

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ № 22/2143-Д-15

К ДОГОВОРУ ПРИСОЕДИНЕНИЯ

№ 22/2143-Д от 06 июля 2012 г.

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

г. Москва

«01» *сентября* 2019 года

В соответствии с пунктом 3.3.1 настоящего договора присоединения Исполнитель вносит изменения (дополнения), которые является 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 со 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 - <http://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.

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 к Договору.
- 4.3. Услуги оказываются в соответствии с Регламентами 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 СКЗИ конфиденциальной информации Заказчика и обеспечения ключевой документацией.
- 4.5. Заказчик вправе выбрать способ оказания услуг:
- без использования Информационной системы Органа криптографической защиты, Регламенты услуг (Приложения № 2,3,6,7),
 - с использованием Информационной системы органа криптографической защиты, Регламенты 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

- 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 Регламентами 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 средства криптографической защиты информации (далее – 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 Исполнителя 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 периода 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 расчётный 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 в праве 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 объеме.

- 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 Составы 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 23.09.2014 № 1/910-П-ДСП «Об утверждении отраслевых требований по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию, составляющую коммерческую тайну, служебную 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. Регламент процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

Приложение № 3. Регламент процесса «Предоставление услуг по организации и обеспечению безопасности с использованием СКЗИ информации ограниченного распространения, не содержащей сведения, составляющие государственную тайну

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

Приложение № 5. Печень и стоимость услуг Исполнителя

Приложение № 6. Положение об Органе криптографической защиты обладателя конфиденциальной информации.

Приложение № 7. Регламент процесса «Подключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «VipNet-Гринатом»

Приложение № 8. Регламент процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с использованием информационной системы Органа криптографической защиты»

Приложение № 9. 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 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.

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:

АО «Гринатом»

Заместитель директора по
информационным технологиям

(по доверенности № 22/300/2018-ДОВ от 27.12.2018)



**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 Регламенту Договора 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.

Заместитель директора по
информационным технологиям
АО «Гринатом»

С.Н. Данилов
(по дов. № 22/309/2018-ДОВ от 28.12.18)



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

У Т В Е Р Ж Д А Ю

Заместитель директора по
информационным технологиям

АО «Гринатом»

С.Н. Данилов

(по дов. № 22/309/2018-ДОВ от 28.12.18)



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

Редакция № 2.5

Москва 2019 г.

Содержание

1.	Назначение и область применения.....	4
2.	Термины, определения и сокращения.....	8
3.	Описание процесса.....	10
3.1	Цель процесса.....	10
3.2	Задачи процесса.....	10
3.4	Основные входы процесса.....	11
3.3	Основные выходы процесса.....	12
3.5	Описание подпроцессов.....	13
3.5.1	Подпроцесс «Предоставление информации в КУЦ».....	13
3.5.1.1	Процедура «Предоставление информации доверенным лицом».....	14
3.5.1.2	Процедура «Предоставление информации почтовым сообщением».....	14
3.5.1.3	Процедура «Предоставление информации при личной явке».....	16
3.5.1.4	Процедура «Предоставление информации по e-mail».....	17
3.5.1.5	Процедура «Предоставление информации по телефону».....	18
3.5.1.6	Процедура «Предоставление OCSP запроса».....	18
3.5.1.7	Процедура «Предоставление TSP запроса».....	19
3.5.1.8	Процедура «Предоставление официальной информации для принятия решения КУЦ».....	19
3.5.2	Подпроцесс «Создание сертификата».....	20
3.5.3	Подпроцесс «Аннулирование сертификата».....	21
3.5.4	Подпроцесс «Приостановление действия сертификата».....	22
3.5.5	Подпроцесс «Возобновление действия сертификата».....	23
3.5.6	Подпроцесс «Подтверждение получения сертификата».....	23
3.5.7	Подпроцесс «Подтверждение подлинности ЭП в ЭД».....	24
3.5.8	Подпроцесс «Предоставление сервиса OCSP».....	25
3.5.9	Подпроцесс «Предоставление сервиса TSP».....	26
3.5.10	Подпроцесс «Получение информации из КУЦ».....	26
3.5.10.1	Процедура «Получение информации при личной явке».....	27
3.5.10.2	Процедура «Получение информации почтовым сообщением».....	27
3.5.10.3	Процедура «Получение информации доверенным лицом».....	28
3.5.10.4	Процедура «Получение информации через службу Спецсвязи России».....	29

