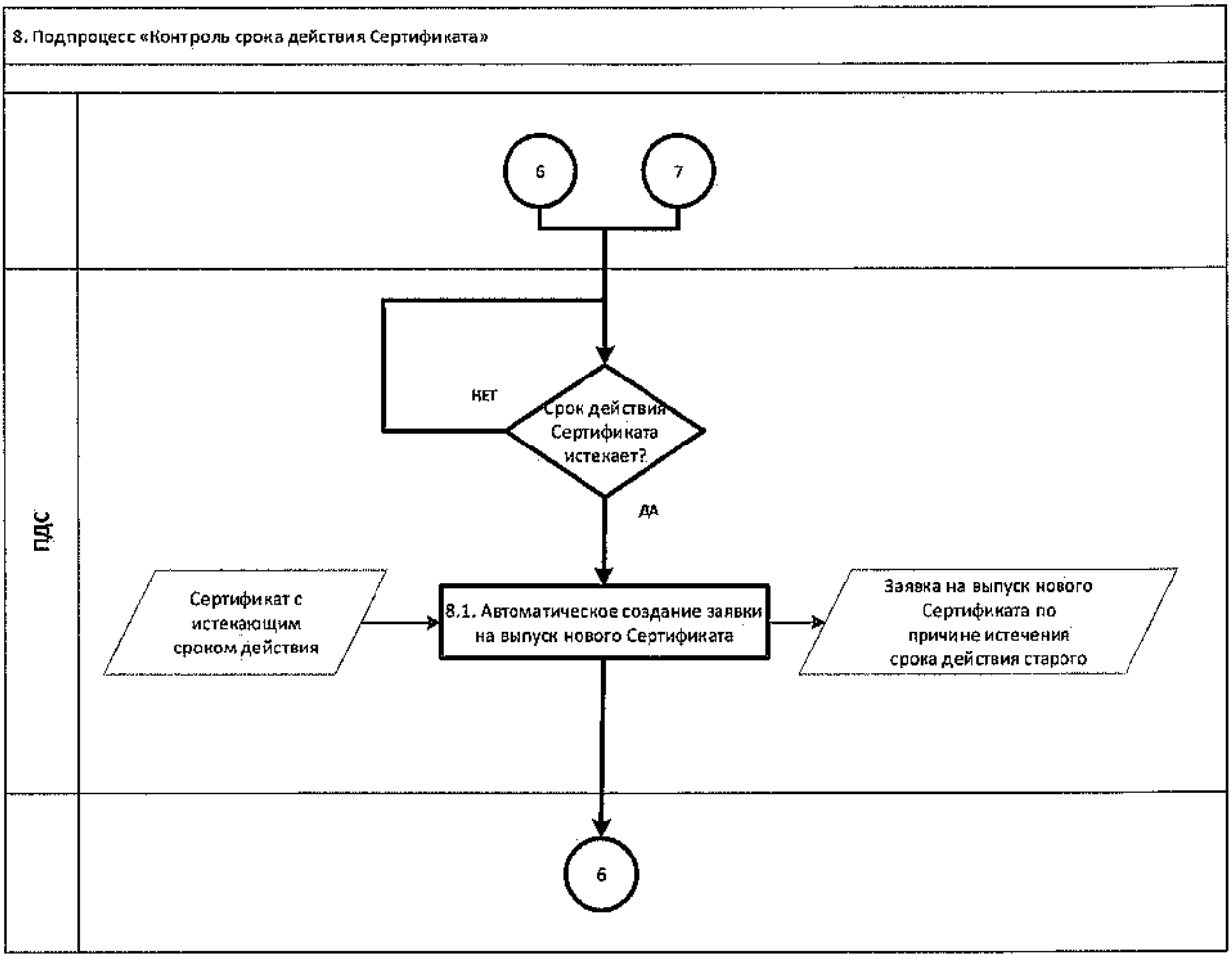

3. Подпроцесс «Создание Подписки»
Администратор безопасности ОКЗ
Куратор от организации
Уполномоченное лицо от организации
2
Кадровые данные Подписчика и его согласие на использование облачной УНЭП получены из ИАС УП?
Да
Нет
Заявка в ПДС на создание Подписки создана Подписчиком?
Да
Нет
Обращение в формализованном виде
3.1. Создание заявки в ПДС на создание Подписки
Заявка в ПДС на создание Подписки
Заявка в ПДС на создание Подписки
3.2. Дополнение заявки на создание Подписки кадровыми данными
Заявка в ПДС на создание Подписки с кадровыми данными
Сертификат на ключевом носителе?
НЕТ
ДА
Заявка согласована?
НЕТ
ДА
Заявка в ПДС на создание Подписки с кадровыми данными
3.3. Подписание заявки на создание Подписки
Подписанная Уполномоченным лицом заявка в ПДС на создание Подписки
6
Конец


4. Подпроцесс «Перевыпуск Сертификата»
Администратор безопасности ОКЗ
Куратор от организации
2
Изменились данные в ИАСУП/ кадровые данные о Подписчике в ПДС изменил Куратор от организации?
Да
Нет
Заявку в ПДС создал Подписчик?
Да
Нет
Обращение в формализованном виде
4.1. Создание заявки в ПДС на перевыпуск Сертификата в рамках подписки
Электронная заявка в ПДС на перевыпуск Сертификата
Кадровые данные взяты из ИАСУП?
Да
Нет
Заявка в ПДС на перевыпуск Сертификата
4.2. Дополнение заявки на создание Подписки кадровыми данными
Заявка в ПДС на перевыпуск Сертификата с кадровыми данными
И
5
6


5. Подпроцесс «Сокращение подписки и аннулирование Сертификата»
Администратор безопасности ОКЗ
Уполномоченное лицо от организации
ПДС
2
4
7
Изменились данные в ИАСУП (Подписчик уволен)/Куратор от организации внес данные в ПДС об увольнении Подписчика?
ДА
НЕТ
Заявку в ПДС создал Подписчик?
ДА
НЕТ
Обращение в формализованном виде
5.1. Создание заявки в ПДС на сокращение Подписки
Заявка в ПДС на сокращение Подписки
Сокращение Подписки на облачный Сертификат?
ДА
НЕТ
Заявка согласована?
НЕТ
ДА
Заявка в ПДС на сокращение Подписки
5.2. Подписание заявки на сокращение Подписки
Подписанная Уполномоченным лицом заявка в ПДС на сокращение Подписки
Из 5.2. Подписанная Уполномоченным лицом заявка в ПДС на сокращение Подписки
Из 4. Заявка в ПДС на перевыпуск Сертификата
Из 7. Заявка на создание Подписки с информацией о причинах отказа в вручении/получении Сертификата
Данные из ИАСУП об увольнении Подписчика/ данные из ПДС об увольнении Подписчика
5.3. Аннулирование Сертификата
Аннулированный Сертификат
Конец


6. Подпроцесс «Создание Сертификата»
ПДС
Оператор УЦ от ПУСК ПДС
3
4
8
Из 3. Подписанная Уполномоченным лицом от организации заявка в ПДС на создание подписки
Из 4. Заявка в ПДС на перевыпуск Сертификата
Из 8. Заявка на выпуск нового Сертификата по причине истечения срока действия старого
6.1. Создание запроса на Сертификат
Ключевой контейнер
Запрос на сертификат
Запрос на сертификат
6.2. Выпуск Сертификата на неаккредитованном УЦ
Сертификат
Сертификат на ключевом носителе?
НЕТ
ДА
Ключевой контейнер
Сертификат
6.3. Запись Сертификата на ключевой носитель
Готовый ключевой носитель
Готовый ключевой носитель
6.4.Создание пакета для передачи Сертификата
Пакет с Сертификатом
7
8


7. Подпроцесс «Вручение Сертификата»
Оператор УЦ от ПУСК ПДС
Администратор безопасности ОИЗ
Подписант
6
Пакет с Сертификатом
7.1. Передача пакета с Сертификатом
Пакет с Сертификатом
7.2. Получение Сертификата
Подтверждение получения Сертификата в ПДС
Паспорт
7.3. Верификация Подписанта
Верификация пройдена?
НЕТ
ДА
Пакет с Сертификатом
7.4. Выдача пакета с Сертификатом
Заявка на создание Подписи
7.8. Внесение данных в заявку на создание Подписи о причинах отказа в выдаче Сертификата
Заявка на создание Подписи с причиной отказа в выдаче Сертификата
Пакет с Сертификатом
7.5. Получение Сертификата
Информация, содержащаяся в Сертификате
7.6. Проверка сведений в Сертификате
Сведения в Сертификате корректны?
НЕТ
ДА
Информация, содержащаяся в Сертификате
7.7. Подтверждение получения Сертификата
Подтверждение получения Сертификата в ПДС
ПИН-код от ключевого контейнера в ПДС
Заявка на создание Подписи
7.9. Внесение данных в заявку на создание Подписи о причинах отказа в получении Сертификата
Заявка на создание Подписи с причиной отказа в получении Сертификата
6
5


8. Подпроцесс «Контроль срока действия Сертификата»
ПДС
6
7
НЕТ
Срок действия Сертификата истекает?
ДА
Сертификат с истекающим сроком действия
8.1. Автоматическое создание заявки на выпуск нового Сертификата
Заявка на выпуск нового Сертификата по причине истечения срока действия старого
6

Приложение №2. Заявление на предоставление услуги

Заявление
на предоставление услуги Платформы доверенных сервисов Госкорпорации «Росатом» по обеспечению усиленными неквалифицированными сертификатами ключей проверки электронной подписи

ПОДКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ (нужное подчеркнуть) « » 20 г.

_____

наименование организации, включая организационно-правовую форму

в лице _____

должность

_____

фамилия, имя, отчество

действующего на основании _____

в рамках оказания услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств запрашивает услугу по предоставлению пользователям автоматизированных информационных систем, подключенных к Платформе доверенных сервисов Госкорпорации «Росатом», сервисов, обеспечивающих функционал усиленной неквалифицированной электронной подписи, согласно перечню:

Тип Сертификата	Автоматизированная информационная система (список)	Количество Сертификатов

Уполномоченное лицо от организации

_____ _____ _____

(должность) (подпись) (ФИО)

М.П.

Приложение № 14 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю
Директор по информационным технологиям
АО «Гринатом»

/ А.Н. Киселёв /

М.П.

ПОРЯДОК

организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну
с использованием Платформы доверенных сервисов Госкорпорации «Росатом»

Москва 2021 г.

Оглавление

1. Назначение и область применения

1.1. Настоящий порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (далее – Порядок) разработан для установления последовательности действий по процессу группы процессов Управления информационными технологиями с целями установления правил и условий предоставления и пользования услугами органа криптографической защиты АО «Гринатом» (далее – ОКЗ) по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну с использованием Платформы доверенных сервисов Госкорпорации «Росатом».

Общая информация об ОКЗ размещена на официальном сайте Корпоративного удостоверяющего центра Госкорпорации «Росатом» https://crypto.rosatom.ru.

1.2. Соблюдение Порядка является обязательным для организаций-обладателей конфиденциальной информации (далее - ООКИ), использующих автоматизированные информационные системы, в которых хранится, обрабатывается и/или передается по каналам связи с использованием средств криптографической защиты информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну и обязательны для выполнения сотрудниками, исполняющими следующие функциональные роли:

1. Подписчик.
2. Уполномоченное лицо от организации.
4. Администратор безопасности ОКЗ.
5. Аналитик ОКЗ.
6. Проверяющий.

2. Термины, сокращения и аббревиатуры

2.1. Термины и определения

Термин	Определение
Администратор безопасности ОКЗ	Уполномоченный работник АО «Гринатом» (по договору) или уполномоченный работник организации-заказчика, наделенный полномочиями по: формированию обращений в ПДС на создание, изменение и сокращение подписки предприятия; осуществлению проверки готовности СКЗИ к эксплуатации;

	выполнению монтажа, установке (инсталляции) криптографических средств; учету СКЗИ в ПДС; уничтожению выведенных из действия СКЗИ
Аналитик ОКЗ	Уполномоченный работник АО «Гринатом» (по договору), наделенный полномочиями по: согласованию и подписанию электронных заявок в ПДС на создание и сокращение подписок предприятий; разработку и поддержание в актуальном состоянии схемы криптографической защиты информации в ПДС; выделению лицензий СКЗИ для предприятий в ПДС; составлению заключений о возможности эксплуатации СКЗИ.
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 АО «Гринатом»	Действующая на постоянной основе рабочая группа из числа сотрудников Управления информационной безопасности
Подписка	Заказ предприятия в ПДС в соответствии с условиями договора присоединения на обеспечение сертификатами или средствами криптографической защиты и информации.
Подписчик, Пользователь СКЗИ	Физическое лицо, для которого оформлена подписка на обеспечение сертификатом и (или) лицензией на средство криптографической защиты информации (обладает учётной записью в домене GK, допущен к работе с СКЗИ, создаёт

	обращения, получает СКЗИ, проходит обучение в ПДС и сдает тестирование)
Средства криптографической защиты информации (СКЗИ)	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
Уполномоченное лицо от организации	Работник юридического лица, указанный в ЕГРЮЛ и имеющий возможность обращаться в Удостоверяющий центр и Орган криптографической защиты от имени юридического лица, либо работник имеющий право действовать от имени юридического лица на основании доверенности (согласовывает и подписывает электронные заявки в ПДС на создание и сокращение подписки организации)
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

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

Сокращение	Расшифровка
АБ	Администратор безопасности ОКЗ
АРМ	Автоматизированное рабочее место
ОКЗ	Орган криптографической защиты АО «Гринатом»
ПДС	Платформа доверенных сервисов «Госкорпорации «Росатом»
СКЗИ	Средство криптографической защиты информации

3. Описание процесса

Описание процесса организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну с использованием ПДС.

3.1. Описание подпроцессов

3.1.1. Подпроцесс «Обработка обращения»

АБ:

- получает обращение от следующих возможных инициаторов:
  Пользователь СКЗИ;
  АБ;
  Уполномоченное лицо предприятия;
  Аналитик ОКЗ,

одним из следующих способов:
  заявка через СУ ИТ;
  электронное письмо на п/я 1111@greenatom.ru;
  звонок в центр поддержки пользователей АО «Гринатом»;

- определяет наличие Подписки у пользователя, указанного в обращении;
- формализует обращение в зависимости от следующих условий:

в случае если Подписка на пользователя, указанного в обращении, отсутствует и обращение не на создание подписки, то процесс завершается;

в случае если Подписка на пользователя, указанного в обращении, отсутствует и обращение на создание подписки, то исходящая информация поступает в подпроцесс «Создание подписки»;

в случае если Подписка на пользователя, указанного в обращении, есть, и обращение на переустановку СКЗИ, то исходящая информация поступает в подпроцесс «Проверка готовности»;

в случае если Подписка на пользователя, указанного в обращении, есть, и обращение не на переустановку СКЗИ, а на сокращение подписки, то исходящая информация поступает в подпроцесс «Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки»;

в случае если Подписка на пользователя, указанного в обращении, есть, и обращение не на переустановку СКЗИ, и не на сокращение подписки, то исходящая информация поступает в подпроцесс «Обеспечение функционирования».

3.1.2. Подпроцесс «Создание подписки»

Входящая информация поступает из подпроцесса «Обработка обращения».

АБ:

- формирует электронную заявку на новую Подписку в ПДС;

Уполномоченное лицо от организации:

- получает электронную заявку на создание Подписки в ПДС;
- подписывает заявку на создание Подписки, *в случае если заявка им согласована.*

В случае если заявка на создание Подписки не согласована, то процесс завершается.

Аналитик ОКЗ:

- получает подписанную Уполномоченным лицом от организации электронную заявку в ПДС на создание Подписки;
- подписывает заявку на создание Подписки, *в случае если заявка им согласована.*

В случае если заявка не согласована, процесс завершается.

Исходящая информация поступает в подпроцесс «Передача СКЗИ».

3.1.3. Подпроцесс «Передача СКЗИ»

Входящая информация поступает из подпроцесса «Создание подписки».

Аналитик:

- выделяет лицензию на СКЗИ согласно полученной заявке.

Лицензия на СКЗИ поступает АБ в ПДС. Дистрибутив на СКЗИ и эксплуатационная техническая документация доступны для загрузки в ПДС.

Исходящая информация поступает в подпроцесс «Проверка готовности».

3.1.4. Подпроцесс «Проверка готовности»

Входящая информация поступает из подпроцессов «Передача СКЗИ» и «Обработка обращения».

АБ:

- осуществляет проверку готовности технических средств и вносит в ПДС информацию по АРМ:

  серийный/инвентарный номер АРМ;
  адрес месторасположения АРМ;
  вид обрабатываемой информации;

область использования СКЗИ;
ФИО пользователя СКЗИ;
номер опечатывающей пломбы;
версию и наименование операционной системы;
версию и наименование сертифицированного антивирусного средства;
версию и наименование сертифицированного СЗИ от НСД;
о настройке СКЗИ в соответствии с документацией на него (ставит отметку);

- формирует приказ о допуске пользователя к самостоятельной работе с СКЗИ и вносит информацию о приказе в ПДС.

Исходящая информация поступает в подпроцесс «Монтаж, установка (инсталляция) криптографических средств».

3.1.5. Подпроцесс «Монтаж, установка (инсталляция) СКЗИ»

Входящая информация поступает из подпроцесса «Проверка готовности».

АБ:

- устанавливает и настраивает СКЗИ в соответствии с Инструкцией по установке СКЗИ (лицензия и дистрибутив для загрузки доступны в ПДС);
- устанавливает ПО «Агент ПДС» (дистрибутив для загрузки доступен в ПДС).

Исходящая информация поступает в подпроцесс «Обучение и допуск пользователя».

3.1.6. Подпроцесс «Обучение и допуск пользователя»

Входящая информация поступает из подпроцесса «Монтаж, установка (инсталляция) СКЗИ».

Пользователь СКЗИ:
- получает по электронной почте уведомление о назначении ему в ПДС курса обучения правилам работы с СКЗИ;
- проходит обучение в ПДС;
- сдает тестирование по итогам обучения.

Активация СКЗИ не произойдет до тех пор, пока пользователь не пройдет назначенный ему курс обучения и не сдаст тестирование по пройденному материалу в ПДС.

В случае получения положительного результата по итогам прохождения тестирования происходит активация СКЗИ, и исходящая информация поступает в подпроцесс «Учет СКЗИ».

В случае получения отрицательного результата по итогам прохождения тестирования, требуется повторно ознакомиться с учебными материалами и снова пройти тестирование.

3.1.7. Подпроцесс «Учет СКЗИ»

Входящая информация поступает из подпроцесса «Обучение и допуск пользователя» или из подпроцесса «Вывод из эксплуатации, уничтожение СКЗИ».

АБ (в случае если информация поступает из подпроцесса «Обучение и допуск пользователя»):

- проверяет наличие приказа о допуске Пользователя СКЗИ к самостоятельной работе с СКЗИ, вносит его реквизиты в ПДС;
- проверяет наличие у Пользователя СКЗИ отметки об успешном прохождении обучения в ПДС;
- проверяет актуальность данных в ПДС по АРМ, Пользователю СКЗИ и установленным СКЗИ;
- закрепляет полученную лицензию на СКЗИ в ПДС за АРМ и Пользователем СКЗИ.

На основании заполненных АБ данных в ПДС происходит актуализация схемы криптографической защиты информации.

Исходящая информация поступает в подпроцесс «Обеспечение функционирования».

АБ (в случае если информация поступает из подпроцесса «Вывод из эксплуатации, уничтожение СКЗИ»):

- ставит отметку в ПДС об уничтожении СКЗИ.

В случае если подписка сокращена, процесс завершается.

3.1.8. Подпроцесс «Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки»

Входящая информация поступает из подпроцесса «Обработка обращения».

АБ:

- формирует заявку на сокращение Подписки в ПДС.

Уполномоченное лицо от организации:

- получает электронную заявку на сокращение Подписки в ПДС;
- подписывает заявку на сокращение подписки, *в случае если заявка им согласована.*

Если заявка на сокращение подписки не согласована, то исходящая информация поступает в подпроцесс «Обеспечения функционирования».

Если заявка на сокращение подписки подписана Уполномоченным лицом от организации, то АБ:

- изымает СКЗИ из аппаратных средств, с которыми они функционировали. При этом СКЗИ считается изъятым из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ, и он полностью отсоединен от аппаратных средств и уничтожает СКЗИ.

Уничтожение должно происходить путем физического уничтожения или путем стирания (разрушения), исключающего возможность их использования, а также восстановления. Непосредственные действия по уничтожению конкретного типа СКЗИ регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями ОКЗ.

СКЗИ должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации. Если срок уничтожения эксплуатационной и технической документацией не установлен, то СКЗИ должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия).

Исходящая информация поступает в подпроцесс «Учет СКЗИ».

3.1.9. Подпроцесс «Обеспечение функционирования»

Входящая информация поступает из подпроцессов «Обработка обращения», «Учет СКЗИ», «Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки».

Функционирование и безопасность применения СКЗИ обеспечивается в соответствии с условиями выданных на них сертификатов соответствия ФСБ России, а также в соответствии с эксплуатационной и технической документацией к этим средствам.

Оригиналы выданных сертификатов соответствия ФСБ России на СКЗИ находятся в ОКЗ АО «Гринатом», копии находятся в ПДС.

АБ (в случае если информация поступает из подпроцесса «Обработка обращения»):

- получает в ПДС заявку (не реже раза в год) на проведение проверки порядка использования СКЗИ в соответствии с эксплуатационной и технической документацией. В состав проверки входит:

  соответствие номеров СКЗИ данным в ПДС;

  соответствие настроек системного ПО, СКЗИ и мер физической защиты СКЗИ требованиям документации к СКЗИ;

  наличие носителей ключевой информации и их соответствие данным, указанным в ПДС;

  наличие актуального приказа о допуске пользователей к самостоятельной работе с СКЗИ.
- в случае необходимости актуализирует данные в ПДС.

Аналитик (в случае если информация поступает из подпроцессов «Учет СКЗИ» или «Обработка обращения»):

- формирует заключение о возможности эксплуатации СКЗИ.

Заключение выдается сроком на 1 год, в случае сохранения доверенной среды функционирования СКЗИ, подтвержденной данными в ПДС.

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.№15686 Н 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);

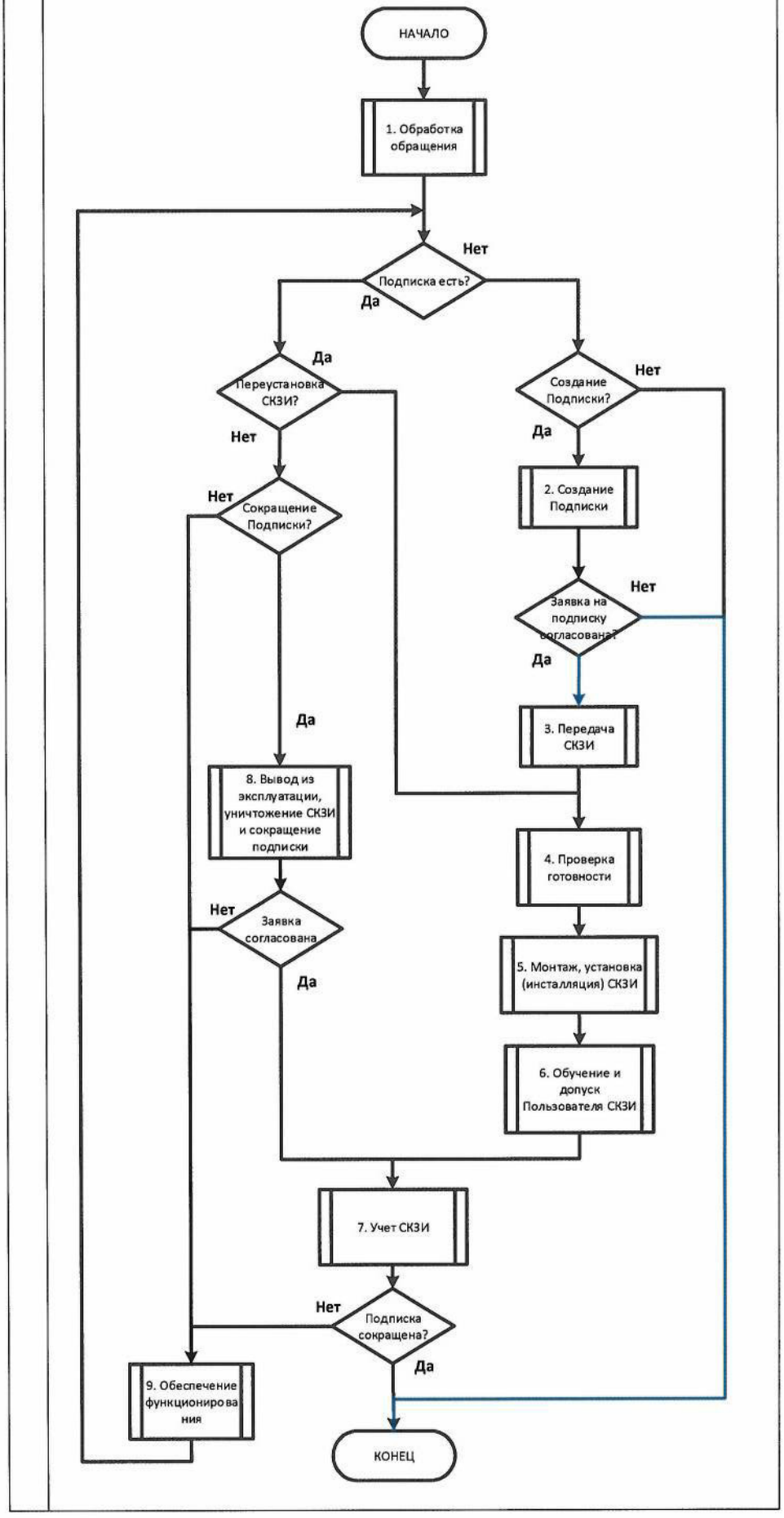
- Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» (с пометкой «Для служебного пользования»);
- Постановление №313 от 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);
- Приказ Госкорпорации «Росатом» от 04.12.2015 № 1/1176-П (с учётом изменений, внесённых приказом Госкорпорации «Росатом» от 26.07.2019 № 1/764-П).

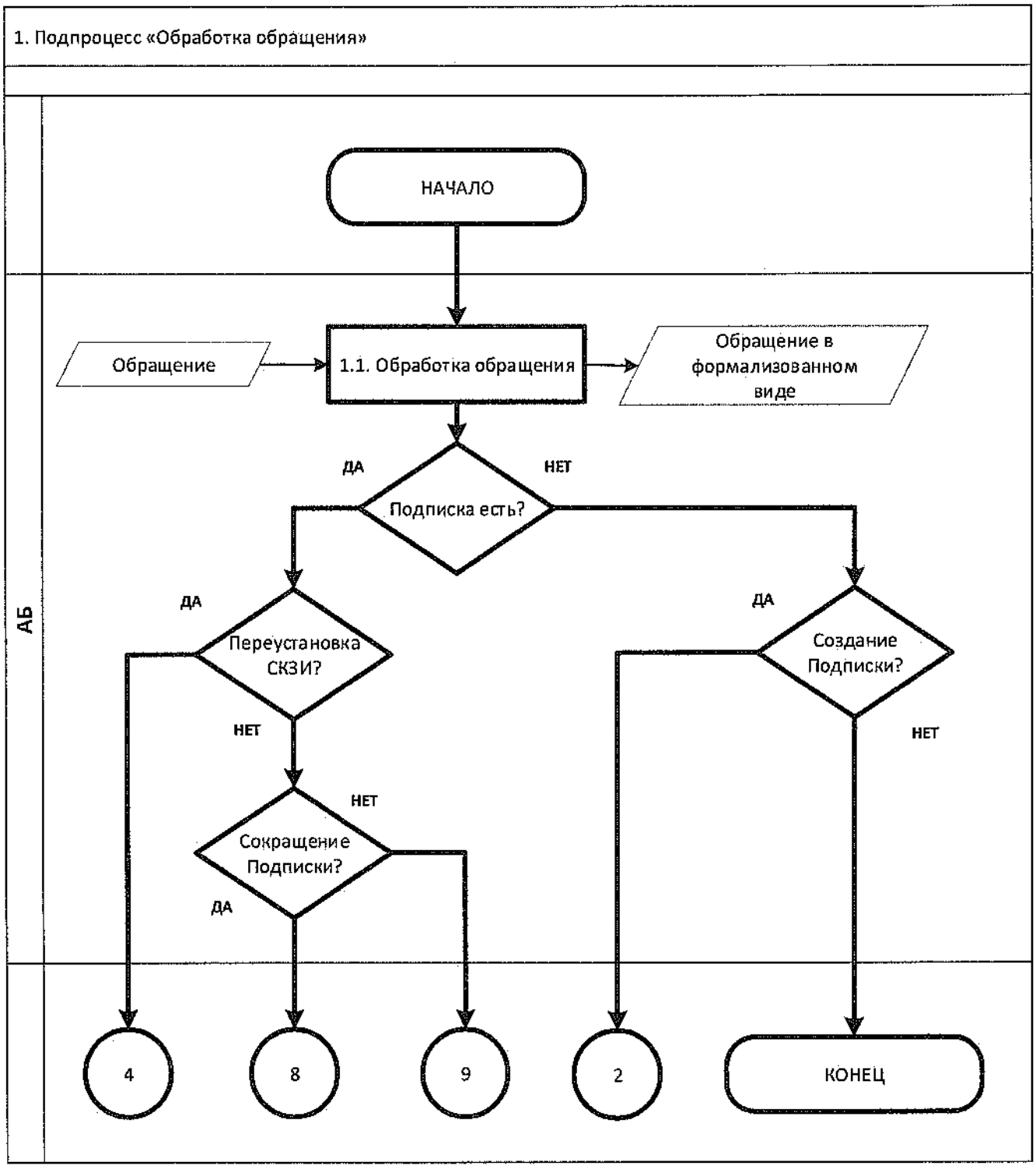
5. Перечень приложений

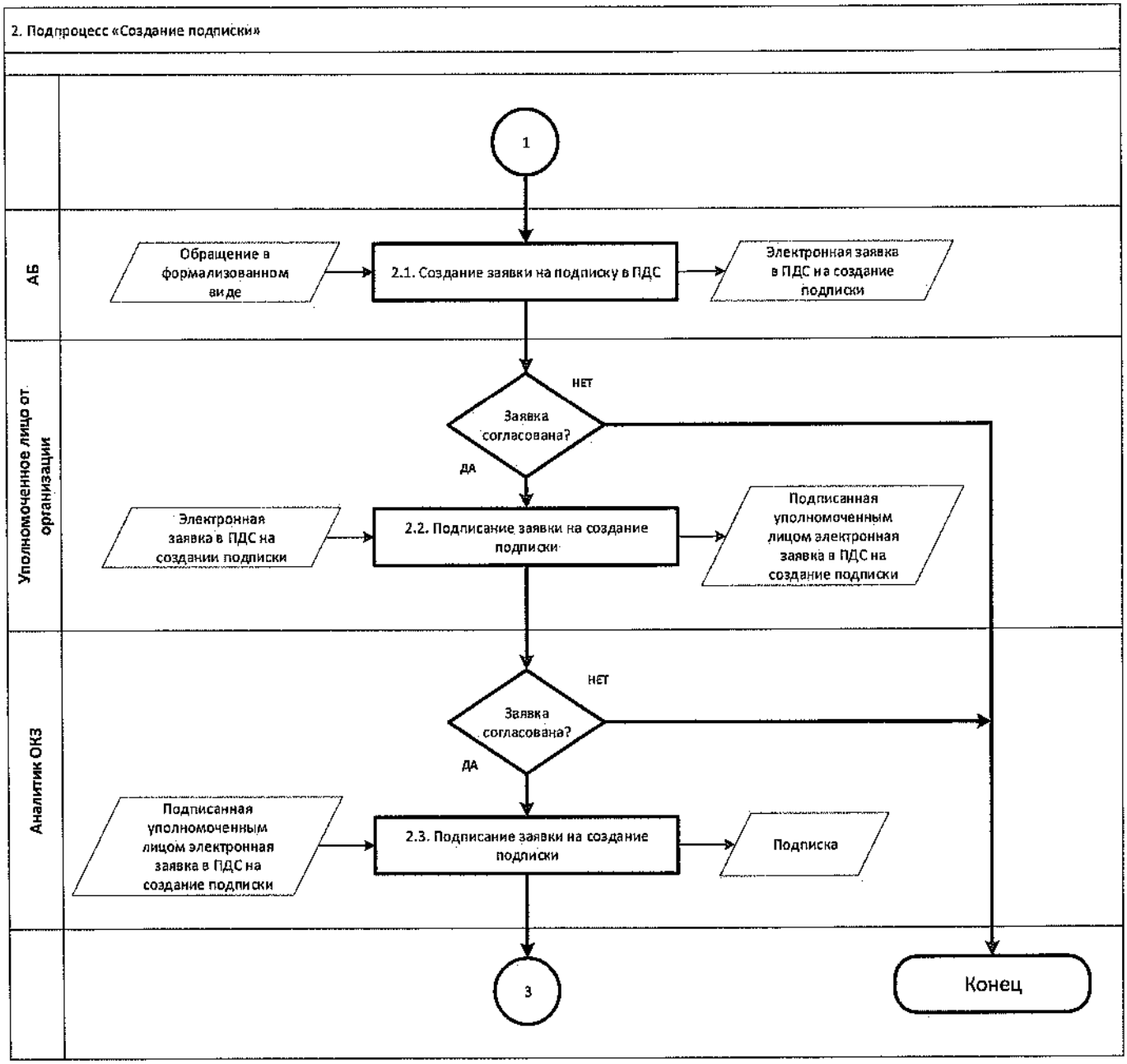
Приложение №1. Схема процесса.

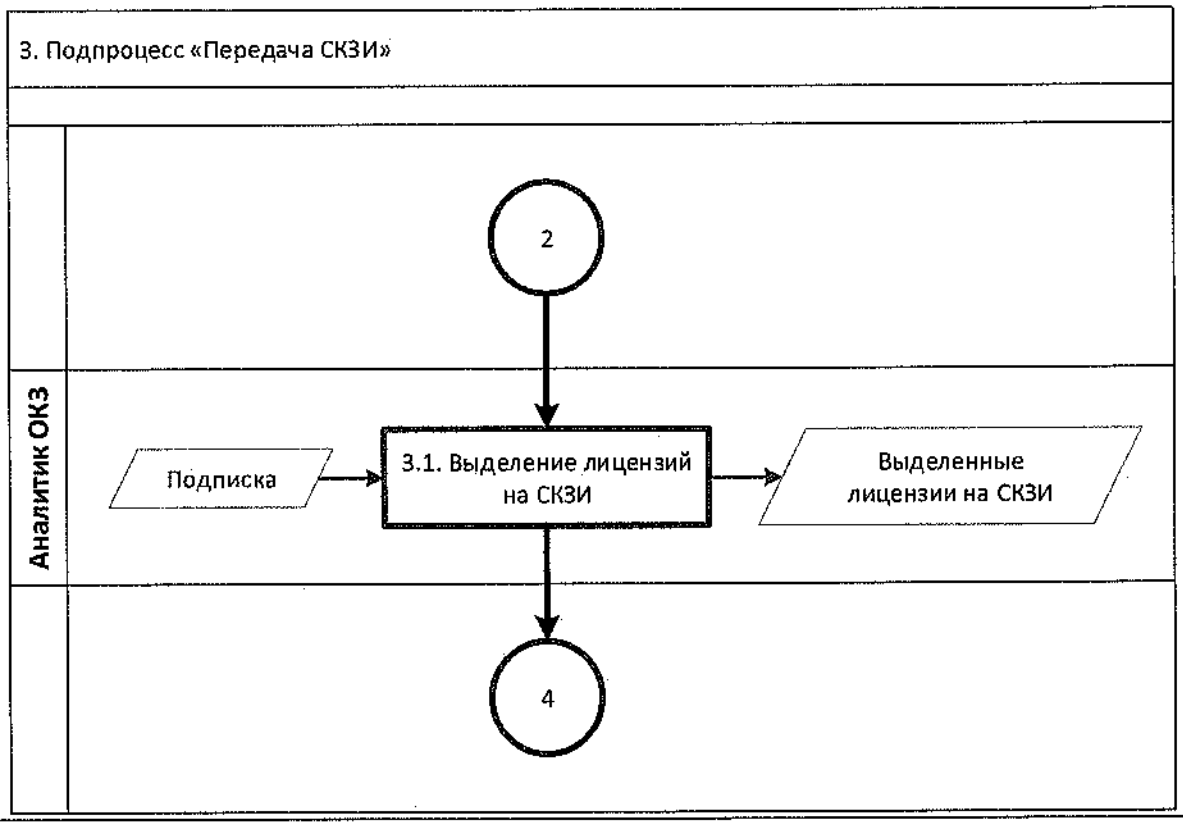
Приложение №1. Схема процесса

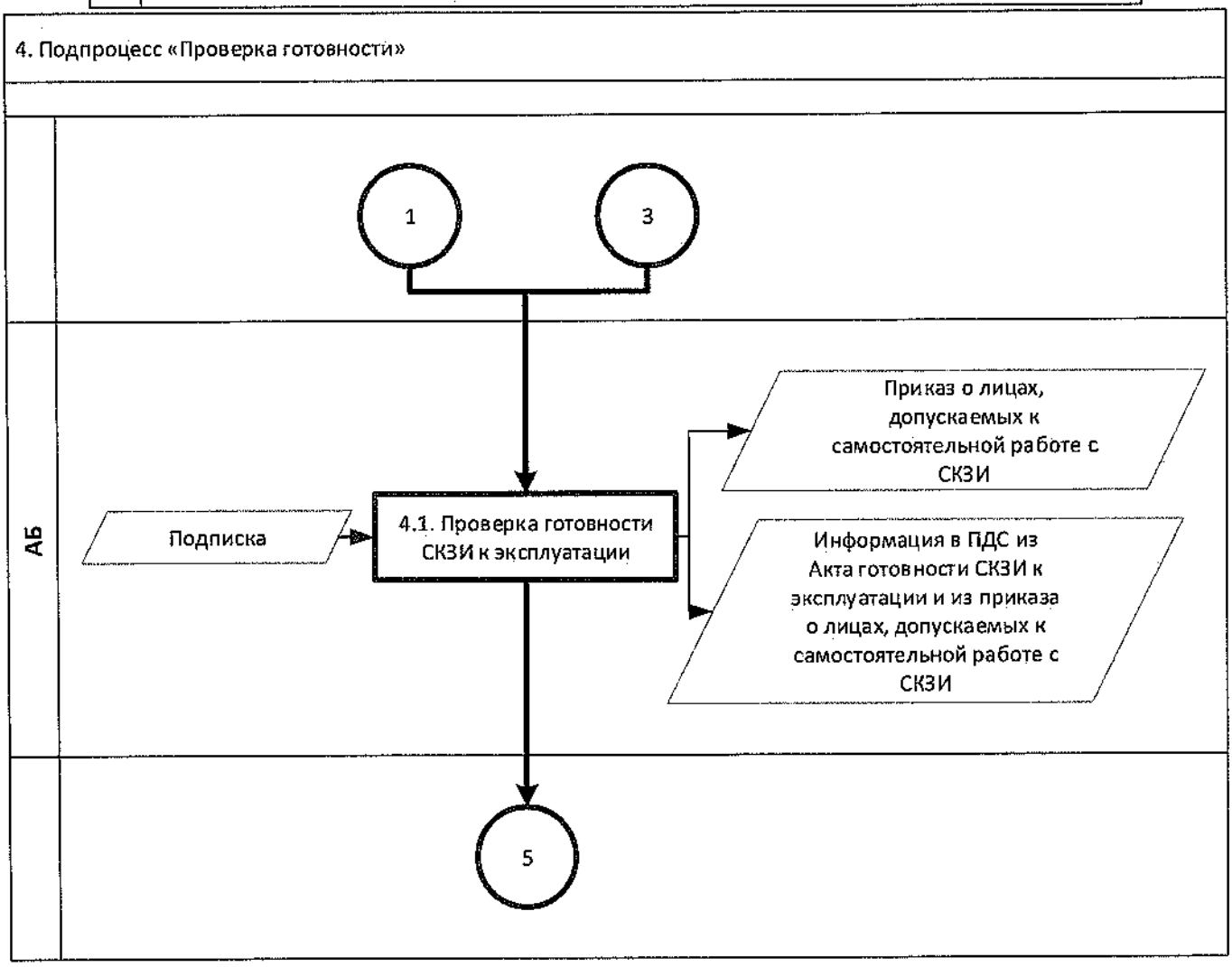
Процесс «Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну с использованием Платформы доверенных сервисов Госкорпорации «Росатом»