3.5.10.5 Процедура «Получение информации из списков отозванных сертификатов»	29
3.5.10.6 Процедура «Получение ответа OCSP сервиса»	30
3.5.10.7 Процедура «Получение ответа TSP сервиса»	30
3.5.10.8 Процедура «Получение информации из реестра КУЦ.	31
4. Нормативные ссылки	31
5. Порядок внесения изменений	31
6. Контроль и ответственность	32
6.1 Контроль выполнения требований Регламента	32
6.2 Ответственность работников за несоблюдение требований Регламента ..	33
7. Перечень приложений	33

1. Назначение и область применения

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

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

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

Руководитель предприятия/организации;

Пользователь КУЦ;

Доверенное лицо;

Оператор КУЦ;

Администратор КУЦ;

Комиссия КУЦ;

Руководитель КУЦ.

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

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

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

<p>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)</p>			
<p>Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»</p>	<p>Действует</p>	<p>Федеральный закон</p>	<p>Данилов С.Н</p>
<p>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»</p>	<p>Действует</p>	<p>Приказ</p>	<p>Данилов С.Н</p>
<p>Приказ ФСБ РФ от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи"</p>	<p>Действует</p>	<p>Приказ</p>	<p>Данилов С.Н</p>

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

и является основой при регламентации следующих подпроцессов и процедур:

Подпроцессы:	
1.	Предоставление информации в КУЦ

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

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;
- приостановления и возобновления действия сертификатов, выданных КУЦ;
- выдачи по обращению заявителя средств ЭП, содержащих ключи ЭП и ключи проверки ЭП, созданные КУЦ;
- ведения реестра выданных и аннулированных сертификатов (далее - реестр сертификатов), в том числе включающего в себя информацию, содержащуюся в сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов и об основаниях таких прекращения или аннулирования;
- создания по обращениям заявителей ключей ЭП и ключей проверки ЭП;
- проверки уникальности ключей проверки ЭП в реестре сертификатов;

- осуществления по обращениям участников электронного взаимодействия проверки ЭП;
- информирования в письменной форме заявителей об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки;
- обеспечения актуальности информации, содержащейся в реестре сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- предоставления безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информации, содержащейся в реестре сертификатов, в том числе информации об аннулировании сертификатов ключей проверки ЭП;
- обеспечения конфиденциальности созданных КУЦ ключей ЭП;
- осуществления иной, связанной с использованием ЭП деятельности.

3.4 Основные входы процесса

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

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

3.3 Основные выходы процесса

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления
1.	Ключевой носитель с ключом электронной подписи и сертификатом, Конверт с пин-кодом и парольной фразой и руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.	Пользователь КУЦ	Организация
2.	Копия сертификата ключа проверки электронной подписи на бумажном носителе	Пользователь КУЦ Оператор КУЦ	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления
3.	Список отозванных сертификатов (СОС)	Все	Организация
4.	Заключение о подтверждении подлинности	Заявителю	Организация
5.	OCSP ответ	Заявителю	Организация
6.	TSP ответ	Заявителю	Организация

3.5 Описание подпроцессов

3.5.1 Подпроцесс «Предоставление информации в КУЦ»

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

Пользователь КУЦ предоставляет информацию в КУЦ в виде:

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

Пользователь КУЦ предоставляет информацию в КУЦ посредством выполнения процедур:

- предоставления информации по e-mail;
- предоставления информации доверенным лицом;
- предоставления информации почтовым сообщением;
- предоставления информации при личной явке;
- предоставления информации по телефону;
- предоставления OCSP запроса;

- предоставления TSP запроса;
- предоставления официальной информации для принятия решения КУЦ.