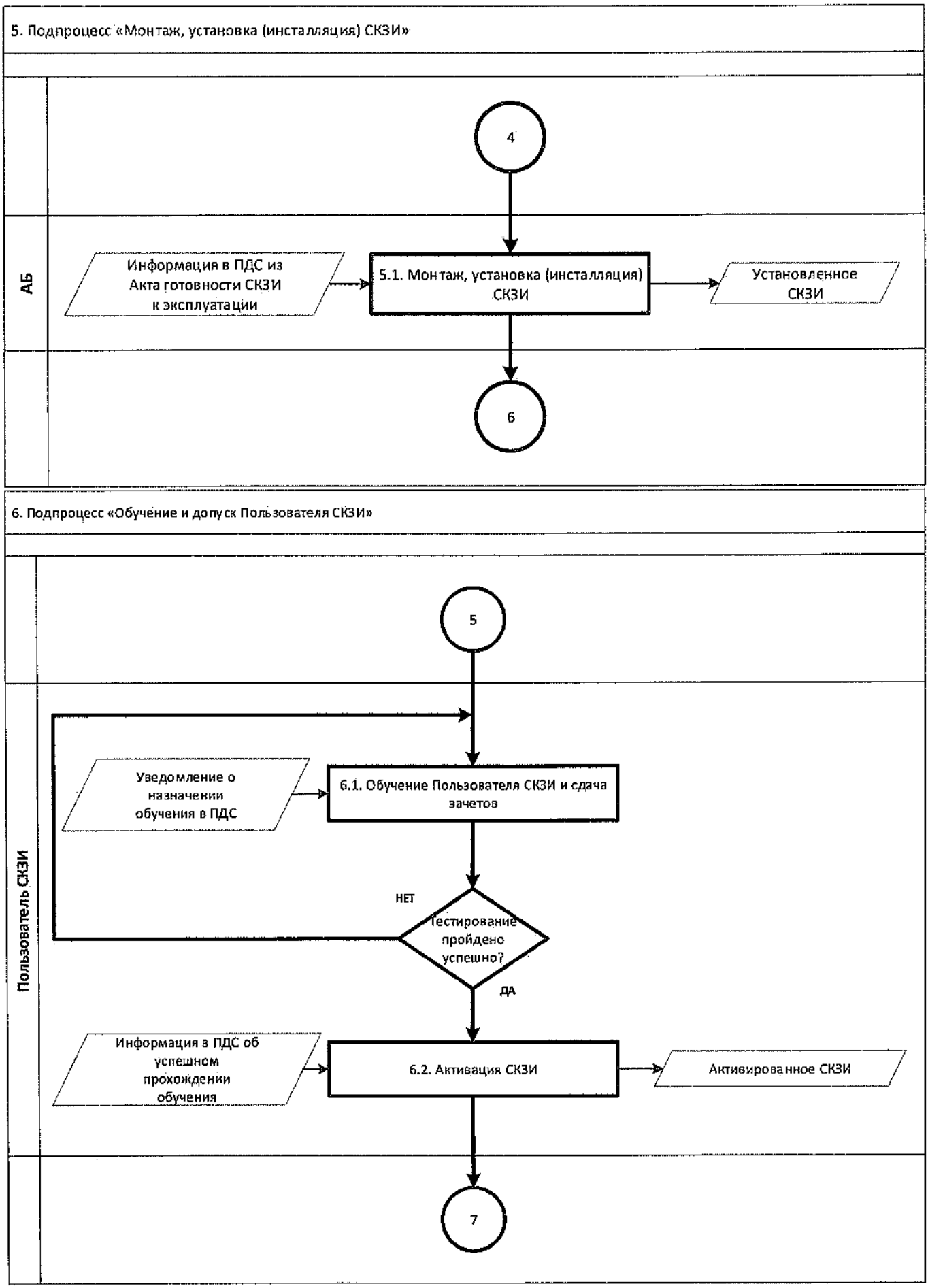


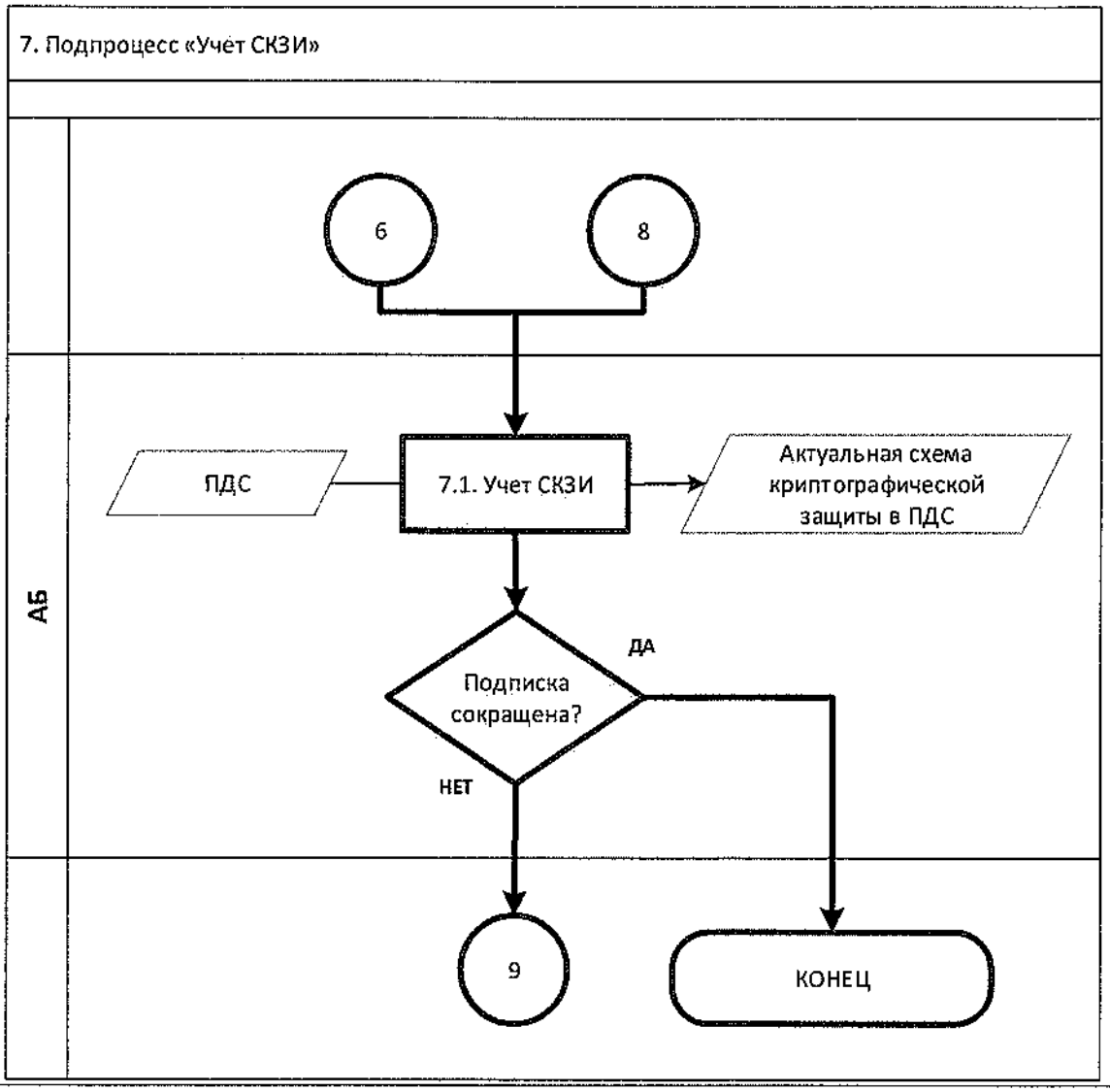

1. Подпроцесс «Обработка обращения»
АБ
НАЧАЛО
Обращение
1.1. Обработка обращения
Обращение в формализованном виде
ДА
НЕТ
Подписка есть?
ДА
Переустановка СКЗИ?
НЕТ
НЕТ
Сокращение Подписки?
ДА
ДА
Создание Подписки?
НЕТ
4
8
9
2
КОНЕЦ

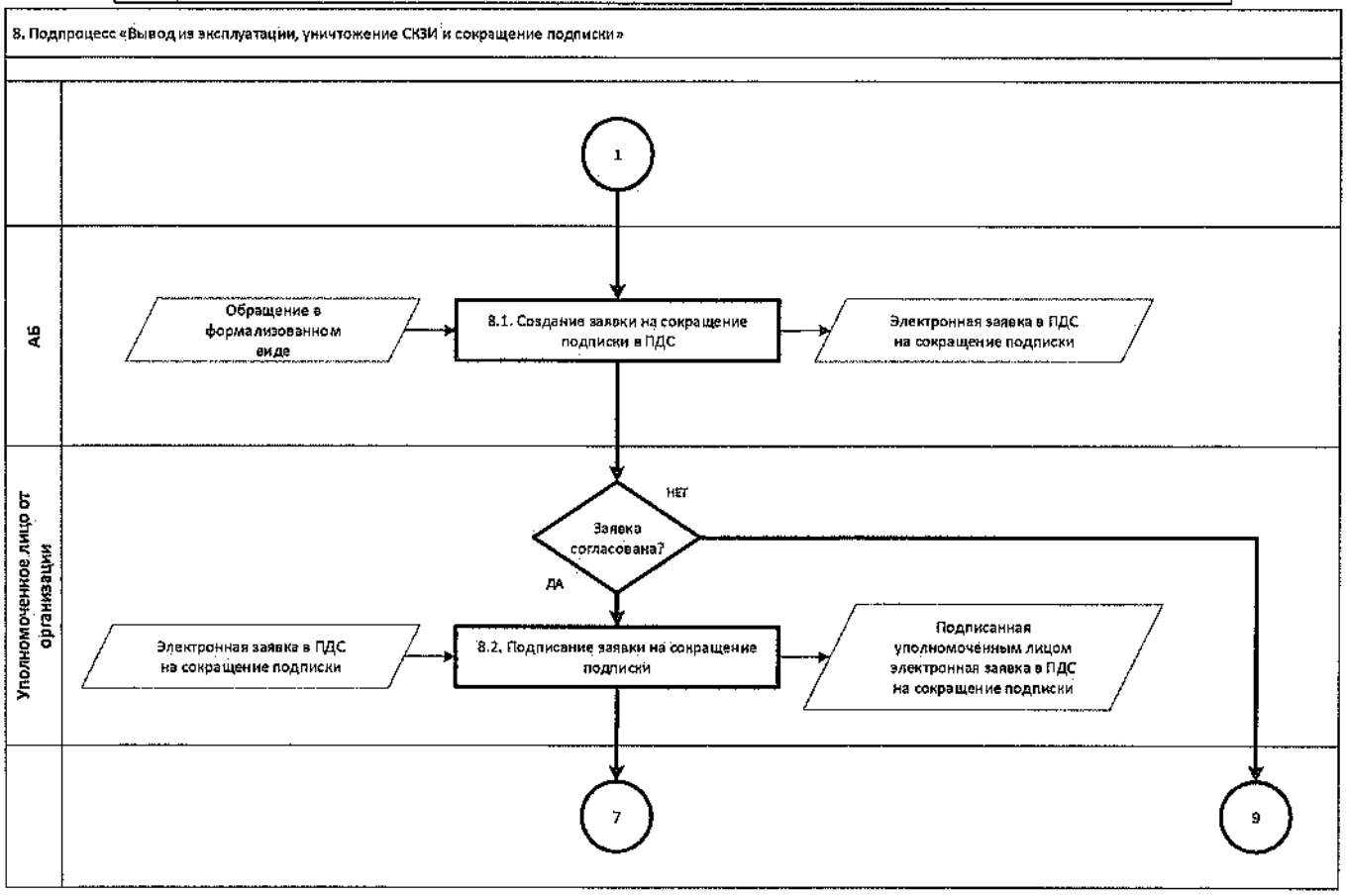

2. Подпроцесс «Создание подписки»
АБ
Уполномоченное лицо от организации
Аналитик ОКЗ
1
Обращение в формализованном виде
2.1. Создание заявки на подписку в ПДС
Электронная заявка в ПДС на создание подписки
Заявка согласована?
НЕТ
ДА
Электронная заявка в ПДС на создании подписки
2.2. Подписание заявки на создание подписки
Подписанная уполномоченным лицом электронная заявка в ПДС на создание подписки
Заявка согласована?
НЕТ
ДА
Подписанная уполномоченным лицом электронная заявка в ПДС на создание подписки
2.3. Подписание заявки на создание подписки
Подписка
3
Конец

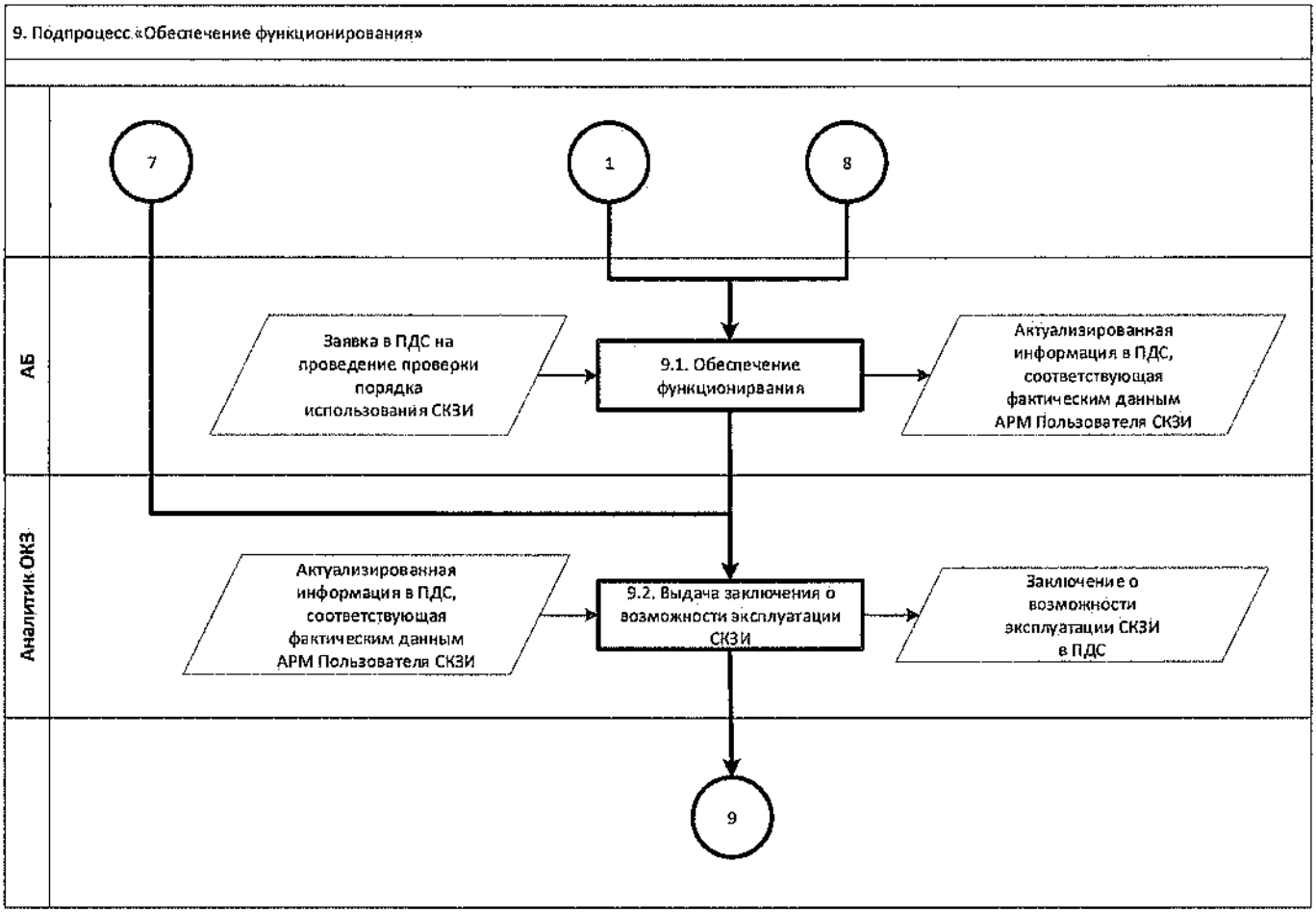

3. Подпроцесс «Передача СКЗИ»
Аналитик ОКЗ
2
Подписка
3.1. Выделение лицензий на СКЗИ
Выделенные лицензии на СКЗИ
4


4. Подпроцесс «Проверка готовности»
АБ
1
3
Подписка
4.1. Проверка готовности СКЗИ к эксплуатации
Приказ о лицах, допускаемых к самостоятельной работе с СКЗИ
Информация в ПДС из Акта готовности СКЗИ к эксплуатации и из приказа о лицах, допускаемых к самостоятельной работе с СКЗИ
5


5. Подпроцесс «Монтаж, установка (инсталляция) СКЗИ»
АБ
4
Информация в ПДС из Акта готовности СКЗИ к эксплуатации
5.1. Монтаж, установка (инсталляция) СКЗИ
Установленное СКЗИ
6
6. Подпроцесс «Обучение и допуск Пользователя СКЗИ»
Пользователь СКЗИ
5
Уведомление о назначении обучения в ПДС
6.1. Обучение Пользователя СКЗИ и сдача зачетов
НЕТ
Тестирование пройдено успешно?
ДА
Информация в ПДС об успешном прохождении обучения
6.2. Активация СКЗИ
Активированное СКЗИ
7


7. Подпроцесс «Учет СКЗИ»
АБ
6
8
ПДС
7.1. Учет СКЗИ
Актуальная схема криптографической защиты в ПДС
Подписка сокращена?
ДА
НЕТ
9
КОНЕЦ


8. Подпроцесс «Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки»
АБ
Уполномоченное лицо от организации
1
Обращение в формализованном виде
8.1. Создание заявки на сокращение подписки в ПДС
Электронная заявка в ПДС на сокращение подписки
Заявка согласована?
НЕТ
ДА
Электронная заявка в ПДС на сокращение подписки
8.2. Подписание заявки на сокращение подписки
Подписанная уполномоченным лицом электронная заявка в ПДС на сокращение подписки
7
9


9. Подпроцесс «Обеспечение функционирования»
АБ
Аналитик СКЗ
7
1
8
Заявка в ПДС на проведение проверки порядка использования СКЗИ
9.1. Обеспечение функционирования
Актуализированная информация в ПДС, соответствующая фактическим данным АРМ Пользователя СКЗИ
Актуализированная информация в ПДС, соответствующая фактическим данным АРМ Пользователя СКЗИ
9.2. Выдача заключения о возможности эксплуатации СКЗИ
Заключение о возможности эксплуатации СКЗИ в ПДС
9

Приложение №15
к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю
Директор по информационным технологиям

/ А.Н. Киселёв /

М.П.

Соглашение
об использовании усиленной неквалифицированной электронной подписи

Москва 2020

Соглашение
об использовании усиленной неквалифицированной электронной подписи

Место подписания «___»_____20__г.

Настоящее соглашение заключено между АО «Гринатом», далее «Оператор ПДС» и _____, далее «Участник», совместно именуемые «Участники электронного взаимодействия», и регулирует применение усиленной неквалифицированной электронной подписи с использованием сервисов Платформы доверенных сервисов Госкорпорации «Росатом» в системах электронного взаимодействия, интегрированных с Платформой доверенных сервисов Госкорпорации «Росатом».

1. Термины и определения

1.1. Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.
1.2. Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (электронному документу) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
1.3. ПДС – Платформа доверенных сервисов Госкорпорации «Росатом», применяемая для управления ключами электронной подписи и сертификатами ключей проверки электронной подписи, удаленного подписания электронных документов и проверки электронной подписи, построенная с использованием компонентов, сертифицированных ФСБ России и аттестованных по требованиям безопасности информации ФСТЭК России.
1.4. Документные системы – корпоративные информационные системы Госкорпорации «Росатом», интегрированные с ПДС, предоставляющие сервисы обмена электронными документами с возможностью подписания усиленной неквалифицированной электронной подписью посредством сервисов ПДС.
1.5. Неквалифицированная электронная подпись - электронная подпись, созданная с использованием средств электронной подписи и полученная в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяющая определить лицо, подписавшее электронный документ и обнаружить факт внесения изменений в электронный документ после момента его подписания.
1.6. Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.
1.7 Сертификат ключа проверки электронной подписи - электронный документ, выданный удостоверяющим центром Госкорпорации «Росатом» через сервисы ПДС и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.
1.8. Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.
1.9. Проверка электронной подписи – процесс подтверждения, что электронная подпись была создана для конкретного документа и документ после этого не был изменен. Проверка неквалифицированной электронной подписи осуществляется доверенными сервисами ПДС.
1.10 Работник – сотрудник Участника, на чье имя выпущен сертификат ключа проверки неквалифицированной электронной подписи, использующий неквалифицированную электронную

подпись в документных системах в рамках своих должностных обязанностей или уполномоченный иным образом для подписания электронных документов в документных системах.

2. Предмет соглашения

2.1. Настоящее соглашение регулирует отношения между участниками электронного взаимодействия в области использования неквалифицированной электронной подписи в документных системах, интегрируемых с ПДС.
2.2. Участники электронного взаимодействия признают, что настоящее соглашение создает условия для признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью.

3. Условия для признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью

- Неквалифицированная электронная подпись используется в соответствии с п.3.1 настоящего соглашения;
- Проверка неквалифицированной электронной подписи осуществляется в соответствии с п.3.2 настоящего соглашения;
- Участники электронного взаимодействия ознакомлены и выполняют обязанности в соответствии с п.3.3 настоящего соглашения;
- Работники Участника, использующие неквалифицированную электронную подпись, подписали соглашение о применении неквалифицированной электронной подписи со своим работодателем по форме Приложения №1 к настоящему соглашению;
- Участник согласился с использованием неквалифицированной электронной подписи в документной системе в рамках отдельных соглашений с операторами документных систем или правил работы в документарной системе.

3.1 Порядок использования неквалифицированной электронной подписи.
3.1.1 Возможность использования неквалифицированной электронной подписи участникам электронного взаимодействия предоставляется АО «Гринатом» в рамках стандартной услуги на основании договора присоединения от «06» июля 2012г. №22/2143-Д.
3.1.2 Неквалифицированная электронная подпись может использоваться только авторизованными пользователями через интерфейс документной системы, интегрированной с ПДС.
3.1.3 Авторизация пользователя осуществляется после прохождения им процедур идентификации и аутентификации. Для достижения среднего и высокого уровня доверия в соответствии с ГОСТ Р 58833-2020 должна использоваться двухфакторная аутентификация.
3.1.4 Неквалифицированная электронная подпись формируется ПДС в электронном документе в соответствии с порядком по инициативе авторизованного участника информационного взаимодействия через интерфейс документной системы, интегрированной с ПДС.
3.1.5 Проверка неквалифицированной электронной подписи осуществляется сервисом проверки подписи ПДС через интерфейс документной системы.
3.1.6 Управление ключами и сертификатами ключей проверки электронной подписи (выпуск, аннулирование) осуществляется через интерфейс документной системы или через пользовательский интерфейс ПДС.
3.1.7 Использование сторонних неквалифицированных электронных подписей не предусматривается.

3.2 Порядок проверки неквалифицированной электронной подписи.

3.2.1 Проверка неквалифицированных электронных подписей предусмотрена только для неквалифицированных электронных подписей, выданных ПДС.
3.2.2 Для проверки электронной подписи участник электронного взаимодействия через интерфейс документной системы отправляет запрос в ПДС на проверку электронной подписи в электронном документе.
3.2.3 Сервис проверки электронной подписи ПДС осуществляет проверку действительности подписи на момент ее формирования, основываясь на достоверной информации по метке времени и статусу сертификата ключа проверки электронной подписи в момент подписания.
3.2.4 Сервис проверки электронной подписи ПДС направляет ответ, содержащий информацию о результатах проверки в документную систему для предъявления участнику информационного взаимодействия.

3.3 Обязанности участников электронного взаимодействия при использовании неквалифицированной электронной подписи.
3.3.1 Обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия.
3.3.2 Уведомлять ПДС, выдавшую 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.
3.3.3 Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

4. Ответственность сторон

4.1. За неисполнение и ненадлежащее исполнение обязательств по настоящему соглашению Участники несут ответственность в соответствии с действующим законодательством Российской Федерации.

5. Заключительные положения

5.1. Во всем остальном, что не установлено настоящим соглашением, Участники руководствуются положениями действующего законодательства Российской Федерации.

6. Реквизиты и подписи сторон

Оператор ПДС	Участник

Приложение №1
к Соглашению об использовании
усиленной неквалифицированной электронной подписи
Форма «Соглашение о применении усиленной неквалифицированной электронной подписи»

Соглашение
о применение усиленной неквалифицированной электронной подписи

_____
(наименование организации)

Место подписания «___»_____20__г.

_____, именуемое в дальнейшем "Работодатель", в лице _____ *(должность)* _____ *(Ф.И.О)*, действующего на основании _____, с одной стороны, и _____ *(Ф.И.О.)* именуемый в дальнейшем "Работник", с другой стороны, совместно именуемые «Стороны» заключили настоящее соглашение об использовании усиленной неквалифицированной электронной подписи, именуемое в дальнейшем "Соглашение", о нижеследующем:

1. Термины и определения

1.1. Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.
1.2. Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (электронному документу) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
1.3. Платформа доверенных сервисов Госкорпорации «Росатом», ПДС – платформа, создающая условия для использования усиленной неквалифицированной электронной подписи, оказывающая услуги по выпуску сертификатов ключей проверки электронной подписи, подписанию, подтверждению подлинности такой подписи и предоставляющая другие сопутствующие сервисы.
1.4. Документные системы – корпоративные информационные системы Госкорпорации «Росатом», интегрированные с ПДС, предоставляющие сервисы обмена электронными документами с возможностью подписания усиленной неквалифицированной электронной подписью посредством сервисов ПДС.
1.5. Неквалифицированная электронная подпись - электронная подпись, созданная с использованием средств электронной подписи и полученная в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяющая определить лицо, подписавшее электронный документ и обнаружить факт внесения изменений в электронный документ после момента его подписания.
1.6. Проверка неквалифицированной электронной подписи – процесс подтверждения, что электронная подпись была создана для конкретного документа и документ после этого не был изменен. Проверка неквалифицированной электронной подписи осуществляется с использованием сервиса ПДС.
1.7. Порядок - порядок применения неквалифицированной электронной подписи в ПДС, опубликованный по адресу https://crypto.rosatom.ru/.

2. Предмет соглашения

2.1. Настоящее Соглашение регулирует отношения между Работником и Работодателем в части использования усиленной неквалифицированной электронной подписи для придания электронным документам юридической значимости, эквивалентной документам на бумажных носителях, подписанным собственноручной подписью участника документной системы.
2.2. Руководствуясь положениями части 2 статьи 6 Федерального закона "Об электронной подписи" №63-ФЗ от 06.04.2011, Работник признает электронные документы, подписанные им в документной системе усиленной неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью.
2.3. Настоящим Работник подтверждает, что ознакомлен с Порядком и обязуется не нарушать его положения, положения настоящего Соглашения и условия Федерального закона "Об электронной подписи" №63-ФЗ от 06.04.2011.
2.4. Настоящим работник выражает согласие на выпуск на его имя сертификата усиленной неквалифицированной электронной подписи удостоверяющим центром Госкорпорации «Росатом» посредством ПДС и дальнейшее его использование для подписания электронных документов в документной системе.

3. Обязанности Работника

3.1. Принимать все меры для обеспечения сохранности ключей электронной подписи в случае хранения их на электронном носителе, переданном Работнику. В случае хранения электронных ключей в ПДС ответственность за сохранность ключей электронной подписи лежит на Операторе ПДС.
3.2. Незамедлительно уведомлять Оператора ПДС об утрате и/или компрометации ключей электронной подписи, а также об относящимся к данной электронной подписи документам, находящемся в обороте.
3.3. Незамедлительно осуществить перевыпуск ключа электронной подписи посредством ПДС в случае утраты и/или компрометации ключа электронной подписи;
3.4. Незамедлительно уведомлять Работодателя об изменении своих данных, содержащихся в сертификате ключа проверки электронной подписи и не использовать ключ электронной подписи с устаревшими данными до перевыпуска неквалифицированного сертификата.
3.5. Соблюдать иные условия использования электронной подписи, установленные Федеральным законом "Об электронной подписи" №63-ФЗ от 06.04.2011, настоящим Соглашением и Порядком.

4. Ответственность сторон

4.1. За неисполнение и ненадлежащее исполнение обязательств по настоящему Соглашению Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

5. Заключительные положения

5.1. Настоящее Соглашение действует с момента его подписания и в течение всего срока действия трудового договора, заключенного между Работником и Работодателем.
5.2. В случае прекращения трудового договора между Работником и Работодателем настоящее Соглашение прекращает свое действие, а Работодатель отзывает сертификат ключа проверки электронной подписи, выданный во исполнение настоящего Соглашения.

5.3. Все дополнения и изменения к настоящему Соглашению оформляются путем подписания сторонами соответствующих дополнительных соглашений.
5.4. Во всем остальном, что не установлено настоящим Соглашением, Стороны руководствуются положениями действующего законодательства Российской Федерации.
5.5. Настоящее Соглашение составлено в двух экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

6. Реквизиты и подписи сторон

Работодатель	Работник

Приложение № 16 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю

Директор по информационным технологиям

АО «Гринатом»

_____ / А.Н. Киселёв /

М.П.

Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом»
(Удостоверяющего центра АО «Гринатом»)

Москва 2020 г.

Оглавление

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Используемые в настоящем документе термины описаны в таблице ниже.

Таблица 1. Список терминов

Термин	Определение
Владелец сертификата ключа проверки электронной подписи	Лицо, которому в установленном Федеральным законом (N 63-ФЗ) порядке выдан сертификат ключа проверки электронной подписи.
Межсетевой экран	Комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.
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.
Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат)	Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.
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.
Список отозванных сертификатов	Электронный документ с электронной подписью удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые были аннулированы до окончания срока их действия.
Удостоверяющий центр	Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом (N 63-ФЗ).
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.
Электронный документ	Документ, информация в котором представлена в электронной форме, способной быть обработанной средствами вычислительной техники

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Устойчивые русскоязычные сокращения, используемые в этом документе, описаны в таблице ниже.

Таблица 2. Список сокращений

Сокращен	Значение
АРМ	Автоматизированное рабочее место
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СКПЭП	Сертификат ключа проверки электронной подписи
СУБД	Системы управления базами данных
КУЦ	Корпоративный удостоверяющий центр Госкорпорации «Росатом»
ЭП	Электронная подпись

Используемые иностранные сокращения, как правило, англоязычные, приведены в таблице ниже.

Таблица 3. Список иностранных сокращений

Сокращение	Значение	Перевод
AIA	Authority Info Access	Доступ к информации о Центре сертификации
CRL	Certificate Revocation List	Список отозванных сертификатов, СОС
CDP	CRL Distribution Point	Пункт распространения CRL
DN	Distinguished Name	Отличительное имя
IETF	Internet Engineering Task Force	Специальная комиссия интернет разработок
ITU	International Telecommunication Union	Международный союз электросвязи, МСЭ
ITU-T	Telecommunication Standardization Sector (ITU's)	Сектор стандартизации электросвязи (в МСЭ), МСЭ-Т
LDAP	Lightweight Directory Access Protocol	Облегчённый протокол доступа к Справочнику
PKI	Public Key Infrastructure	Инфраструктура ключей проверки ЭП
RDN	Relative Distinguished Name	Относительное отличительное имя

1. Общие положения

1.1. Предмет регулирования Порядка

Настоящий Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом») (Далее – Регламент) определяет механизмы и условия предоставления и использования услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом») (Далее – КУЦ), включая обязанности КУЦ и сотрудников КУЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, необходимые для безопасной работы КУЦ.

1.2. Сведения о КУЦ

Акционерное общество «Гринатом»

(полное наименование юридического лица)

115230, Москва, 1-й Нагатинский проезд., д. 10, стр. 1

(почтовый адрес)

ca@rosatom.ru

(адрес электронной почты)

Контактный телефон +7 (499) 949-49-19 доб. 54-54

Деятельность КУЦ в том числе его обособленных подразделений (филиалов) по работе с пользователями КУЦ и созданию сертификатов ключей проверки ЭП организована в одну рабочую смену с 9.00 до 18.00 в будние дни.

Выходными днями являются: суббота, воскресение, а также дни общенациональных праздников.

1.3. Справочные телефоны КУЦ, его обособленных подразделений (филиалов)

адрес: 665816, Россия, Иркутская обл., г. Ангарск, ул.14 декабря, д.22

Телефон: 8(3955)54-32-47

адрес: 600007, Владимирская область, г.Владимир ул.Северная, д. 1а

Телефон: +7 (4922) 47-38-26

адрес: 427620, Удмуртская респ., г.Глазов ул.Белова д.7

Телефон: 8 (34141) 96346 ; 8 (34141) 96349

адрес: 663690 Красноярский край г.Зеленогорск ул.Первая Промышленная, д.1

Телефон: 8(39169) 9-39-36; 8(39169) 9-43-23

адрес: 601909, Владимирская область, г.Ковров, ул.Социалистическая д.26

Телефон: 8(49232) 9-40-04 (доб. 11-67); 8(49232) 9-40-04 (доб. 11-66)

адрес: 603064, Нижегородская область, г. Нижний Новгород, пр. Ленина, д.93 каб. 634

Телефон: +7 (499) 949-49-19 доб. 7887; +7 (831) 268-15-68 доб. 7887

адрес: 630110, Новосибирская область, г. Новосибирск, ул.Б.Хмельницкого, д.94

Телефон: +7 (038)274-89-33

адрес: 624130, Свердловская обл., г. Новоуральск, ул. Мичурина, д.29, ОПС а/я 10 Филиал АО «Гринатом» в г. Новоуральске.

Телефон: +7 (34370) 5-69-51; +7 (34370) 5-31-33

адрес: 191036, г. Санкт-Петербург, ул. 2-ая Советская, д. 7

Телефон для связи с оператором КУЦ: 8(499)949-49-19 доб.(030) 5-42-29

адрес: 607328, Нижегородская обл., Дивеевский р-н, п. Сатис, ул. Парковая д.3. стр.5-1

Телефон:7 (83130) 70-9-70 доб. 603

адрес: 636039, г. Северск Томской обл., ул. Ленина 90

Телефон:8(3823) 52-46-41; 8(3823) 52-71-63

адрес: 144001, Россия, Московская обл., г.Электросталь, ул.Карла Маркса, д.12

Телефон: 8 496 577 31 74, вн. 31 74; 8 496 577 31 74, вн. 43 93

1.4. Порядок информирования о предоставлении услуг КУЦ

Настоящий Регламент распространяется:

- В электронной форме на официальном сайте: http://crypto.rosatom.ru

Порядок получения информации заявителями по вопросам предоставления услуг КУЦ доступен по телефонному обращению на справочный телефон +7 (499) 949-49-19 доб. 54-54

Телефон для справок: +7 (499) 949-29-99 доб.: 0; с КТС: внутренний 1111

Телефон для связи с оператором КУЦ: +7 (499) 949-49-19 доб: 5454

1.5. Стоимость услуг

Услуга КУЦ по предоставлению копий сертификатов ключей проверки ЭП в электронной форме, находящихся в Реестре сертификатов, предоставляется на безвозмездной основе.

Состав и стоимость предоставляемых иных услуг определяется КУЦ

Порядок информирования заинтересованных лиц о стоимости услуг КУЦ определён Договором присоединения и опубликован на сайте КУЦ https://crypto.rosatom.ru/dokumentatsiya/dogovor/.

Срок и порядок расчетов за оказание услуг КУЦ определён Договором присоединения и опубликован на сайте КУЦ https://crypto.rosatom.ru/dokumentatsiya/dogovor/

1.6. Область применения Регламента

Настоящий Регламент является средством официального уведомления и

информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг КУЦ.

1.7. Срок действия Регламента

Настоящий Регламент вступает в силу со дня его публикации. Срок действия Регламента — 10 лет.

Если КУЦ официально не уведомит своих пользователей о прекращении действия Регламента, то Регламент автоматически пролонгируется на следующий срок.

Официальное уведомление о прекращении действия Регламента осуществляется путём публикации об этом сведений на официальном сайте КУЦ.

1.8. Структура КУЦ

Структура КУЦ включает в себя Отдел криптографической защиты АО «Гринатом». Отдел криптографической защиты обеспечивает решение следующих задач:

Администратор КУЦ:

- управление деятельностью КУЦ;
- координация деятельности КУЦ;
- взаимодействие с Пользователями КУЦ в части разрешения вопросов, связанных с применением средств ЭП, ключей и сертификатов ключей проверки ЭП, создаваемых КУЦ;
- взаимодействие с Пользователями КУЦ в части разрешения вопросов, связанных с подтверждением электронной подписи КУЦ в сертификатах ключей проверки ЭП, созданных КУЦ;
- организация и выполнение мероприятий по защите ресурсов КУЦ;

создание и предоставление копий сертификатов ключей проверки ЭП на бумажном носителе по обращению их владельцев;

- аннулирование (отзыв) сертификатов ключей проверки ЭП по обращениям владельцев сертификатов ключей проверки ЭП;
- предоставление Пользователям КУЦ сведений об аннулированных сертификатах ключей проверки ЭП;
- техническое обеспечение процедуры подтверждения электронной подписи в документах, по обращениям Пользователей КУЦ;
- техническое обеспечение процедуры подтверждения подлинности электронных подписей КУЦ в созданных сертификатах ключей проверки ЭП по обращениям Пользователей КУЦ.
- организация и выполнение мероприятий по эксплуатации программных и технических средств обеспечения деятельности КУЦ;

Оператор КУЦ:

- регистрация Пользователей КУЦ;
- ведение Реестра зарегистрированных Пользователей КУЦ;
- предоставление служебных ключей ЭП и сертификатов служебных ключей проверки ЭП по обращению Пользователей КУЦ;
- распространение средств электронной подписи и шифрования.
- создание и вручение ключей Пользователей КУЦ;
- предоставление сертификатов ключей проверки ЭП в электронной форме Пользователей КУЦ;

1.9. Пользователи КУЦ

Пользователями КУЦ называются лица, зарегистрированные в КУЦ — лица, прошедшие полную процедуру идентификации и аутентификации в КУЦ;

Стать зарегистрированным Пользователем КУЦ может только физическое лицо, являющееся представителем юридического лица, при наличии доверенности, которая даёт данному физическому лицу право пользоваться услугами КУЦ от имени юридического лица.

Владельцем сертификата и ключа ЭП может быть только зарегистрированный Пользователь КУЦ, физическое лицо.

В тех случаях, когда сертификаты ключей проверки ЭП требуются для работы каких-либо устройств или программ, назначается ответственное лицо, на имя которого КУЦ изготавливает сертификаты.

1.10. Разрешение споров

Сторонами в споре, в случае его возникновения, считаются КУЦ и Пользователь КУЦ.

Стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путём переговоров.

Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе переговоров, должны рассматриваться в Арбитражном суде в соответствии с действующим законодательством Российской Федерации.

1.11. Ответственность

КУЦ не несёт никакой ответственности в случае нарушения Пользователями КУЦ положений настоящего Регламента.

Претензии к КУЦ ограничиваются указанием на несоответствие его действий настоящему Регламенту.

1.12. Прекращение деятельности

Деятельность КУЦ может быть прекращена в порядке, установленном законодательством Российской Федерации.

В случае принятия решения о прекращении своей деятельности КУЦ:

1) сообщает об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

2) передаёт в уполномоченный федеральный орган в установленном порядке реестр квалифицированных сертификатов установленным порядком;

3) передает на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

1.13. Порядок утверждения и внесения изменений в Регламент

Настоящий Регламент составляется в письменной форме и заверяется собственноручной подписью Руководителя КУЦ и печатью КУЦ.

КУЦ в одностороннем порядке вносит изменения в Регламент.

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.

2. Перечень реализуемых КУЦ функций (Оказываемых услуг)

В процессе своей деятельности КУЦ предоставляет потребителям или Пользователям КУЦ следующие виды услуг:

1) создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с пунктом 4 части 4 статьи 8 Федерального закона № 63-ФЗ;

1.1) осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;

2) устанавливает сроки действия сертификатов ключей проверки электронных подписей;

3) аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;

4) выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

5) ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

6) устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";

7) создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

8) проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

9) осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

10) осуществляет иную связанную с использованием электронной подписи деятельность.

3. Права и обязанности

3.1. Права КУЦ

КУЦ имеет право:

– Предоставлять сертификаты ключей проверки ЭП в электронной форме, находящихся в Реестре КУЦ, всем лицам, обратившимся в КУЦ;

– Не проводить регистрацию лиц, обратившихся по вопросу представления сертификатов ключей проверки ЭП в электронной форме, находящихся в Реестре КУЦ;

– Отказать в создании сертификата ключа проверки ЭП зарегистрированным пользователям КУЦ, без указания причин отказа;

– Отказать в аннулировании (отзыве) сертификата ключа проверки ЭП владельцу сертификата, в случае если истёк установленный срок действия ключа ЭП, соответствующего ключу проверки ЭП в сертификате;

3.2. Права Пользователей КУЦ

Пользователи КУЦ, имеют следующие права:

– Получать в электронной форме списки отозванных сертификатов ключей проверки ЭП, созданные КУЦ;

– Получать в электронной форме сертификаты ключа проверки ЭП КУЦ;

– Получать в электронной форме сертификаты ключа проверки ЭП Пользователей КУЦ, находящиеся в Реестре сертификатов ключей проверки ЭП КУЦ;

– Применять сертификаты ключа проверки ЭП КУЦ для проверки электронных подписей КУЦ в сертификатах ключа проверки ЭП пользователей, созданных КУЦ.

– Применять сертификаты ключа проверки ЭП Пользователей КУЦ для проверки электронных подписей в электронных документах в соответствии со сведениями, указанными в сертификатах ключа проверки ЭП.

– Применять список отозванных сертификатов ключей проверки ЭП для проверки статуса сертификатов ключей проверки ЭП.

– Обращаться в КУЦ за подтверждением подлинности электронных подписей в электронных документах;

– Обращаться в КУЦ за подтверждением подлинности электронных подписей КУЦ в созданных КУЦ сертификатах ключей проверки ЭП пользователей;

– Обращаться в КУЦ для аннулирования (отзыва) своих сертификатов ключей проверки ЭП в течение срока действия соответствующих ключей ЭП.

3.3. Обязанности КУЦ

3.3.1. Ключи электронной подписи КУЦ

КУЦ обязан выполнять порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, установленных КУЦ в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения обязанностей.

КУЦ обязан использовать для создания ключей ЭП КУЦ и формирования электронных подписей только средства криптографической защиты информации (средства электронной подписи), входящие в состав выбранной комплектации «КриптоПро УЦ» согласно (ЖТЯИ.00078-01 30 01).

При использовании в соответствии с положениями формуляра (ЖТЯИ.00078-01 30 01), ПАК «КриптоПро УЦ 2.0» удовлетворяет «Требованиям к средствам удостоверяющего центра» ФСБ России вариант исполнения 5 – классу КС2 (используются СКЗИ/средства ЭП класса КС2).

КУЦ обязан использовать ключи ЭП КУЦ только для подписи издаваемых им сертификатов ключей проверки ЭП и списков отозванных сертификатов.

КУЦ обязан принять меры по защите ключей ЭП КУЦ в соответствии с положениями настоящего Регламента.

КУЦ обязан обеспечивать конфиденциальность созданных ключей электронных подписей до момента вручения владельцам.

3.3.2. Синхронизация времени

КУЦ организует работу по Всемирному координированному времени (UTC) с учётом часового пояса места расположения КУЦ.

КУЦ обязан синхронизировать по времени все программные и технические средства обеспечения деятельности по предназначению.

3.3.3. Создание ключей ЭП и ключей проверки ЭП

КУЦ обязан отказать Пользователю КУЦ в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что Пользователь КУЦ владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи.

КУЦ для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган.

КУЦ запрещается использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.

КУЦ обязан отказать заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи

КУЦ обязан создать ключ ЭП и ключ проверки ЭП зарегистрированному Пользователю КУЦ с использованием средств электронной подписи, сертифицированных в соответствии с действующим законодательством Российской Федерации.

КУЦ обязан обеспечить сохранение в тайне созданного ключа ЭП.

КУЦ обязан записать ключ на носитель, в соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей.

КУЦ обязан выполнять процедуру генерации ключей и запись ключей на отчуждаемый носитель только с использованием программного и/или аппаратного средства, сертифицированного в соответствии с законодательством Российской Федерации.

КУЦ обязан обеспечить защиту ключевого носителя от копирования.

КУЦ обязан обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей проверки ЭП Пользователей КУЦ.

КУЦ обязан обеспечить уникальность значений ключей проверки ЭП в созданных сертификатах ключей проверки ЭП пользователей КУЦ.

КУЦ запрещается указывать в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном этому удостоверяющему центру любым другим удостоверяющим центром.

КУЦ обязан хранить следующую информацию:

1) реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;

2) сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;

3) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

КУЦ должен хранить указанную информацию в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации. Хранение информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

3.3.4. Выдача сертификатов

При выдаче квалифицированного сертификата КУЦ обязан в порядке, установленном законодательством, идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата.

Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", КУЦ обязан отказать такому лицу в проведении указанной идентификации.

Устанавливаются - наименование, организационно-правовая форма, идентификационный номер налогоплательщика, а также основной государственный регистрационный номер и адрес юридического лица

При выдаче квалифицированного сертификата КУЦ обязан получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата

При выдаче квалифицированного сертификата аккредитованный КУЦ обязан в установленном порядке идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата (в целях получения от заявителя, выступающего от имени юридического лица, подтверждения правомочия обращаться за получением квалифицированного сертификата).

При получении квалифицированного сертификата Пользователем УЦ ознакомить с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной

электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. КУЦ обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

КУЦ одновременно с выдачей квалифицированного сертификата должен предоставить владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

При выдаче квалифицированного сертификата КУЦ направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате. Требования к порядку предоставления владельцам квалифицированных сертификатов сведений о выданных им квалифицированных сертификатах с использованием единого портала государственных и муниципальных услуг устанавливаются Правительством Российской Федерации. При выдаче квалифицированного сертификата КУЦ по желанию владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.

3.3.5. Уведомления

КУЦ обязан предложить использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", физическим лицам, обратившимся к нему в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством сети "Интернет"), и указать страницу сайта в информационно-телекоммуникационной сети "Интернет", с которой безвозмездно предоставляются эти средства.

При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети "Интернет" при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств, аккредитованный удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

Страница для скачивания шифровальных (криптографических) средств –

https://www.cryptopro.ru/downloads

Уведомление о факте создания сертификата ключа проверки ЭП

КУЦ обязан информировать пользователей КУЦ об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных

с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки

КУЦ обязан официально уведомить о факте создания сертификата ключа проверки ЭП его владельца.

Срок уведомления — не позднее 24 часов с момента создания сертификата ключа проверки ЭП.

Официальным уведомлением о факте создании сертификата является отправка почтового сообщения по электронной почте с прикреплённым сертификатом ключа проверки ЭП с адреса отправителя ca@rosatom.ru.

Временем отправки почтового сообщения признается время отправки почтового

сообщения с почтового сервера ca@rosatom.ru, осуществляющего отправку почтовых сообщений КУЦ, и включённое в заголовок почтового сообщения.

Уведомление о факте аннулирования сертификата ключа проверки ЭП

КУЦ обязан официально уведомить о факте аннулирования сертификата ключа проверки ЭП его владельца.

Срок уведомления — не позднее 12 часов с момента занесения сведений о факте аннулирования сертификата в список отозванных сертификатов.

Официальным уведомлением о факте аннулирования сертификата является опубликование списка отозванных сертификатов, который содержит сведения об сертификате, в репозитории КУЦ по адресам:

http://crl1.rosatom.ru
http://crl1.rosatom.local
http://crl2.rosatom.ru
http://crl2.rosatom.local

Временем аннулирования сертификата ключа проверки ЭП признается время занесения сведений об сертификате в список отозванных сертификатов, указанное в списке отозванных сертификатов.

Временем опубликования списка отозванных сертификатов признается время создания списка отозванных сертификатов, указанное в списке отозванных сертификатов.

КУЦ обязан включать полный адрес (URL) списка отозванных сертификатов в издаваемые сертификаты.

3.3.6. Реестр сертификатов ключей проверки ЭП

КУЦ обязан вести Реестр всех созданных сертификатов ключей проверки ЭП пользователей КУЦ в течение установленного срока хранения.

КУЦ обязан обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий

КУЦ обязан обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к реестру квалифицированных сертификатов КУЦ в любое время в течение срока деятельности этого удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

КУЦ обязан предоставлять безвозмездно любому лицу по его обращению в соответствии с порядком доступа к реестру сертификатов, определённом в п.4.13. информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи.