3.5.1.1 Процедура «Предоставление информации доверенным лицом»

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

- Заявление на создание квалифицированного сертификата ключа проверки электронной подписи (Приложение №4), заполненное в соответствии с Правилами заполнения заявлений на создание сертификатов ключей проверки электронной подписи (Приложение №5);
- документ, подтверждающий полномочия Пользователя КУЦ в системе либо доверенность полномочного представителя юридического лица, наделённого правом использования ЭП (Приложение №6);
- доверенность доверенного лица, наделённого правом получения ключевого носителя и сертификата ключа проверки электронной подписи (Приложение №7);
- основной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования заявителя (в случае необходимости включения в сертификат поля СНИЛС).

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

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

3.5.1.2 Процедура «Предоставление информации почтовым сообщением»

Пользователь КУЦ подготавливает и отправляет в адрес КУЦ информацию для:

- создания сертификата;

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

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

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

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

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

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

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

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

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

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

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

3.5.1.3 Процедура «Предоставление информации при личной явке»

Пользователь КУЦ прибывает в КУЦ для:

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

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

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

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

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

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

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

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

Оператор КУЦ рассматривает предоставленные документы на правильность и полноту и переходит к предоставлению услуги, либо, в случае если документы заполнены неверно, сообщает об этом Руководителю КУЦ, который принимает решение об отказе в принятии документов.

3.5.1.4 Процедура «Предоставление информации по e-mail»

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

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

Официальный E-mail КУЦ: ca@rosatom.ru

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

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

В случае поступления в КУЦ сообщения e-mail, не содержащего скан-копию сертификата или содержащего иную информацию, обработка данных

сообщений производится Руководителем КУЦ по правилам обработки сообщений электронной почты.

3.5.1.5 Процедура «Предоставление информации по телефону»

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

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

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

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

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

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

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

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

3.5.1.6 Процедура «Предоставление OCSP запроса»

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

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».

3.5.1.7 Процедура «Предоставление TSP запроса»

Пользователь КУЦ осуществляет обращение к службе штампов времени КУЦ для получения штампов времени посредством реализации протокола получения штампа времени TSP (Time-Stamp Protocol), реализующего RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».

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».

3.5.1.8 Процедура «Предоставление официальной информации для принятия решения КУЦ»

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

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

КУЦ вправе приостановить действие сертификата Пользователя КУЦ в случаях компрометации или подозрения на компрометацию ключа ЭП Пользователя КУЦ в том случае, если Пользователю КУЦ не было известно о возможном факте компрометации ключей, а также в случаях неисполнения обязательств Пользователя КУЦ по Договору присоединения. После

приостановления действия сертификата Оператор КУЦ сообщает Пользователю КУЦ о наступлении события, повлекшего приостановление действия сертификата, и уведомляет его о том, что действие сертификата Пользователя КУЦ приостановлено.

3.5.2 Подпроцесс «Создание сертификата»

Подпроцесс «Создание сертификата» регламентирует создание сертификатов КУЦ.

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

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

Оператор КУЦ осуществляет проверку достоверности документов и сведений, представленных Пользователем КУЦ. Оператор КУЦ запрашивает и получает из государственных информационных ресурсов:

- 1) выписку из единого государственного реестра юридических лиц в отношении заявителя - юридического лица;
- 2) выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя - индивидуального предпринимателя;
- 3) выписку из Единого государственного реестра налогоплательщиков в отношении заявителя - иностранной организации.

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

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

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

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

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

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

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

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

Руководитель КУЦ осуществляет планирование, контроль показателей и управление подпроцессом.

3.5.3 Подпроцесс «Аннулирование сертификата».

Подпроцесс «Аннулирование сертификата» регламентирует аннулирование сертификатов КУЦ.