КУЦ обязан публиковать выписки из Реестра, позволяющие определить

действительность сертификатов ключей проверки ЭП пользователей КУЦ.

Выписка из Реестра КУЦ предоставляется в виде списка отозванных сертификатов в электронной форме и формате, определённом настоящим Регламентом.

3.3.7. Восстановление работоспособности КУЦ после сбоев

В целях недопущения технических сбоев КУЦ обязан обеспечить выполнение мероприятий, направленных на их предотвращение и оперативное восстановление работоспособности средств КУЦ, руководствуясь «Порядком технического обслуживания средств обеспечения деятельности КУЦ», изложенным в настоящем Регламенте. В случае возникновения технического сбоя КУЦ должен обеспечить информирование участников информационных систем о статусе сертификатов не позднее восьми часов с момента наступления сбоя (обеспечить публикацию списков отозванных сертификатов), а полное восстановление работоспособности КУЦ – не позднее суток с момента наступления сбоя.

3.3.8. Прекращение деятельности

В случае принятия решения о прекращении своей деятельности:

КУЦ обязан сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

КУЦ обязан передать в уполномоченный федеральный орган в установленном порядке реестр выданных квалифицированных сертификатов;

КУЦ обязан передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

3.4. Обязанности Пользователей КУЦ

Пользователи КУЦ, обязаны:

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

- перед использованием сертификата ключа проверки ЭП, созданного этим КУЦ, удостовериться, что назначения ключа и назначения сертификата, указанные в сертификате, соответствуют предполагаемому использованию сертификата, согласно настоящему Регламенту.

- хранить в тайне свой ключ ЭП, принимать всевозможные меры для предотвращения его потери, раскрытия, изменения или несанкционированного использования;

- не использовать для электронной подписи ключи электронной подписи, если ему известно, что эти ключи используются или использовались ранее другими лицами;

- использовать ключи ЭП только для целей, разрешённых назначениями ключа и назначениями сертификата, согласно настоящему Регламенту.

- использовать сертификаты своих ключей проверки ЭП только для целей, разрешённых назначениями ключа и назначениями сертификата, которые указаны в сертификате, согласно настоящему Регламенту;

- предоставлять идентифицирующую информацию в объёме, определённом положениями настоящего Регламента.

4. Процедуры и механизмы

4.1. Процедура Идентификации и аутентификации пользователей КУЦ

Первичная идентификация и аутентификация зарегистрированного Пользователя КУЦ выполняется по документу, удостоверяющему личность, предъявляемому лично.

Идентификация Пользователя проводится при его личном присутствии или посредством идентификации Пользователя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации Пользователя с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации". При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации. Создание сертификатов ключей проверки электронных подписей и выдача таких сертификатов Пользователем в отношении усиленных неквалифицированных электронных подписей также могут осуществляться при определении лица, подающего заявление в электронной форме без личного присутствия с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации, и при условии организации взаимодействия удостоверяющего центра с единой системой идентификации и аутентификации, гражданами (физическими лицами) и организациями с применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации

Удалённая аутентификация зарегистрированного Пользователя КУЦ при доступе к Информационной системе органа криптографической защиты и Информационной системе «Платформа доверенных сервисов» выполняется в соответствии с приказом Госкорпорации «Росатом» №1517 «Об утверждении Единых отраслевых методических указании по предоставлению пользователям доступа к централизованным ИТ-ресурсам Госкорпорации «Росатом» и организаций Госкорпорации «Росатом»

4.2. Процедура создания ключей электронных подписей и ключей проверки электронных подписей

Пользователь КУЦ создает ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (зарегистрирован Министерством юстиции Российской Федерации 3 марта 2005 г., регистрационный N 6382), с изменениями, внесенными приказом ФСБ России 12 апреля 2010 г. N 173 "О внесении изменений в некоторые нормативные правовые акты ФСБ России" (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный N 17350);

КУЦ создает ключ электронной подписи и ключ проверки электронной подписи для заявителя в соответствии с правилами пользования средствами криптографической защиты

информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09 февраля 2005 г. №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона «Об электронной подписи» создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности

Создание ключа электронной подписи и ключа проверки электронной подписи на автоматизированном рабочем месте КУЦ производится после выполнения требований, установленных постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049),

4.3. Порядок смены ключей КУЦ

Плановая смена ключей КУЦ

Плановая смена ключей (ключа ЭП и соответствующего ему ключа проверки ЭП) КУЦ выполняется в течение срока действия ключа ЭП КУЦ.

При использовании СКЗИ «КриптоПро CSP» плановая смена ключей КУЦ выполняется не ранее, чем через 1 год, и не позднее, чем через 1 год и 3 месяца после начала действия ключа ЭП КУЦ.

Процедура плановой смены ключей КУЦ осуществляется в следующем порядке:

КУЦ формирует новый ключ ЭП и соответствующий ему ключ проверки ЭП;

КУЦ направляет запрос на создание нового сертификата ЭП КУЦ в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации изготавливает сертификат нового ключа проверки ЭП и подписывает его электронной подписью с использованием ключа ЭП Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации направляет в КУЦ новый сертификат КУЦ

Старые ключи ЭП КУЦ используются в течение своего срока действия для формирования списков отозванных сертификатов в электронной форме, изданных КУЦ в период действия старых ключей ЭП КУЦ.

Доверенным способом получения нового квалифицированного сертификата КУЦ Пользователям КУЦ является скачивание нового квалифицированного сертификата КУЦ с официального сайта по защищённому протоколу HTTPS - https://crypto.rosatom.ru/ca/tsepochka-sertifikatov/ исключающее уничтожение, модифицирование, блокирование при передаче.

Внеплановая смена ключей КУЦ

Внеплановая смена ключа электронной подписи КУЦ осуществляется в случае нарушения конфиденциальности ключа электронной подписи или угрозы нарушения конфиденциальности такого ключа электронной подписи

Процедура внеплановой смены ключей КУЦ выполняется в порядке, определённом процедурой плановой смены ключей КУЦ.

Одновременно с внеплановой сменой ключа электронной подписи производится

прекращается действие всех квалифицированных сертификатов, созданных с использованием этого ключа электронной подписи, с занесением сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

Виды угроз нарушения конфиденциальности ключа электронной подписи КУЦ:

- Оставление ключа электронной подписи КУЦ без контроля
- Разглашение ключа электронной подписи КУЦ администратором КУЦ.

4.4. Порядок осуществления смены ключа электронной подписи владельца квалифицированного сертификата

Смена ключа электронной подписи владельца квалифицированного сертификата осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи 14 Федерального закона «Об электронной подписи»;

Требования к заявлению на смену ключа электронной подписи владельца квалифицированного сертификата аналогичны заявлению на создание ключа электронной подписи и содержатся в п.4.5. настоящего регламента

Заявление на смену ключа электронной подписи владельца квалифицированного сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца квалифицированного сертификата, при этом в случае, если смена ключа электронной подписи владельца квалифицированного сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, соответствующее заявление подписывается иной усиленной квалифицированной электронной подписью владельца квалифицированного сертификата.

Процедура выдачи квалифицированного сертификата и ключа электронной подписи владельцу описана в п.4.5.

4.5. Процедура создания и выдачи квалифицированных сертификатов

В зависимости от выбранного Пользователем КУЦ способа, порядок подачи заявления на создание и выдачу квалифицированных сертификатов определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

В зависимости от выбранного Пользователем КУЦ способа, форма заявления на создание и выдачу квалифицированных сертификатов Приведена в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации

«Росатом» (Приложение №12 к договору присоединения)

Заявление на создание и выдачу квалифицированного сертификата может быть оформлено как на бумажном носителе (в соответствии с Порядком Предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»), так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью Пользователя КУЦ (в соответствии с Порядком Предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Платформа доверенных сервисов»)

Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность;

Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства;

Личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц;

Порядок установления личности заявителя определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

Перечень документов, запрашиваемых КУЦ у заявителя для создания и выдачи квалифицированного сертификата, в том числе для удостоверения личности заявителя, в соответствии с частью 2 статьи 17 и частью 2 статьи 18 Федерального закона №63-ФЗ определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

В случае если для подтверждения сведений, вносимых в квалифицированный сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель представляет в КУЦ документ соответствующей формы

Порядок проверки достоверности документов и сведений, представленных заявителем определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 Федерального закона «Об электронной подписи» КУЦ запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона «Об электронной подписи»;

В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и КУЦ установлена личность заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя – юридического лица, на обращение за получением квалифицированного сертификата, КУЦ осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае КУЦ отказывает заявителю в выдаче квалифицированного сертификата;

Порядок создания квалифицированного сертификата определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

После создания квалифицированного сертификата КУЦ осуществляет регистрацию квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи»

По желанию лица, которому выдан квалифицированный сертификат, КУЦ на безвозмездной основе производит регистрацию указанного лица в единой системе идентификации и аутентификации

Порядок выдачи квалифицированного сертификата определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

При выдаче квалифицированного сертификата КУЦ производит информирование заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки путём предоставления руководства по обеспечению безопасности.

Срок создания и выдачи квалифицированного сертификата с момента получения КУЦ соответствующего заявления составляет не более 10 рабочих дней.

4.6. Процедура подтверждения действительности электронной подписи, использованной для подписания электронных документов

Требования к заявлению на подтверждение действительности электронной подписи, в том числе перечень прилагаемых к такому заявлению документов; срок предоставления услуги по подтверждению действительности электронной подписи в электронном документе; а так же порядок оказания услуги определены в документе:

– Порядок подтверждения подлинности электронной подписи в электронном документе (утвержденный приказом АО «Гринатом» от 19.11.2012 №22/284-П)

Порядок оказания услуги содержит процедуру проверки действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата КУЦ, выданного ему головным удостоверяющим центром.

4.7. Процедура прекращении действия и аннулировании квалифицированного сертификата

Квалифицированный сертификат прекращает свое действие в случаях, установленных статьей 14 Федерального закона «Об электронной подписи».

КУЦ признает квалифицированный сертификат аннулированным, если:

не подтверждено, что владелец квалифицированного сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;

установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;

вступило в силу решение суда, которым установлено, что квалифицированный сертификат содержит недостоверную информацию;

Порядок подачи и приема заявления о прекращении действия квалифицированного сертификата, в том числе порядок подтверждения полномочий владельца квалифицированного сертификата, а так же порядок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов и требования к заявлению определены в документах:

– Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)

– Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)

– Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

Заявления о прекращении действия квалифицированного сертификата могут быть направлены в КУЦ как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью.

Срок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов не превышает двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи», или в течение двенадцати часов с момента получения КУЦ соответствующих сведений.

4.8. Порядок ведения реестра квалифицированных сертификатов;

Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов производится путём внесения сведений в реестр Оператором КУЦ

Обеспечение защиты информации, содержащейся в реестре квалифицированных сертификатов от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий производится путём применения сертифицированных средств КУЦ в качестве реестра сертификатов КУЦ.

Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов, производится за счёт применения средств отказоустойчивости и проведения организационно-технических мероприятий по поддержанию доступности.

Реестр квалифицированных сертификатов КУЦ ведётся в форме ПАК «Центр регистрации» и предназначен для обеспечения реализации следующих функций КУЦ:

- Ведения Реестра зарегистрированных пользователей КУЦ;
- Ведения Реестра сертификатов ключей проверки ЭП КУЦ;
- Ведения Реестра запросов на создание сертификатов ключей проверки ЭП пользователей КУЦ;
- Ведения Реестра запросов на аннулирование (отзыв) сертификатов ключей проверки ЭП пользователей КУЦ;

Информация о прекращении действия или аннулировании квалифицированного сертификата вносится в реестр квалифицированных сертификатов в срок не более 12 часов после поступления заявления о прекращении действия или аннулировании квалифицированного сертификата.

УЦ определяет следующий порядок доступа к реестру сертификатов - предоставление сведений из реестра квалифицированных сертификатов КУЦ производится по запросам пользователей через форму размещённую на сайте: https://crypto.rosatom.ru/ca/reestr-sertifikatov/

КУЦ предоставляет по запросу информацию о выпущенных сертификатах, путем заполнения формы с указанием (серийного номера квалифицированного сертификата, ФИО владельца квалифицированного сертификата, Email на который необходимо получить информации о выпущенном квалицированном сертификате АО «Гринатом»).

Доступ любому лицу к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата осуществляется безвозмездно.

Публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов производится путём публикации действующего списка отозванных сертификатов.

Предоставление информации о сертификате осуществляется в течении 24 часов после подачи заявки в электронном виде.

4.9. Порядок технического обслуживания реестра квалифицированных сертификатов.

Максимальный срок проведения технического обслуживания реестра квалифицированных сертификатов составляет 12 часов;

В случае проведения технического обслуживания реестра квалифицированных

сертификатов Администратор КУЦ производит уведомление участников информационного взаимодействия о проведении технического обслуживания путём публикации сведений о проведений технического обслуживания на сайте КУЦ: https://crypto.rosatom.ru/ca/reestr-sertifikatov/

4.10. Порядок проведения разбора конфликтной ситуации, связанной с применением электронной подписи в электронном документе

Настоящий раздел описывает порядок разбора конфликтной ситуации на основе работы согласительной комиссии, формируемой из числа участников информационной системы и сотрудников КУЦ, как третьей стороны, обеспечивающей подтверждение подлинности электронной подписи в электронных документах в отношении сертификатов ключей проверки электронной подписи, созданных КУЦ. КУЦ в описанном случае является организатором работы согласительной комиссии.

В общем случае порядок разбора конфликтной ситуации устанавливается оператором информационной системы, либо соглашением между участниками информационной системы и может отличаться от приведенного.

Разрешение конфликтных ситуаций, возникающих в информационной системе и связанных с применением электронной подписи, осуществляется согласительной комиссией. Согласительная комиссия создается с целью разрешения конфликтных ситуаций при обмене (в связи с обменом) и применении электронных документов, подписанных электронной подписью.

Конфликтная ситуация может возникнуть между участниками информационной системы. При возникновении разногласий участник информационной системы (сторона-инициатор), обязан направить в КУЦ заявление о разногласиях, возникших при обмене (в связи с обменом) и применением электронных документов с другим участником информационной системы (сторона-ответчик), подписанное собственноручной подписью уполномоченного на данное действие лицом, с подробным изложением причин разногласий и предложением создать комиссию по ее разрешению.

По заявлению о разногласиях КУЦ формирует согласительную комиссию, в которую входят:

- представитель КУЦ – председатель комиссии.
- Пользователь информационной системы – представитель участника информационной системы (сторона-инициатор), который непосредственно участвовал в информационном обмене электронными документами, по которым возникли разногласия;
- Пользователь информационной системы - представитель участника информационной системы (сторона-ответчик), который непосредственно участвовал в информационном обмене электронными документами, по которым возникли разногласия.

Комиссия осуществляет свою деятельность по месторасположению КУЦ. Язык работы согласительной комиссии – русский.

Сторона-инициатор представляет заявление о разногласии (уведомление о возникших разногласиях) с указанием:

- даты подачи заявления (уведомления);
- информации, идентифицирующей инициатора и ответчика;
- обстоятельств, на которых основаны заявленные требования;
- обоснованного расчета заявленных требований;
- нормы законодательных и иных нормативных правовых актов, на основании которых заявляется требование;

- прилагаемые к заявлению (уведомлению) о разногласии документы, составляющие доказательную базу.

До начала работы согласительной комиссии стороне - инициатору рекомендуется убедиться в целостности установленных на его технических средствах программного обеспечения, в том числе средства электронной подписи, а также отсутствии несанкционированных действий со стороны третьих лиц.

Сторона-ответчик обязана в период работы комиссии представить стороне-инициатору и комиссии возражения по каждому требованию, изложенному в заявлении о разногласиях, либо согласиться с предъявляемыми требованиями.

В возражениях ответчика на каждое требование должны содержаться документально обоснованные ответы или сделана ссылка на доказательства, которые могут быть представлены в ходе работы комиссии.

Любая сторона в ходе работы комиссии может внести ходатайства об изменении или дополнении своих требований или возражений.

Комиссия в ходе разбирательства в любой момент может затребовать от сторон предоставления документов, вещественных или иных доказательств в устанавливаемый комиссией срок.

Рассмотрение конфликтной ситуации производится на основании всех представленных документов, доказательств.

В том случае, если обстоятельства, имеющие значение для принятия решения по делу, могут быть исследованы только на основе применения специальных научных знаний, комиссия вправе назначить экспертизу по подтверждению подлинности электронной подписи в электронном документе.

Проведение экспертизы возлагается на КУЦ, выдавший сертификат ключа проверки электронной подписи, с использованием которого была сформирована электронная подпись электронного документа, являющегося предметом разногласий. Запрос на проведение экспертизы оформляется заявлением на подтверждение подлинности электронной подписи в электронном документе, подающемся в КУЦ от лица участника информационной системы - владельца сертификата ключа проверки электронной подписи (см. пункт 6.10 и 6.11 настоящего Регламента).

Порядок проведения экспертных работ КУЦ по подтверждению подлинности электронной подписи в электронном документе устанавливается КУЦ. Для проведения указанных работ электронные документы и их электронная подпись экспортируются из информационной системы в соответствующие файлы и предоставляются вместе с заявлением на подтверждение подлинности электронной подписи в КУЦ. Результатом проведения экспертных работ является заключение КУЦ.

Экспертиза может быть назначена комиссией по обоснованному ходатайству любой из сторон или по ее собственной инициативе.

По итогам работы согласительной комиссии составляется акт, в котором содержится краткое изложение выводов комиссии и решение комиссии по рассматриваемому разногласию.

Помимо изложения выводов согласительной комиссии и решения комиссии акт содержит следующие данные:

- состав комиссии;
- дату и место составления акта;
- дату и время начала и окончания работы комиссии;
- краткий перечень мероприятий, проведенных комиссией;
- выводы комиссии;

- собственноручные подписи членов комиссии;
- указание на особое мнение члена (или членов комиссии), в случае наличия такового.

Акт составляется в 3-х экземплярах и предоставляется по одному экземпляру для каждой из сторон конфликтной ситуации, а также удостоверяющему центру.

5. Порядок исполнения обязанностей Удостоверяющего центра

5.1. информирование заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

При выдаче квалифицированного сертификата КУЦ производит информирование заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки путём предоставления руководства по обеспечению безопасности.

5.2. выдача по обращению заявителя средств электронной подписи.

Порядок выдачи и учёта средств электронной подписи определён в документе: «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»

Средства электронной подписи в соответствии с частью 4 статьи 6 Федерального закона «Об электронной подписи» обеспечивают возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями;

5.3. обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов производится путём внесения сведений в реестр Оператором КУЦ

Обеспечение защиты информации, содержащейся в реестре квалифицированных сертификатов от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий производится путём применения сертифицированных средств КУЦ в качестве реестра сертификатов КУЦ.

5.4. обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети "Интернет" в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов;

Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов, производится за счёт применения средств отказоустойчивости и проведения организационно-технических мероприятий по поддержанию доступности.

5.5. порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей.

Ключи ЭП пользователей КУЦ записываются при их генерации на типы ключевых носителей, которые поддерживаются используемым средством криптографической защиты информации.

В качестве ключевых носителей используются сертифицированные ключевые носителю Рутокен.

Ключи ЭП на ключевом носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует сотрудник КУЦ в соответствии с требованиями на используемое средство криптографической защиты информации.

Для обеспечения конфиденциальности Ключи ЭП создаются в не экспортируемом формате. По запросу пользователя с обоснованием причин и по согласованию Администратора КУЦ ключи ЭП могут быть созданы в экспортируемом формате.

Сотрудник КУЦ сообщает сформированный пароль (ПИН-код) владельцу ключей ЭП.

Ключи ЭП до момента передачи владельцу находятся на временном хранении ключей электронных подписей у Сотрудника КУЦ или доверенного лица КУЦ. Срок временного хранения не может превышать срок действия сертификата ключа проверки электронной подписи, соответствующего данному ключу ЭП. В случае истечения срока временного хранения ключи ЭП подлежат уничтожению в десятидневный срок.

Ответственность за сохранение пароля (ПИН-кода) в тайне до момента передачи владельцу возлагаются на сотрудника КУЦ, ответственного за создание данного ключа. Для вручения ключа ЭП владельцу Оператор КУЦ имеет право передать ключ уполномоченному доверенному лицу КУЦ. Созданные ключи и ПИН-коды к ним хранятся исключительно в специальных помещениях КУЦ с ограничением доступа посторонних лиц в данные помещения.

После вручения квалифицированного сертификата ответственность за сохранение пароля (ПИН-кода) в тайне возлагается на владельца ключей ЭП.

Сотрудники КУЦ, являющиеся владельцами ключей ЭП, также выполняют указанные в разделе меры защиты ключей ЭП.

5.6. осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона "Об электронной подписи";

После создания квалифицированного сертификата КУЦ осуществляет регистрацию квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи»

5.7. осуществление по желанию лица, которому выдан квалифицированный сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации;

По желанию лица, которому выдан квалифицированный сертификат, КУЦ на безвозмездной основе производит регистрацию указанного лица в единой системе идентификации и аутентификации

5.8. предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня

прекративших свое действие (аннулированных) квалифицированных сертификатов.

Предоставление сведений из реестра квалифицированных сертификатов КУЦ производится по запросам пользователей через форму размещённую на сайте: https://crypto.rosatom.ru/ca/reestr-sertifikatov/

Доступ любому лицу к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата осуществляется безвозмездно.

6. Политика конфиденциальности

6.1. Типы конфиденциальной информации

Ключ ЭП владельца сертификата ключа проверки ЭП является конфиденциальной информацией данного Пользователя КУЦ.

Персональная и корпоративная информация пользователей КУЦ, содержащаяся в КУЦ, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки ЭП, списка отозванных сертификатов, считается конфиденциальной и не публикуется.

Информация, хранящаяся в журналах аудита КУЦ, считается конфиденциальной и не подлежит разглашению.

Отчётные материалы по выполненным проверкам деятельности КУЦ являются конфиденциальными, за исключением заключения по результатам проверок, публикуемого в соответствии с настоящим Регламентом.

6.2. Типы информации, не являющейся конфиденциальной

Информация, не являющейся конфиденциальной информацией, является открытой информацией.

Открытая информация может публиковаться по решению КУЦ. Место, способ и время публикации также определяется решением КУЦ.

Информация, включаемая в сертификаты ключей проверки ЭП пользователей КУЦ и списки отозванных сертификатов, издаваемые КУЦ, не считается конфиденциальной.

Также не считается конфиденциальной информация о настоящем Регламенте.

6.3. Исключительные полномочия официальных лиц

УЦ не раскрывает информацию, относящуюся к типу конфиденциальной информации, каким бы то ни было третьим лицам, за исключением:

- случаев, определённых в настоящем Регламенте;
- случаев, требующих раскрытия в соответствии с действующим законодательством или при наличии судебного постановления.

7. Дополнительные положения

7.1. Сроки действия ключей КУЦ

Максимальный срок действия ключа ЭП и сертификата ключа проверки ЭП КУЦ определяются требованиями применяемого средства криптографической защиты информации.

Для «КриптоПро УЦ» установлены следующие максимальные сроки действия ключей ЭП и ключей проверки ЭП КУЦ.

При использовании СКЗИ «КриптоПро CSP» 1 год и 3 месяца или 3 года (при условии, что общее время использования ключа ЭП для выполнения целевых функций в течение 3-х лет его действия ограничено 1 годом и 3 месяцами, остальное время ключ ЭП используется только для подписи списков отозванных сертификатов). Сроки действия сертификата ключа проверки ЭП составляют 16 и 18 лет соответственно.

При создании и хранении ключа ЭП посредством ПАКМ «КриптоПро HSM» – 3 года или 5 лет (при условии, что общее время использования ключа ЭП для выполнения целевых функций в течение пяти лет его действия ограничено 3 годами, остальное время ключ ЭП используется только для подписи списков отозванных сертификатов). Сроки действия сертификата ключа проверки ЭП составляют 18 и 20 лет соответственно.

Начало периода действия ключа ЭП КУЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП.

7.2. Требования к средствам электронной подписи, использующимся в составе КУЦ и требования к средствам электронной подписи пользователей КУЦ

Средства электронной подписи КУЦ и средства электронной подписи пользователя КУЦ должны удовлетворять требованиям Федерального закона №63-ФЗ «Об электронной подписи» и требованиям Приказа ФСБ Российской Федерации от 27.12.2011 г. №796.

Формирование и проверка электронной подписи на серверных компонентах КУЦ, а именно на Центре сертификации и Центре регистрации осуществляется Администратором КУЦ или в автоматическом режиме, под контролем лица, ответственного за создание и проверку ЭП в ЦС.

На Автоматизированном рабочем месте Администратора Центра регистрации выполнение операции создания электронной подписи под запросами на регистрацию, запросами на сертификат, запросами на управление статусом сертификата осуществляется только после того, как Администратор КУЦ ознакомится с содержимым подписываемого документа. После ознакомления Администратор КУЦ подтверждает создание электронной подписи. Выполнение операции создания электронной подписи заканчивается уведомлением о выполнении операции, связанной с созданием электронной подписи (положительный результат свидетельствует об успешном создании ЭП, отрицательный – ЭП не создана).

На Автоматизированных рабочих местах Администратора Центра регистрации и разбора конфликтных ситуаций выполнение операции проверки электронной подписи сопровождается ознакомлением с электронным документом, информированием о внесении изменений в электронный документ (при изменении электронного документа появляется сообщение – электронная подпись – «Не верна»), отображением сертификата ключа проверки ЭП подписчика данного электронного документа.

7.3. Сроки действия ключей ЭП и сертификатов ключей проверки ЭП пользователей КУЦ

Максимальный срок действия ключа ЭП Пользователя КУЦ, соответствующего сертификату ключа проверки ЭП, владельцем которого он является, определяется требованиями средства криптографической защиты информации, использующим данный ключ ЭП.

Начало периода действия ключа ЭП Пользователя КУЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП Пользователя КУЦ.

Срок действия ключа проверки ЭП устанавливается равным сроку действия сертификата ключа проверки ЭП.

Максимальный срок действия сертификата ключа проверки ЭП Пользователя КУЦ определяется требованиями средства криптографической защиты информации, использующим ключ ЭП пользователя, соответствующий указанному сертификату.

Установлены следующие максимальные сроки действия ключей ЭП и ключей проверки ЭП Пользователей КУЦ:

- Срок действия ключа ЭП — 1 год 3 месяца; При этом устанавливается, что срок действия ключа для планового использования составляет 1 год. Срок действия сертификата на период смены ключа составляет 3 месяца)
- Срок действия ключа проверки ЭП — 1 год 3 месяца, но не более сроков действия соответствующих ключей проверки ЭП, обеспечиваемых используемыми пользователями ПАК «КриптоПро УЦ 2.0» средствами ЭП и средствами КУЦ.

Конкретный срок действия сертификата ключа проверки ЭП устанавливается КУЦ в момент его создания.

Максимальные сроки действия ключа ЭП и ключа проверки ЭП Пользователя КУЦ определяются типом запрашиваемого сертификата. Тип сертификата назначается Оператором КУЦ. При назначении сроков действия КУЦ учитывает пожелания пользователей из запроса на сертификат, которые, однако, не могут вывести назначенные сроки из интервала времени, ограниченного максимальными сроками действия.

Приложение №1 к настоящему регламенту содержит описание всех шаблонов сертификатов, поддерживаемых КУЦ, с указанием сроков действия ключа ЭП и ключа проверки ЭП.

7.4. Архивное хранение документированной информации

Архивированию подлежат следующая документированная информация:

- Реестр сертификатов ключей проверки ЭП пользователей КУЦ;
- сертификаты ключей проверки ЭП КУЦ;
- журналы аудита программно-аппаратных средств обеспечения деятельности КУЦ;
- заявления на аннулирование (отзыв) сертификатов ключей проверки ЭП;

Источником комплектования архивного фонда КУЦ являются подразделения КУЦ, обеспечивающие документирование.

Архивные документы хранятся в специально оборудованном помещении-архивохранилище.

Документы, подлежащие архивному хранению, являются документами временного хранения.

Срок хранения архивных документов устанавливается 5 лет.

Выделение архивных документов к уничтожению и уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников Отдела криптографической защиты и назначаемой приказом руководителя КУЦ.

8. Структуры сертификатов и списков отозванных сертификатов

8.1. Структура квалифицированного сертификата

Квалифицированный сертификат ключа проверки электронной подписи в электронной форме создается в формате X.509 версии 3, структура квалифицированного сертификата ключа проверки ЭП должна удовлетворять требованиям Федерального закона №63ФЗ «Об электронной подписи» (с учетом изменений, вносимых Федеральным законом №445-ФЗ) и Приказа ФСБ России от 27.12.2011 г. №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Структура квалифицированного 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 34.11/34.10-2012
Issuer	УЦ Издатель сертификата	Согласно Таблицы заполнения поля Субъект (для ЮЛ, автоматическое создание/проверка ЭП)
Validity Period	Срок действия сертификата	Действителен с (not Before): дд.мм.гггг чч:мм:сс UTC Действителен по (not After): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	Согласно Таблицы заполнения поля Субъект
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Signature	ЭП КУЦ издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Дополнения сертификата		
Authority Key Identifier	Идентификатор ключа КУЦ издателя сертификата	Идентификатор ключа подписи Удостоверяющего центра, на котором подписан данный сертификат; УЦ – издатель сертификата, заполняется Согласно Таблицы заполнения поля Субъект (для ЮЛ, авторматическое создание/проверка ЭП); Серийный номер сертификата КУЦ
Key Usage (critical)	Область использования ключа	Набор областей использования ключа (реализуется установкой соответствующих битов в значение «1»).
Certificate Policies	Политика сертификации	[1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1
Subject Sign Tool	Средство ЭП владельца сертификата	Средство электронной подписи: СКЗИ "КриптоПро CSP" (версия 4.0)
Issuer Sign Tool	Средство ЭП и средство К У Ц, использующиеся для создания сертификатов	Средство электронной подписи: СКЗИ "КриптоПро CSP" (версия 4.0) Заключение на средство ЭП: Сертификат соответствия № СФ/124-3380 от 11.05.2018 Средство КУЦ: ПАК "КриптоПро УЦ" версии 2.0 Заключение на средство КУЦ: Сертификат соответствия № СФ/128-3592 от 17.10.2018
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор ключа подписи владельца сертификата
Extended Key Usage (необязательное дополнение)	Расширенная область использования ключа	Набор расширенных областей использования ключа объектных идентификаторов
CRL Distribution Point (необязательное дополнение)	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/Name.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, Name – наименование файла списка отозванных сертификатов
Authority Information Access (необязательное дополнение)	Адрес Службы актуальных статусов сертификатов, Адрес размещения информации о сертификате КУЦ	URL адреса Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP URL адреса размещения файла сертификата КУЦ
Private Key Period (необязательное дополнение)	Период использования ключа подписи	Действителен с (not Before): дд.мм.гггг чч:мм:сс UTC Действителен по (not After): дд.мм.гггг чч:мм:сс UTC
	В сертификат могут быть добавлены дополнительные поля и дополнения согласно RFC 5280	

Таблица заполнения поля Субъект квалифицированного сертификата ключа проверки электронной подписи

Физическое лицо	Физическое лицо – индивидуальный предприниматель	Юридическое лицо с информацией о представителе (российское юрлицо)	Юридическое лицо без информации о представителе (автоматическое создание и/или проверка ЭП) (российское юрлицо)	Юридическое лицо с информацией о представителе (иностранное юрлицо)	Юридическое лицо без информации о представителе (автоматическое создание и/или проверка ЭП) (иностранное юрлицо)
commonName (общее имя) ФИО	commonName (общее имя) ФИО	commonName (общее имя) – полное или сокращенное наименование юридического лица в соответствии с учредительными документами	commonName (общее имя) полное или сокращенное наименование юридического лица в соответствии с учредительными документами	commonName (общее имя) – полное или сокращенное наименование юридического лица в соответствии с учредительными документами	commonName (общее имя) – полное или сокращенное наименование юридического лица в соответствии с учредительными документами
surname (фамилия) – фамилия	surname (фамилия) – фамилия	surname (фамилия) – фамилия представителя		surname (фамилия) – фамилия представителя	
givenName (приобретенное имя) – имя и отчество	givenName (приобретенное имя) – имя и отчество	givenName (приобретенное имя) – имя и отчество представителя		givenName (приобретенное имя) – имя и отчество представителя	
countryName (наименование страны) – двухсимвольный код	countryName (наименование страны) – двухсимвольный код	countryName (наименование страны) – двухсимвольный код RU	countryName (наименование страны) – двухсимвольный код RU	countryName (наименование страны) – двухсимвольный код	countryName (наименование страны) – двухсимвольный код
stateOrProvinceName (наименование штата или области) наименование субъекта РФ	stateOrProvinceName (наименование штата или области) наименование субъекта РФ	stateOrProvinceName (наименование штата или области) наименование субъекта РФ	stateOrProvinceName (наименование штата или области) - наименование субъекта РФ		
localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)
streetAddress (название улицы, номер дома) опционально	streetAddress (название улицы, номер дома) опционально	streetAddress (название улицы, номер дома)	streetAddress (название улицы, номер дома)	streetAddress (название улицы, номер дома)	streetAddress (название улицы, номер дома)
		organizationName (наименование организации)	organizationName (наименование организации)	organizationName (наименование организации)	organizationName (наименование организации)
		organizationUnitName (подразделение)	organizationUnitName (подразделение) опционально	organizationUnitName (подразделение)	organizationUnitName (подразделение) опционально
		title (должность) – должность представителя		title (должность) – должность представителя	
E-mail (адрес электронной почты) опционально	E-mail (адрес электронной почты) опционально	E-mail (адрес электронной почты) опционально	E-mail (адрес электронной почты) опционально	E-mail (адрес электронной почты) опционально	E-mail (адрес электронной почты) опционально
		OGRN (ОГРН)	OGRN (ОГРН)		
SNILS (СНИЛС)	SNILS (СНИЛС)	SNILS (СНИЛС) представителя			
INN (ИНН)	INN (ИНН)	INN (ИНН) – юридического лица	INN (ИНН) – юридического лица	INN (ИНН) – юридического лица	INN (ИНН) – юридического лица
	OGRNIP (ОГРНИП)				

8.2. Структура списка отозванных сертификатов, изготавливаемого КУЦ в электронной форме

УЦ изготавливает списки отозванных сертификатов ключей проверки ЭП пользователей КУЦ в электронной форме (далее по тексту раздела — СОС) формата X.509 версии 2.

При создании списка отозванных сертификатов КУЦ использует следующие расширения:

- Расширение «Authority Key Identifier» содержит идентификатор ключа КУЦ;
- Расширение «Reason Code» содержит код причины отзыва сертификата ключа проверки ЭП;
- Расширение «Microsoft CA Version» содержит номер сертификата Центра сертификации.

9. Программные и технические средства обеспечения деятельности КУЦ

Для реализации своих услуг и обеспечения жизнедеятельности КУЦ использует следующие программные и технические средства:

- Программный комплекс обеспечения реализации целевых функций КУЦ (ЖТЯИ.00078-01 99 01), далее по тексту — ПК КУЦ;
- Технические средства обеспечения работы ПК КУЦ, далее по тексту — ТС КУЦ;
- Программные и программно-аппаратные средства защиты информации, (далее - СЗИ КУЦ)

9.1. Программный комплекс обеспечения реализации целевых функций КУЦ

Каждый логический компонент «КриптоПро УЦ» оснащается необходимым набором программных компонент «КриптоПро УЦ», которые поставляются в виде единого пакета установки «КриптоПро УЦ. Комплекс программ» (ЖТЯИ.00078-01 99 01).

Пакет установки «КриптоПро УЦ» устанавливает следующие программы:

- ПАК «Сервер центр сертификации»
- ПАК «Сервер центр регистрации»
- Программный компонент КУЦ «Консоль управления ЦР»
- Программный компонент КУЦ «Консоль экспертизы ЭП»

Роль КУЦ — это набор программ, которые при правильной установке и настройке позволяют компьютеру выполнять определённую функцию КУЦ. Роли КУЦ определяют основную функцию, назначение или цель использования компьютера. Можно назначить компьютер для выполнения одной роли, которая интенсивно используется в КУЦ, или для выполнения нескольких ролей, если каждая из них применяется лишь изредка.

Логические компоненты КУЦ могут разворачиваться не только на серверных, но и на клиентских операционных системах (в отличие от Windows, где «Диспетчер сервера» доступен только на серверных операционных системах и все Роли могут быть добавлены только на серверах).

Роли КУЦ позволяют настроить сервер или рабочую станцию в качестве одной или нескольких логических структурных элементов КУЦ. Они обычно имеют собственные базы данных, в которых создаются очереди запросов. После правильной установки и настройки Роли КУЦ функционируют автоматически. Это позволяет компьютерам, на которых они установлены, выполнять назначенные задачи при ограниченном участии пользователя.

Программные компоненты КУЦ, требуемые для разворачивания логических структурных компонент КУЦ

Логический компонент КУЦ	Требуемые программные компоненты «КриптоПро УЦ»
Центр сертификации	Программный компонент КУЦ «Диспетчер УЦ», Роль УЦ «Сервер центров сертификации»
Центр регистрации	Программный компонент КУЦ «Диспетчер УЦ», Роль УЦ «Сервер центров регистрации»
АРМ обслуживающего персонала	Программный компонент УЦ «Консоль управления ЦР»
АРМ разбора конфликтных ситуаций	Программный компонент УЦ «Консоль экспертизы ЭП»
АРМ пользователя	Специальные программные компоненты «КриптоПро УЦ» не требуются

Центр сертификации является логическим компонентом КУЦ и предназначен для обеспечения реализации следующих целевых функций КУЦ:

- Формирования сертификатов ключей проверки ЭП пользователей КУЦ в электронной форме с использованием ключа ЭП и сертификата ключа проверки ЭП КУЦ;
- Формирования списков отозванных сертификатов ключей проверки ЭП пользователей КУЦ в электронной форме с использованием ключей ЭП и сертификатов ключей проверки ЭП КУЦ на основе эталонной копии списка отозванных сертификатов ключей проверки ЭП пользователей КУЦ;
- Ведения эталонной копии Реестра сертификатов ключей проверки ЭП КУЦ;
- Ведения эталонной копии списка отозванных сертификатов ключей проверки ЭП пользователей КУЦ;
- Обеспечения уникальности ключей проверки ЭП в изданных сертификатах ключей проверки ЭП пользователей КУЦ.

Центр регистрации является логическим компонентом КУЦ и предназначен для обеспечения реализации следующих целевых функций КУЦ:

- Ведения Реестра зарегистрированных пользователей КУЦ;
- Ведения Реестра сертификатов ключей проверки ЭП КУЦ;
- Ведения Реестра заявлений на создание сертификатов ключей проверки ЭП пользователей КУЦ;
- Ведения Реестра заявлений на аннулирование (отзыв) сертификатов ключей проверки ЭП пользователей КУЦ;
- Предоставления программных средств для зарегистрированных пользователей КУЦ для обеспечения реализации их прав в части пользования предоставляемыми программными средствами.

АРМ обслуживающего персонала ЦР предназначен для обеспечения реализации своих функциональных обязанностей сотрудникам КУЦ.

АРМ разбора конфликтных ситуаций предназначен для обеспечения своих функциональных обязанностей сотрудникам КУЦ в части взаимодействия с пользователями КУЦ при разрешении вопросов, связанных с подтверждением электронной подписи КУЦ в сертификатах ключей проверки ЭП, созданых КУЦ в электронной форме.

9.2. Технические средства обеспечения работы ПК КУЦ

Технические средства обеспечения работы ПК КУЦ включают в себя:

- Выделенный сервер Центра сертификации;
- Выделенный сервер Центра регистрации;
- Телекоммуникационное оборудование;
- Компьютеры рабочих мест сотрудников КУЦ;
- Устройства печати на бумажных носителях (принтеры).

9.3. Программные и программно-аппаратные средства защиты информации

Программные и программно-аппаратные средства защиты информации включают в себя:

- Средства криптографической защиты информации;
- Программно-аппаратные комплексы защиты от несанкционированного доступа типа «электронный замок»;
- Устройства для обеспечения бесперебойного питания серверов Центра сертификации и Центра регистрации;
- Устройства обеспечения температурно-влажностного режима и кондиционирования служебных и рабочих помещений КУЦ;
- Устройства обеспечения противопожарной безопасности помещений КУЦ.

На компонентах КУЦ используются средства криптографической защиты информации (средства электронной подписи), входящие в состав комплектации «КриптоПро УЦ».

9.4. Перечень событий, регистрируемых программным комплексом обеспечения реализации целевых функций КУЦ

Основные типы событий, регистрируемые программными компонентами КУЦ:

Центром Сертификации:

- Поступление запроса на сертификат;
- Издание сертификата;
- Издан СОС;
- Невыполнение внутренней операции программной компоненты;
- Системные события общесистемного программного обеспечения.

Центром Регистрации:

- Помещен запрос на регистрацию;
- Принят запрос на регистрацию;
- Отклонен запрос на регистрацию;
- Помещен запрос на сертификат;
- Принят запрос на сертификат;
- Отклонен запрос на сертификат;
- Установка сертификата подтверждена пользователем;
- Помещен запрос на отзыв сертификата;
- Принят запрос на отзыв сертификата;
- Отклонен запрос на отзыв сертификата;
- Помещен запрос на первый сертификат;
- Запрошен список отозванных сертификатов;

- Опубликован список отозванных сертификатов;
- Невыполнение внутренней операции программной компоненты;
- Установлено сетевое соединение с внешней программной компонентой;
- Системные события общесистемного программного обеспечения.

Структуры записей событий приведены в эксплуатационной документации ПК КУЦ и общесистемного программного обеспечения.

9.5. Перечень данных программного комплекса обеспечения реализации целевых функций КУЦ, подлежащих резервному копированию

При эксплуатации программного комплекса обеспечения реализации целевых функций КУЦ ежесуточно выполняется резервное копирование данных компонент ПК КУЦ.

Перечень данных ПК КУЦ, подлежащих резервному копированию, включает в себя:

- Базу данных КУЦ, включающую журнал выданных сертификатов, очередь запросов, сертификаты ключей проверки ЭП КУЦ;
- Журналы аудита компонент ПК КУЦ в составе, определённом эксплуатационной документацией ПК КУЦ.

9.6. Порядок технического обслуживания средств обеспечения деятельности КУЦ

Порядок технического обслуживания средств обеспечения деятельности КУЦ, построенного на базе программно-аппаратного комплекса «Удостоверяющий Центр «КриптоПро УЦ» содержит описание и правила выполнения работ по техническому обслуживанию средств удостоверяющего центра.

Техническое обслуживание средств обеспечения деятельности КУЦ направлено на обеспечение постоянной готовности указанных средств к использованию по прямому назначению и предотвращению выхода их из строя.

Техническое обслуживание средств обеспечения деятельности КУЦ включает:

- техническое обслуживание вычислительной техники и периферийного оборудования;
- техническое обслуживание общесистемного и специализированного программного обеспечения.

9.6.1. Техническое обслуживание вычислительной техники и периферийного оборудования

К средствам вычислительной техники и периферийному оборудованию КУЦ относятся:

- Сервер Центра сертификации;
- Сервер Центра регистрации;
- Автоматизированные рабочие места привилегированных пользователей Удостоверяющего центра (администраторов КУЦ и операторов КУЦ);
- Автоматизированное рабочее место разбора конфликтных ситуаций;
- Программно-аппаратный криптографический модуль (ПАКМ) «КриптоПро HSM» (может отсутствовать в случае использования на Центре сертификации СКЗИ «КриптоПро CSP»);
- Источник бесперебойного питания (может отсутствовать в случае использования в эксплуатирующей организации единой централизованной системы бесперебойного питания);
- Сетевое и коммутационное оборудование.

Все виды работ по техническому обслуживанию вычислительной техники и периферийного оборудования проводятся по установленному графику, вне зависимости от

технического состояния изделия. Уменьшать установленный объем и изменять периодичность технического обслуживания не рекомендуется.

Для поддержания работоспособности КУЦ производятся периодические осмотры входящего в него оборудования.

Техническое обслуживание вычислительной техники и периферийного оборудования включает в себя следующие виды работ:

№	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1.	Проверка внешнего вида корпусов оборудования, сетевого и соединительного шнуров на отсутствие повреждений	Ежедневно	Проводится визуально	Допускается проводить внешний осмотр оборудования без выключения напряжения питания. Эксплуатация оборудования с повреждениями категорически запрещается.
2.	Проверка работоспособности	Ежедневно	Проверяется исправность оборудования посредством выполнения штатных задач, запускаемых в связи с основной деятельностью удостоверяющего центра (по назначению)	Проводится с учётом местных условий эксплуатации
3.	Проверка пломбировки, маркировки, целостности корпусов оборудования	Ежедневно	Проводится визуально	При нарушении пломбировки, маркировки, целостности корпуса оборудования дальнейшая эксплуатация изделия запрещена до установления причин нарушения пломбировки, маркировки, целостности корпуса
4.	Очистка от пыли и грязи	Один раз в месяц	Отключить изделие от сети переменного тока. Удалить с поверхности изделия пыль, грязь и влагу. Для очистки изделия от пыли и грязи допускается использование мягкой ветоши (легкая безворсовая ткань, например, марля хлопчатобумажная ГОСТ 11109 – 74) и неагрессивных моющих растворов.	Очистку выполнять путем последовательной протирки поверхностей: 1) влажной салфеткой, смоченной в 5 % растворе бытовых моющих средств; 2) влажной салфеткой, смоченной в чистой воде; 3) сухой салфеткой. При протирке не допускать попадания влаги на разъемные соединения и токоведущие цепи
5.	Контрольная проверка работоспособности оборудования	Один раз в год	Проверку оборудования необходимо выполнять путем прогона контрольной задачи	Контрольная проверка оборудования необязательна в случае его устойчивой работоспособности по назначению
6.	Текущий ремонт	По мере необходимости	Оборудование может быть отремонтировано у эксплуатирующей организации. В случае выхода из строя подлежит замене или ремонту в условиях предприятия изготовителя.	
7.	Дополнительные работы	Согласно руководства по эксплуатации на	В том случае, если требованиями эксплуатационной документации на конкретное оборудование	

		конкретное оборудование	предусмотрено обязательное выполнение определенных работ по его техническому обслуживанию, то данные работы должны быть включены в указанный перечень проводимых работ	

Оборудование рекомендуется периодически (один раз в год) подвергать техническому осмотру с участием специалистов предприятия-изготовителя или специалистов рекомендуемого предприятием-изготовителем сервисного центра.

По истечении срока гарантии оборудования рекомендуется заключение с предприятием изготовителем или соответствующим сервисным центром договора на техническое обслуживание оборудования.

Запрещается осуществлять самовольную регулировку, ремонт, переустановку или вносить какие-либо изменения в конструкцию оборудования.

Техническое обслуживание оборудования, входящего в состав КУЦ, производится в соответствии с инструкциями по эксплуатации каждого аппарата в него входящего.

Все неисправности оборудования, обнаруженные при периодических осмотрах, должны устраняться по мере их выявления и регистрироваться в соответствующем журнале.

9.6.2. Техническое обслуживание общесистемного и специализированного программного обеспечения

Общесистемное программное обеспечение включает в себя структурные компоненты операционной системы, средства управления базами данных, а также стандартные средства администрирования операционной системы.

К специализированному программному обеспечению относятся:

- Средства криптографической защиты информации (СКЗИ «КриптоПро CSP», ПАКМ «КриптоПро HSM»);
- Средства обеспечения деятельности КУЦ (ПАК «Удостоверяющий центр «КриптоПро УЦ»);
- Антивирусные средства;
- Средства резервного хранения данных.

Техническое обслуживание общесистемного программного обеспечения включает в себя выполнение следующих видов работ:

№ п/п	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1.	Проверка целостности загрузочных секторов диска и общесистемных файлов	При включении серверов Центра сертификации, Центра регистрации, АРМ привилегированных пользователей, АРМ разбора конфликтных ситуаций,	Проводится средствами аппаратно-программного модуля доверенной загрузки типа «Электронный замок» до загрузки операционной системы	
2.	Проверка работоспособности операционной системы	Ежедневно	Проверяется исправность системы посредством выполнения общесистемных задач, запускаемых в связи с основной деятельностью удостоверяющего центра (по назначению)	Проводится с учётом местных условий эксплуатации
3.	Проверка на наличие вирусов	Ежедневно	Осуществляется с использованием специализированных средств антивирусного контроля. Рекомендуется использовать в автоматическом режиме	
4.	Обновление операционной	По мере выхода критических	Осуществляется с использованием стандартных средств	

	системы	обновлений операционной системы	администрирования операционной системы (Windows Update)	
5.	Создание резервного образа диска	Один раз в неделю	Осуществляется с использованием специализированных средств резервного хранения данных	
6.	Проверка наличия свободного дискового пространства на системном диске и удаление ненужных файлов	Один раз в месяц	Проводится с использованием стандартных средств администрирования операционной системы	
7.	Проверка состояния файловой системы	Один раз в три месяца	Проводится с использованием стандартных средств администрирования операционной системы	
8.	Восстановление работоспособности операционной системы	По мере необходимости	Осуществляется посредством восстановления или переустановки операционной системы, а также восстановления образа всего диска	

Техническое обслуживание специализированного программного обеспечения включает в себя выполнение следующих видов работ:

№	Наименовани работы	Периодичность выполнения работы	Порядок проведения	Примечание
1.	Проверка целостности программных модулей СКЗИ и ПАК «КриптоПро УЦ»	При включении серверов Центра сертификации, Центра регистрации, АРМ привилегированных пользователей, АРМ разбора конфликтных ситуаций,ПАКМ «КриптоПро HSM»	Проводится средствами аппаратно-программного модуля доверенной загрузки типа «Электронный замок» до загрузки операционной системы	
2.	Проверка работоспособности СКЗИ и ПАК «КриптоПро УЦ»	Ежедневно	Проверяется исправность средств в связи с основной деятельностью удостоверяющего центра (по назначению)	Проводится с учётом местных условий эксплуатации
3.	Обновление антивирусных баз	Ежедневно	Осуществляется с использованием специализированных средств антивирусного контроля. Рекомендуется использовать в автоматическом режиме	
4.	Создание резервных копий баз данных удостоверяющего центра	Ежедневно	Осуществляется с использованием специализированных средств резервного хранения данных. Рекомендуется выполнять в автоматическом режиме	
5.	Создание резервного образа диска	Один раз в неделю	Осуществляется с использованием специализированных средств резервного хранения данных	
6.	Контрольная проверка работоспособности СКЗИ «КриптоПро CSP» и ПАК	Один раз в 6 месяцев	Проверку работоспособности средств обеспечения деятельности удостоверяющего центра необходимо выполнять путем выполнения тестовых задач, связанных с основной	

	«КриптоПро УЦ»		деятельностью удостоверяющего центра.	
7.	Восстановление работоспособности удостоверяющего центра	По мере необходимости	Осуществляется посредством восстановления или переустановки программных компонент удостоверяющего центра, а также восстановления образа всего диска	

В части технического обслуживания средств криптографической защиты информации и средств обеспечения деятельности КУЦ является организацией – лицензиатом ФСБ России, имеющей соответствующую лицензию на техническое обслуживание шифровальных (криптографических) средств. Сотрудники КУЦ привлекаемые к проведению данных работ, имеют документ (сертификат), подтверждающий прохождение обучения сотрудника на специализированных курсах.

10. Роли обслуживающего персонала средств обеспечения деятельности КУЦ

КУЦ осуществляет разделение ролей обслуживающего персонала средств обеспечения деятельности КУЦ. Каждая роль имеет свой набор задач, возможность осуществления которых задаётся параметрами безопасности, сопоставленными данной роли.

Перечень и описание обязанностей ролей, выполняемых обслуживающим персоналом КУЦ на сервере ЦС и на сервере ЦР приведён в таблицах ниже.

Ролевое администрирование сервера ЦС

Роли и группы	Разрешение безопасности	Описание
Администратор ЦС	Управление ЦС	Установка и разворачивание ЦС, формирование и уничтожение ключа ЭП и сертификатом ключа проверки ЭП ЦС (совместно с Администратором ЦС), управление ключом шифрования и сертификатом Веб-сервера ЦС, регистрация ЦР, архивирование и восстановление баз ЦР. Это роль операционной системы. Определяется членством в группе локальных администраторов операционной системы. Настройка и обслуживание ЦС, загрузка ключа ЭП ЦС. Это роль ЦС, которая включает в себя возможность назначать все остальные роли. Эта роль также называется КУЦ. Данные разрешения назначаются с помощью Диспетчера КУЦ.
Администратор безопасности ЦС	Управление аудитом и журналом безопасности	Настройка, просмотр и обслуживание журналов аудита. Аудит — это функциональная возможность операционной системы. Аудитор — это роль операционной системы.

Ролевое администрирование сервера ЦР

Роли и группы	Разрешение безопасности Сервера ЦР	Описание

	Администратор центра регистрации Чтение, Подача запросов, Одобрение запросов, Настройка параметров, Настройка безопасности	Установка и разворачивание ЦР, управление ключом ЭП и сертификатом ЦР, управление ключом шифрования и сертификатом Вебсервера ЦР, регистрация администраторов КУЦ, архивирование и восстановление баз ЦР. Это роль операционной системы. Определяется членством в группе локальных администраторов операционной системы. Это роль клиента ЦР, которая включает в себя возможность назначать все остальные роли ЦР и настраивать Центр регистрации. Данные разрешения назначаются с помощью Диспетчера КУЦ и Консоли управления ЦР. Администратор ЦР — это клиенты ЦР, которым разрешено регистрировать пользователей и запрашивать сертификаты в ЦС. Настраивается в Консоли Управления ЦР. Администратор ЦР отличается от Оператора ЦР возможностью создавать других Операторов ЦР и настраивать ЦР, в том числе параметры безопасности. Администраторы ЦР выполняют свои функции через Консоль управления ЦР.
Администратор безопасности ЦР	Управление аудитом и журналом безопасности	Настройка, просмотр и обслуживание журналов аудита. Аудит — это функциональная возможность операционной системы. Аудитор — это роль операционной системы.
Оператор ЦР	Чтение, Подача запросов, Одобрение запросов	Оператор ЦР — это клиенты ЦР, которым разрешено регистрировать пользователей и запрашивать сертификаты в ЦС. Операторы ЦР выполняют свои функции через Консоль управления ЦР.

11. Обеспечение безопасности

11.1. Инженерно-технические меры защиты информации

11.1.1. Размещение технических средств КУЦ

Сервера Центра сертификации, Центра регистрации и телекоммуникационное оборудование размещены в серверном помещении.

Сервера Центра сертификации, Центра регистрации и телекоммуникационное оборудование размещаются в шкафу-стойке.

Остальные технические средства КУЦ размещаются в рабочих помещения КУЦ по схеме организации рабочих мест персонала.

11.1.2. Физический доступ в помещения

Серверное помещение КУЦ оборудовано системой контроля доступа с идентификацией по карте. Серверное помещение оборудовано исполнительным устройством системы контроля доступа электромеханического типа.

Рабочие и служебные помещения КУЦ подключены к системе контроля доступа и оборудованы механическими замками

Идентификационные карты для доступа в помещения КУЦ, подключенные к системе

контроля доступа, выдаются сотрудникам КУЦ по распоряжению руководителя КУЦ.

Ключи механических замков рабочих помещений КУЦ выдаются сотрудникам КУЦ по распоряжению руководителя КУЦ на основании схемы организации рабочих мест персонала.

11.1.3. Электроснабжение и кондиционирование воздуха

Технические средства КУЦ подключены к общегородской сети электроснабжения.

Электрические сети и электрооборудование, используемые в КУЦ, отвечают требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

Сервера Центра сертификации и Центра регистрации, телекоммуникационное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу в течение не менее 1 часа после прекращения основного электроснабжения.

Технические средства, эксплуатируемые на рабочих местах сотрудников КУЦ, источниками бесперебойного питания не оборудуются.

Серверное помещение оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Служебные помещения КУЦ, используемые для архивного хранения документов на бумажных, магнитных и оптических носителях оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурновлажностного режима, вентиляции и очистки воздуха.

Рабочие и прочие служебные помещения КУЦ оборудованы средствами вентиляции и кондиционирования воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

11.1.4. Подверженность воздействию влаги

Защита серверов Центра сертификации и Центра регистрации и телекоммуникационного оборудования от воздействия влаги обеспечивается их размещением в шкафу-стойке (cabinet).

11.1.5. Предупреждение и защита от возгорания

Серверное помещение КУЦ оборудовано системой автоматического пожаротушения, пожарной сигнализации и дымоудаления.

Пожарная безопасность помещений КУЦ обеспечивается в соответствии с нормами и требованиями СНиП по классу Ф3.5, устанавливаемыми законодательством Российской Федерации.

11.1.6. Хранение документированной информации

Документальный фонд КУЦ, как фондообразователя, подлежит хранению в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

11.1.7. Уничтожение документированной информации

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками КУЦ, обеспечивающими документирование.

11.2. Программно-аппаратные меры защиты информации

11.2.1. Организация доступа к техническим средствам КУЦ

Доступ к техническим средствам КУЦ, размещённым в серверном помещении, осуществляется с использованием системы контроля доступа.

Идентификационные карты доступа в серверное помещение выдаются сотрудникам на основании приказа руководителя КУЦ.

Организация доступа к техническим средствам КУЦ, размещённых на рабочих местах сотрудников КУЦ, возлагается на сотрудников КУЦ, ответственных за эксплуатацию данных технических средств.

11.2.2. Организация доступа к программным средствам КУЦ

Сервера Центра сертификации и Центра регистрации оснащены сертифицированными программно-аппаратными комплексами защиты от несанкционированного доступа типа «Электронный замок».

Рабочие места сотрудников КУЦ, на которых эксплуатируются программные приложения «АРМ администратора ЦР» и «АРМ разбора конфликтных ситуаций» также оснащены сертифицированными программно-аппаратными комплексами защиты от несанкционированного доступа типа «Электронный замок».

Доступ системных администраторов общесистемного программного обеспечения серверов Центра сертификации и Центра регистрации для выполнения регламентных работ осуществляется в присутствии сотрудников КУЦ, отвечающих за эксплуатацию соответствующего прикладного программного обеспечения (Центра сертификации и/или Центра регистрации).

11.2.2.1. Общий перечень объектов доступа КУЦ

К объектам доступа КУЦ относятся:

- технические средства компонент КУЦ;
- программное обеспечение компонент КУЦ: ПО центра сертификации, ПО Центра регистрации, ПО АРМ администратора Центра регистрации, ПО АРМ разбора конфликтных ситуаций, ПО, предназначенное для регистрации и управления сертификатами пользователей КУЦ;
- базы данных компонент КУЦ: база данных ЦС, база данных ЦР;
- ключи ЭП и сертификаты ключей проверки ЭП;
- списки отозванных сертификатов КУЦ.

11.2.2.2. Перечень объектов доступа, предоставляемых сотрудникам КУЦ

Операторам КУЦ:

- технические средства АРМ администратора Центра регистрации;
- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- рабочие сертификаты ключей проверки ЭП пользователей КУЦ;
- ключи ЭП и сертификаты ключей проверки ЭП, использующиеся для эксплуатации Центра сертификации и Центра регистрации;
- списки отозванных сертификатов.

Администраторам КУЦ:

- списки отозванных сертификатов КУЦ.
- база данных Центра сертификации и Центра регистрации КУЦ;

- программное обеспечение Центра сертификации и Центра регистрации КУЦ;
- технические средства АРМ разбора конфликтных ситуаций;
- технические средства Центра сертификации и Центра регистрации КУЦ;
- технические средства АРМ администратора Центра регистрации;
- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- технические сертификаты ключей проверки ПАК КУЦ
- рабочие ключи и рабочие сертификаты ключей проверки ЭП пользователей КУЦ;
- списки отозванных сертификатов.
- технические средства компонент КУЦ;
- программное обеспечение компонент КУЦ;
- базы данных Центра сертификации и Центра регистрации.

11.2.3. Контроль целостности программного обеспечения

Контролю целостности подлежат следующие программные компоненты из состава программного обеспечения, эксплуатируемого КУЦ:

- Программные модули средств электронной подписи и криптографической защиты информации;
- Программные модули Комплекса программ Удостоверяющего центра.
- Состав программных модулей, подлежащих контролю целостности, определяется внутренним документом КУЦ, утверждаемый руководителем КУЦ.

Система контроля целостности программных модулей, подлежащих контролю целостности, основывается на аппаратном контроле целостности и общесистемного программного обеспечения до загрузки операционной системы.

Данная система контроля целостности обеспечивается использованием сертифицированного устройства типа «электронный замок».

Контроль целостности программных модулей средств электронной подписи и криптографической защиты информации осуществляется средствами средств электронной подписи и криптографической защиты информации.

Периодичность выполнения мероприятий по контролю целостности — ежесуточно.

11.2.4. Контроль целостности технических средств

Контроль целостности технических средств технических средств КУЦ обеспечивается опечатыванием корпусов устройств, препятствующим их неконтролируемому вскрытию.

Опечатывание устройств выполняется перед вводом технических средств в эксплуатацию и после выполнения регламентных работ.

Контроль целостности печатей осуществляется в начале каждой рабочей смены.

11.2.5. Защита внешних сетевых соединений

Защита конфиденциальной информации, передаваемой между программно-техническими средствами обеспечения деятельности КУЦ осуществляется путём шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных в соответствии с действующим законодательством Российской Федерации.

Защита программно-технических средств обеспечения деятельности КУЦ от

несанкционированного доступа по внешним сетевым соединениям осуществляется путем использования межсетевого экрана сертифицированного ФСБ России не ниже 4-го класса защиты.

При организации сетевого взаимодействия компонентов ПАК «КриптоПро УЦ 2.0» между собой в пределах одой контролируемой зоны используются шифровальные (криптографических) средства сертифицированные по классу КВ.

Технические средства аккредитованного удостоверяющего центра - Центр регистрации и Центр сертификации ПАК «КриптоПро УЦ 2.0» не подключены к техническим средствам общедоступных сетей связи, в том числе, сети Интернет.

11.2.5.1. Перечень информации, подлежащей защите

- Заявление на создание сертификата ключа проверки ЭП;
- Заявление на аннулирование (отзыв) сертификата ключа проверки ЭП;
- Ключевая фраза пользователя. Передаваемая из КУЦ информация:
- Бланк копии сертификата ключа проверки ЭП для вывода на бумажный носитель;
- Список сертификатов ключа проверки ЭП Пользователя КУЦ и их статус;
- Список запросов на сертификаты ключей проверки ЭП Пользователя КУЦ и их статус;
- Список запросов на аннулирование (отзыв) сертификатов ключей проверки ЭП Пользователя КУЦ и их статус.

11.3. Организационные меры защиты информации

11.3.1. Предъявляемые требования к персоналу КУЦ

Персонал КУЦ, производящий обслуживание КУЦ, имеет высшее профессиональное образование и профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области более 2 лет.

11.3.2. Организация доступа персонала к документам и документации

Доступ сотрудников КУЦ к документам и документации, составляющей документальный фонд организации, организован в соответствии с должностными инструкциями и функциональными обязанностями.

11.3.3. Охрана здания и помещений

КУЦ имеет собственную (привлекаемую) службу охраны здания и помещений, обеспечивающую:

- Обнаружение и задержание нарушителей, пытающихся проникнуть в здание (помещения) КУЦ;
- Сохранность материальных ценностей и документов;
- Предупреждение происшествий и ликвидацию их последствий.

11.4. Юридические меры защиты информации

КУЦ имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг.

Системы безопасности КУЦ и защиты информации созданы и поддерживаются на договорной основе с юридическими лицами, осуществляющими свою деятельность на основании лицензий, полученных в соответствии с действующим законодательством Российской Федерации.

Все меры по защите информации в КУЦ введены в действие приказами руководителя КУЦ.

Для обеспечения деятельности КУЦ использует средства электронной подписи и криптографической защиты информации, сертифицированные в соответствии с действующим законодательством Российской Федерации.

Исключительные имущественные права на информационные ресурсы КУЦ находятся в собственности КУЦ.

Пользователям КУЦ предоставляются неисключительные имущественные права на копии сертификатов и списков отозванных сертификатов, изготавливаемые КУЦ в объёме прав согласно разделу 3.2 настоящего Регламента.

12. Взаимодействие КУЦ с федеральными органами исполнительной власти в сфере использования электронной подписи

Для использования пользователями КУЦ квалифицированной электронной подписи и создания квалифицированных сертификатов ключей проверки ЭП КУЦ должен быть аккредитован Уполномоченным федеральным органом исполнительной власти в области применения электронной подписи (Статья 6, пункт 2, ФЗ №63-ФЗ «Об электронной подписи»).

Порядок и требования к аккредитации устанавливаются ФЗ №63-ФЗ «Об электронной подписи» (Статья 16) и Правилами аккредитации Удостоверяющих центров, устанавливаемых федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

Приложение №17 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю

Директор по информационным технологиям

АО «Гринатом»

_____ / А.Н. Киселёв /

М.П.

ПОРЯДОК

применения усиленной квалифицированной электронной подписи

Москва 2020 г.

Содержание

1. Назначение и область применения

1.1. Настоящий Порядок применения усиленной квалифицированной электронной подписи (далее - Порядок) разработан с целями установления порядка использования усиленной квалифицированной электронной подписи при осуществлении электронного документооборота между участниками электронного взаимодействия в соответствии с Федеральным законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 06.04.2011г. №63-ФЗ «Об электронной подписи», другими федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, регулирующими отношения, возникающими в сфере информации, информационных технологий и защиты информации.

1.2. Порядок определяет обязательные для использования правила при использовании квалифицированной электронной подписи при осуществлении электронного взаимодействия с помощью любой документной системы, интегрированной с Платформой доверенных сервисов Госкорпорации «Росатом».

1.3. Участник электронного взаимодействия, до начала использования квалифицированной электронной подписи, обязан ознакомиться с данным Порядком.

1.4. Соблюдение Порядка является обязательным для предприятий/ организаций, использующих автоматизированные информационные системы, в которых применяются сертификаты ключей проверки электронных подписей, создаваемые Корпоративным удостоверяющим центром Госкорпорации «Росатом».

1.5. Ответственным за актуализацию Порядка и контроль его исполнения в соответствии с требованиями Положения о системе регламентирующих документов Госкорпорации «Росатом» является директор Департамента по информационным технологиям АО «Гринатом».

1.6. Актуальная версия Порядка размещена по адресу: https://crypto.rosatom.ru.

2. Термины, сокращения и аббревиатуры

2.1. Термины и определения

Термин	Определение
Аннулированный сертификат ключа подписи	Сертификат ключа проверки электронной подписи, действие которого прекращено в связи с: • истечением срока его действия; • получением заявления от его владельца; • вступлением в силу решения суда, влекущего аннулирование сертификата; • прекращением деятельности Удостоверяющего центра без перехода его функций другим лицам; • аннулированием квалифицированного сертификата Удостоверяющим центром.
Владелец сертификата ключа проверки электронной подписи	Лицо, которому в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»,

	Регламентом УЦ создан сертификат ключа проверки электронной подписи.
Документная система	Корпоративная/локальная информационная система, интегрированная с Платформой доверенных сервисов Госкорпорации «Росатом», предоставляющая сервисы управления электронными документами с возможностью подписания квалифицированной/неквалифицированной электронной подписями посредством сервисов Платформы доверенных сервисов Госкорпорации «Росатом»
Квалифицированный сертификат ключа проверки электронной подписи	Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011г. №63-ФЗ «Об электронной подписи» 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, и являющийся в связи с этим официальным документом.
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.
Платформа доверенных сервисов Госкорпорации «Росатом»	Автоматизированная информационная система, предназначенная для комплексной автоматизации процессов управления ключами электронной подписи и сертификатами ключей проверки электронной подписи, предоставления сервисов удаленного подписания электронных документов, проверки электронной подписи, и сервисов управления средствами криптографической защиты информации
Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом»)	Основной руководящий документ УЦ, отражающий обязанности участников электронного взаимодействия и членов группы администраторов в части выдачи сертификата ключа проверки электронной подписи Пользователям, принятые форматы данных, а также основные организационно-технические мероприятия, необходимые для безопасного функционирования УЦ (опубликован на crypto.rosatom.ru).
Реестр удостоверяющего центра	Набор документов УЦ в электронной и/или бумажной форме, включающий следующую информацию: • реестр заявлений на регистрацию в УЦ; • реестр зарегистрированных участников электронного взаимодействия УЦ; • реестр заявок на изготовление сертификатов в УЦ; • реестр заявлений на изготовление сертификатов ключа проверки электронной подписи; • реестр заявлений на аннулирование (прекращение действия) сертификатов ключа проверки электронной подписи; • реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;

	• реестр сертификатов ключа проверки электронной подписи; • реестр изготовленных списков отозванных сертификатов ключей проверки электронной подписи.
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.
Служба актуальных статусов сертификатов	Веб-сервис Удостоверяющего центра, обеспечивающий информирование Пользователей Удостоверяющего центра о статусе сертификатов ключей проверки электронной подписи посредством реализации протокола OCSP.
Служба штампов времени	Веб-сервис Удостоверяющего центра, обеспечивающий предоставление доверенных меток времени посредством реализации протокола TSP для ПДС по запросам участникам электронного взаимодействия при работе в документных системах.
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.
Средство электронной подписи	Шифровальное (криптографическое) средство, 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	Акционерное общество «Гринатом» (АО «Гринатом»), осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».
Участник электронного взаимодействия	Лицо, зарегистрированное в УЦ АО «Гринатом» в установленном Регламентом Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом») порядке, персональные данные которого указаны в сертификате ключа проверки электронной подписи.
Штамп времени электронного документа	Электронный документ, подписанный электронной подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.
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.

Электронный документ	Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.
Cryptographic Message Syntax	Стандарт, определяющий формат и синтаксис криптографических сообщений.
Online Certificate Status Protocol	Протокол установления статуса сертификата открытого ключа, реализующий RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP».
Time-Stamp Protocol	Протокол получения штампа времени, реализующий RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».

В Порядке используются термины, установленные Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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

Термин	Определение
Сертификат	Квалифицированный сертификат ключа проверки электронной подписи
ПАК	Программно-аппаратный комплекс
ПДС	Платформа доверенных сервисов Госкорпорации «Росатом»
Регламент УЦ	Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом»)
Реестр УЦ	Реестр удостоверяющего центра
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр
ЭД	Электронный документ
ЭП	Электронная подпись
CMS	Cryptographic Message Syntax
CRL	Certificates Revocation List
OCSP	Online Certificate Status Protocol
TSP	Time-Stamp Protocol

3. Обязанности Участника электронного взаимодействия

3.1. Участник электронного взаимодействия обязан:

- следовать положениям настоящего Порядка;
- использовать ключи ЭП и соответствующие им Сертификаты для подписания/шифрования ЭД в документных системах;
- для формирования ЭП применять только действующий ключ ЭП и соответствующий ему Сертификат;
- обеспечить сохранность в тайне и защиту от несанкционированного доступа персональной аутентификационной информации для доступа к документной системе и личному ключу ЭП;

– при компрометации личной ключевой информации или аутентификационной информации немедленно прекратить ее использование, руководствоваться и соблюдать порядок выполнения действий, установленный Регламентом УЦ.

4. Удостоверяющий центр и сертификаты ключей проверки электронных подписей

4.1. Удостоверяющим центром, создающим Сертификаты для использования в документных системах, является аккредитованный Корпоративный удостоверяющий центр Госкорпорации «Росатом» (АО «Гринатом»).
4.2. Для применения в документных системах могут использоваться Сертификаты, созданные только Корпоративным удостоверяющим центром Госкорпорации «Росатом» (АО «Гринатом»).
4.3. Порядок создания, выдачи и прекращения действия Сертификатов определяется Регламентом УЦ.
4.4. Идентификационные данные, занесенные в поле «Субъект» («Subject Name») Сертификата идентифицируют Владельца сертификата ключа проверки электронной подписи и соответствуют идентификационным данным Владельца сертификата ключа проверки электронной подписи, зарегистрированным в реестре Удостоверяющего центра.
4.5. Для определения статуса Сертификата используется список отозванных сертификатов, издаваемый и публикуемый УЦ в порядке и с периодичностью, определяемыми УЦ.
4.6. Местом публикации списков отозванных сертификатов принимается адрес информационного ресурса, определенный в расширении «Точки распространения списков отзыва (CRL)» («CRL Distribution Point») (OID – 2.5.29.31) сертификата ключа подписи.
4.7. Для определения статуса Сертификата также может использоваться Служба актуальных статусов сертификатов (в том случае, если сервис указанной Службы предоставляется Удостоверяющим центром или ПДС) и единая система идентификации и аутентификации Российской Федерации.

5. Средства электронной подписи

5.1. В качестве средств ЭП, обеспечивающих реализацию функций создания и проверки ЭП с использованием ключа ЭП, должны использоваться средства ЭП, имеющие подтверждение соответствия требованиям, установленным в соответствии с требованиями законодательства Российской Федерации.
5.2. Использование средства ЭП должно осуществляться в соответствии с требованиями формуляра и эксплуатационной документации на данное средство ЭП.

6. Электронные документы, подписываемые электронной подписью

6.1. Участник электронного взаимодействия вправе ЭД подписывать ЭП.

6.2. ЭД, подписанные ЭП, признаются равнозначными документам, подписанным собственноручной подписью в случае выполнения всех условий равнозначности ЭД, подписанного ЭП, документу на бумажном носителе, подписанному собственноручной подписью.
6.3. ЭД и его ЭП в документной системе представляются в виде файлов. ЭП может быть как открепленной (в виде отдельного файла), так и прикрепленной. При этом открепленная ЭП представляется в виде криптографического сообщения, формат которого определяется RFC 3852 «Cryptographic Message Syntax (CMS)», с учетом использования криптографических алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94 в соответствии с RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».
6.4. Форматы ЭД определяются документной системой.

7. Порядок формирования и проверки электронной подписи

7.1. Формирование ЭП в ЭД осуществляется в ПДС с использованием средств ЭП.
7.2. Формирование ЭП может быть осуществлено только Владельцем сертификата ключа проверки электронной подписи, соответствующий ключ ЭП которого действует на момент формирования ЭП.
7.3. При формировании ЭП:
7.3.1. с использованием сервиса ЭП на базе «КриптоПро DSS», участник электронного взаимодействия должен подтвердить свое волеизъявление на подписание ЭД с использованием мобильного приложения «Модуль аутентификации DSS Client для ПАК "КриптоПро DSS». Перед подтверждением подлежащий подписанию ЭД должен быть полностью отображен Участнику электронного взаимодействия в интерфейсе документной системы, либо в мобильном приложении «Модуль аутентификации DSS Client для ПАК «КриптоПро DSS».
7.3.2. с использованием сертифицированного ФСБ России СКЗИ и отчуждаемого ключевого носителя с ключом ЭП, Участник электронного взаимодействия должен предъявить пин-код к ключевому контейнеру.
7.4. Допускается подписание одной ЭП нескольких ЭД одновременно (пакет документов) в случае таких возможностей документной системы.
7.5. ЭД может иметь несколько ЭП от нескольких различных Участников электронного взаимодействия.
7.6. При формировании ЭП в ЭД с помощью документной системы, фиксируется время подписания данного ЭД и информация о статусе Сертификата (OCSP) Владельца сертификата ключа проверки электронной подписи на момент подписания ЭД. При этом фиксация времени подписания ЭД осуществляется посредством получения метки доверенного времени (TSP).
7.7. Время, содержащееся в метке доверенного времени, полученное при подписании ЭП ЭД, признается временем подписания ЭД.

7.8. Полученная метка доверенного времени и информация о статусе Сертификата Участника электронного взаимодействия, а также иные данные, необходимые для установления статуса Сертификата на момент подписания ЭД при его хранении, обработке и передаче должны быть включены в состав криптографического сообщения и представлены в соответствии с форматом, установленным RFC 5126 «CMS Advanced Electronic Signatures (CAdES)».

7.9. Подтверждение подлинности ЭП в ЭД осуществляется с использованием сервиса по проверке Сертификатов «КриптоПро SVS», интегрируемой с ПДС и/или с использованием единой системы идентификации и аутентификации Российской Федерации.

8. Условия равнозначности электронного документа, подписанного квалифицированной электронной подписью, документу на бумажном носителе, подписанному собственноручной подписью

8.1. Информация в электронной форме, подписанная квалифицированной ЭП, признается ЭД, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

8.2. Достоверной информацией о моменте подписания ЭД признается время, содержащееся в доверенной метке времени, полученное при подписании ЭД с использованием применяемого средства ЭП, интегрируемого с ПДС.

9. Порядок разрешения конфликтных ситуаций, связанных с применением электронной подписи

Разрешение конфликтных ситуаций осуществляется в соответствии с Регламентом УЦ.

10. Нормативные ссылки

Федеральный закон от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

Приложение №18 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю

Директор по информационным технологиям

АО «Гринатом»

_____ / А.Н. Киселёв /

М.П.

ПОРЯДОК

применения усиленной неквалифицированной электронной подписи

Москва 2020 г.

Содержание

1. Назначение и область применения

1.1. Настоящий Порядок применения усиленной неквалифицированной электронной подписи (далее - Порядок) разработан с целями установления порядка использования усиленной неквалифицированной электронной подписи при осуществлении электронного документооборота между участниками электронного взаимодействия в соответствии с Федеральным законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 06.04.2011г. №63-ФЗ «Об электронной подписи», другими федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, регулирующими отношения, возникающими в сфере информации, информационных технологий и защиты информации.

1.2. Порядок определяет обязательные для использования правила при использовании неквалифицированной электронной подписи при осуществлении электронного взаимодействия с помощью любой документной системы, интегрированной с Платформой доверенных сервисов Госкорпорации «Росатом».

1.3. Участник электронного взаимодействия, до начала использования неквалифицированной электронной подписи, обязан ознакомиться с данным Порядком.

1.4. Соблюдение Порядка является обязательным для предприятий/ организаций, использующих автоматизированные информационные системы, в которых применяются сертификаты ключей проверки электронных подписей, создаваемые Корпоративным удостоверяющим центром Госкорпорации «Росатом».

1.5. Ответственным за актуализацию Порядка и контроль его исполнения в соответствии с требованиями Положения о системе регламентирующих документов Госкорпорации «Росатом» является директор Департамента по информационным технологиям АО «Гринатом».

1.6. Актуальная версия Порядка размещена по адресу: https://crypto.rosatom.ru.

2. Термины, сокращения и аббревиатуры

2.1. Термины и определения

Термин	Определение
Аннулированный сертификат ключа подписи	Сертификат ключа проверки электронной подписи, действие которого прекращено в связи с: • истечением срока его действия; • получением заявления от его владельца; • вступлением в силу решения суда, влекущего аннулирование сертификата; • прекращением деятельности Удостоверяющего центра без перехода его функций другим лицам; • аннулированием неквалифицированного сертификата Удостоверяющим центром.
Владелец сертификата ключа проверки электронной подписи	Лицо, которому в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»,

	Регламентом УЦ создан сертификат ключа проверки электронной подписи.
Документная система	Корпоративная/локальная информационная система, интегрированная с Платформой доверенных сервисов Госкорпорации «Росатом», предоставляющая сервисы управления электронными документами с возможностью подписания квалифицированной/неквалифицированной электронной подписями посредством сервисов Платформы доверенных сервисов Госкорпорации «Росатом»
Неквалифицированный сертификат ключа проверки электронной подписи	Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011г. №63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный неаккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом.
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.
Платформа доверенных сервисов Госкорпорации «Росатом»	Автоматизированная информационная система, предназначенная для комплексной автоматизации процессов управления ключами электронной подписи и сертификатами ключей проверки электронной подписи, предоставления сервисов удаленного подписания электронных документов, проверки электронной подписи, и сервисов управления средствами криптографической защиты информации
Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом»)	Основной руководящий документ УЦ, отражающий обязанности участников электронного взаимодействия и членов группы администраторов в части выдачи сертификата ключа проверки электронной подписи Пользователям, принятые форматы данных, а также основные организационно-технические мероприятия, необходимые для безопасного функционирования УЦ (опубликован на crypto.rosatom.ru).
Реестр удостоверяющего центра	Набор документов УЦ в электронной и/или бумажной форме, включающий следующую информацию: • реестр заявлений на регистрацию в УЦ; • реестр зарегистрированных участников электронного взаимодействия УЦ; • реестр заявок на изготовление сертификатов в УЦ; • реестр заявлений на изготовление сертификатов ключа проверки электронной подписи; • реестр заявлений на аннулирование (прекращение действия) сертификатов ключа проверки электронной подписи; • реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;

	• реестр сертификатов ключа проверки электронной подписи; • реестр изготовленных списков отозванных сертификатов ключей проверки электронной подписи.
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.
Служба актуальных статусов сертификатов	Веб-сервис Удостоверяющего центра, обеспечивающий информирование Пользователей Удостоверяющего центра о статусе сертификатов ключей проверки электронной подписи посредством реализации протокола OCSP.
Служба штампов времени	Веб-сервис Удостоверяющего центра, обеспечивающий предоставление доверенных меток времени посредством реализации протокола TSP для ПДС по запросам участникам электронного взаимодействия при работе в документных системах.
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.
Средство электронной подписи	Шифровальное (криптографическое) средство, 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	Акционерное общество «Гринатом» (АО «Гринатом»), осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».
Участник электронного взаимодействия	Лицо, зарегистрированное в УЦ АО «Гринатом» в установленном Регламентом Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом») порядке, персональные данные которого указаны в сертификате ключа проверки электронной подписи.
Штамп времени электронного документа	Электронный документ, подписанный электронной подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.
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.

Электронный документ	Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.
Cryptographic Message Syntax	Стандарт, определяющий формат и синтаксис криптографических сообщений.
Online Certificate Status Protocol	Протокол установления статуса сертификата открытого ключа, реализующий RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP».
Time-Stamp Protocol	Протокол получения штампа времени, реализующий RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».

В Порядке используются термины, установленные Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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

Термин	Определение
Сертификат	Неквалифицированный сертификат ключа проверки электронной подписи
ПАК	Программно-аппаратный комплекс
ПДС	Платформа доверенных сервисов Госкорпорации «Росатом»
Регламент УЦ	Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом»)
Реестр УЦ	Реестр удостоверяющего центра
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр
ЭД	Электронный документ
ЭП	Электронная подпись
CMS	Cryptographic Message Syntax
CRL	Certificates Revocation List
OCSP	Online Certificate Status Protocol
TSP	Time-Stamp Protocol

3. Обязанности Участника электронного взаимодействия

3.1. Участник электронного взаимодействия обязан:

- следовать положениям настоящего Порядка;
- использовать ключи ЭП и соответствующие им Сертификаты для подписания/шифрования ЭД в документных системах;
- для формирования ЭП применять только действующий ключ ЭП и соответствующий ему Сертификат;
- обеспечить сохранность в тайне и защиту от несанкционированного доступа персональной аутентификационной информации для доступа к документной системе и личному ключу ЭП;

- при компрометации личной ключевой информации или аутентификационной информации немедленно прекратить ее использование, руководствоваться и соблюдать порядок выполнения действий, установленный Регламентом УЦ.

4. Удостоверяющий центр и сертификаты ключей проверки электронных подписей

4.1. Удостоверяющим центром, создающим Сертификаты для использования в документных системах, является неаккредитованный УЦ.
4.2. Для применения в документных системах могут использоваться Сертификаты, созданные только УЦ.
4.3. Порядок создания, выдачи и прекращения действия Сертификатов определяется Регламентом УЦ.
4.4. Идентификационные данные, занесенные в поле «Субъект» («Subject Name») Сертификата идентифицируют Владельца сертификата ключа проверки электронной подписи и соответствуют идентификационным данным Владельца сертификата ключа проверки электронной подписи, зарегистрированным в реестре Удостоверяющего центра.
4.5. Для определения статуса Сертификата используется список отозванных сертификатов, издаваемый и публикуемый УЦ в порядке и с периодичностью, определяемыми УЦ.
4.6. Местом публикации списков отозванных сертификатов принимается адрес информационного ресурса, определенный в расширении «Точки распространения списков отзыва (CRL)» («CRL Distribution Point») (OID – 2.5.29.31) сертификата ключа подписи.
4.7. Для определения статуса Сертификата также может использоваться Служба актуальных статусов сертификатов (в том случае, если сервис указанной Службы предоставляется Удостоверяющим центром или ПДС).

5. Средства электронной подписи

5.1. В качестве средств ЭП, обеспечивающих реализацию функций создания и проверки ЭП с использованием ключа ЭП, должны использоваться средства ЭП, имеющие подтверждение соответствия требованиям, установленным в соответствии с требованиями законодательства Российской Федерации.
5.2. Использование средства ЭП должно осуществляться в соответствии с требованиями формуляра и эксплуатационной документации на данное средство ЭП.

6. Электронные документы, подписываемые электронной подписью

6.1. Участник электронного взаимодействия вправе ЭД подписывать ЭП.
6.2. ЭД, подписанные ЭП, признаются равнозначными документам, подписанным собственноручной подписью в случае выполнения всех условий равнозначности ЭД, подписанного ЭП, документу на бумажном носителе, подписанному собственноручной подписью.

6.3. ЭД и его ЭП в документной системе представляются в виде файлов. ЭП может быть как открепленной (в виде отдельного файла), так и прикрепленной. При этом открепленная ЭП представляется в виде криптографического сообщения, формат которого определяется RFC 3852 «Cryptographic Message Syntax (CMS)», с учетом использования криптографических алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94 в соответствии с RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».
6.4. Форматы ЭД определяются документной системой.

7. Порядок формирования и проверки электронной подписи

7.1. Формирование ЭП в ЭД осуществляется в ПДС с использованием средств ЭП.
7.2. Формирование ЭП может быть осуществлено только Владельцем сертификата ключа проверки электронной подписи, соответствующий ключ ЭП которого действует на момент формирования ЭП.
7.3. При формировании ЭП:
7.3.1. с использованием сервиса ЭП на базе «КриптоПро DSS», участник электронного взаимодействия должен подтвердить свое волеизъявление на подписание ЭД с использованием OTP-via-E-Mail, либо OTP-via-push.
7.3.2. с использованием сертифицированного ФСБ России СКЗИ и отчуждаемого ключевого носителя с ключом ЭП, Участник электронного взаимодействия должен предъявить пин-код к ключевому контейнеру.
7.4. Допускается подписание одной ЭП нескольких ЭД одновременно (пакет документов) в случае таких возможностей документной системы.
7.5. ЭД может иметь несколько ЭП от нескольких различных Участников электронного взаимодействия.
7.6. При формировании ЭП в ЭД с помощью документной системы, фиксируется время подписания данного ЭД и информация о статусе Сертификата (OCSP) Владельца сертификата ключа проверки электронной подписи на момент подписания ЭД. При этом фиксация времени подписания ЭД осуществляется посредством получения метки доверенного времени (TSP).
7.7. Время, содержащееся в метке доверенного времени, полученное при подписании ЭП ЭД, признается временем подписания ЭД.
7.8. Полученная метка доверенного времени и информация о статусе Сертификата Участника электронного взаимодействия, а также иные данные, необходимые для установления статуса Сертификата на момент подписания ЭД при его хранении, обработке и передаче должны быть включены в состав криптографического сообщения и представлены в соответствии с форматом, установленным RFC 5126 «CMS Advanced Electronic Signatures (CAdES)».
7.9. Подтверждение подлинности ЭП в ЭД осуществляется с использованием сервиса по проверке Сертификатов «КриптоПро SVS», интегрируемой с ПДС.

8. Условия равнозначности электронного документа, подписанного неквалифицированной электронной подписью, документу на бумажном носителе, подписанному собственноручной подписью

8.1. Информация в электронной форме, подписанная неквалифицированной электронной подписью, признается ЭД, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания ЭД, подписанных неквалифицированной ЭП, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи.
8.1.1 Шаблон Соглашения об использовании усиленной неквалифицированной электронной подписи размещен на crypto.rosatom.ru.
Порядок проверки неквалифицированной электронной подписи:

– проверка неквалифицированных ЭП предусмотрена только для неквалифицированных ЭП, выданных ПДС;

– для проверки ЭП Участник электронного взаимодействия через интерфейс документной системы отправляет запрос в ПДС на проверку ЭП в ЭД;

– сервис проверки ЭП в ПДС осуществляет проверку действительности подписи на момент ее формирования, основываясь на достоверной информации по метке времени и статусу сертификата ключа проверки электронной подписи в момент подписания. Сертификат, относящийся к ЭП, действителен на момент подписания и его серийный номер не содержится в актуальном на указанный момент времени списке отозванных сертификатов.

– сервис проверки ЭП в ПДС осуществляет проверку целостности (неизменности) ЭД на основании сравнения хеша полученного ЭД с хешем, сформированным при подписании;

– сервис проверки ЭП в ПДС направляет ответ, содержащий информацию о результатах проверки в документную систему для предъявления участнику информационного взаимодействия.

8.2. Достоверной информацией о моменте подписания ЭД признается время, содержащееся в доверенной метке времени, полученное при подписании ЭД с использованием применяемого средства ЭП, интегрируемого с ПДС.

9. Порядок разрешения конфликтных ситуаций, связанных с применением электронной подписи

Разрешение конфликтных ситуаций осуществляется в соответствии с Регламентом УЦ.

10. Нормативные ссылки

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

Федеральный закон от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».