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

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

КУЦ аннулирует сертификат Пользователя КУЦ в следующих случаях:

- по Заявлению на аннулирование сертификата ключа проверки электронной подписи Пользователя КУЦ.
- по заявлению Руководителя предприятия/организации Пользователя КУЦ в случае отзыва доверенности Пользователя КУЦ или изменении его полномочий;
- по истечении срока, на который действие сертификата было приостановлено, аннулирование производится автоматически;
- в случае прекращения действия Договора;

- в случае, если не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- в случае, если установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- в случае, если вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.
- при компрометации ключа ЭП Уполномоченного лица КУЦ. Временем аннулирования сертификата Пользователя КУЦ признается время компрометации ключа Уполномоченного лица КУЦ, фиксирующееся в реестре КУЦ.

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

3.5.4 Подпроцесс «Приостановление действия сертификата»

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

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

КУЦ приостанавливает действие сертификата Пользователя КУЦ в следующих случаях:

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

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

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

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

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

3.5.5 Подпроцесс «Возобновление действия сертификата».

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

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

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

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

3.5.6 Подпроцесс «Подтверждение получения сертификата»

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

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

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

Оператор КУЦ при получении бумажной копии сертификата, подписанной Пользователем КУЦ, сверяет полученные данные с данными из реестра КУЦ. В случае если данные в бумажной копии сертификата верны,

Оператор КУЦ сохраняет её в архиве КУЦ и переходит к подпроцессу «Возобновление действия сертификата».

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

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

3.5.7 Подпроцесс «Подтверждение подлинности ЭП в ЭД»

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

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

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

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

Заявление должно содержать следующую информацию:

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

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

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

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

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

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

Заключение содержит:

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

Отчет по выполненной проверке содержит:

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

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

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

3.5.8 Подпроцесс «Предоставление сервиса OCSP».

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

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

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

3.5.9 Подпроцесс «Предоставление сервиса TSP».

Данный подпроцесс регламентирует порядок предоставления штампов времени по протоколу TSP.

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

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

3.5.10 Подпроцесс «Получение информации из КУЦ»

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

Пользователь КУЦ получает информацию из КУЦ в виде:

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

Пользователь КУЦ получает информацию из КУЦ посредством выполнения процедур:

- получения информации при личной явке;
- получения информации почтовым сообщением;
- получения информации через доверенное лицо;
- получения информации через службу Спецсвязи России;
- получения информации из списков отозванных сертификатов;

- получения ответа на OCSP запрос;
- получения ответа на TSP запрос.

3.5.10.1 Процедура «Получение информации при личной явке»

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

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

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

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

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

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

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

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

3.5.10.2 Процедура «Получение информации почтовым сообщением»

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

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

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

Второй экземпляр Заключения Удостоверяющего центра о подтверждении подлинности электронной подписи в электронном документе и Заявление о подтверждении подлинности электронной подписи в электронном документе Оператор КУЦ сохраняет в архиве КУЦ.

3.5.10.3 Процедура «Получение информации доверенным лицом»

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

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

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

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

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

Доверенное лицо передаёт Пользователю КУЦ комплект документов.

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

3.5.10.4 Процедура «Получение информации через службу Спецсвязи России»

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

Входящая информация поступает из подпроцесса «Создание сертификата».

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

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

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

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

3.5.10.5 Процедура «Получение информации из списков отозванных сертификатов»

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

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

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

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

списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов.

Период публикации СОС составляет 12 (двенадцать) часов.

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

3.5.10.6 Процедура «Получение ответа OCSP сервиса»

Входящая информация поступает из подпроцесса «Предоставление сервиса OCSP».

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

OCSP-ответ признается действительным при одновременном выполнении следующих условий:

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

3.5.10.7 Процедура «Получение ответа TSP сервиса»

Входящая информация поступает из подпроцесса «Предоставление сервиса TSP».

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

Служба штампов времени по запросам Пользователей КУЦ формирует и предоставляет Пользователям КУЦ штампы времени. Штамп времени,

относящийся к подписанному ЭП ЭД, признается действительным при одновременном выполнении следующих условий:

- подтверждена подлинность ЭП Службы штампов времени (Оператора Службы штампов времени) в штампе времени;
- сертификат Службы штампов времени (Оператора Службы штампов времени) на момент подтверждения подлинности ЭП штампа времени действителен;
- ключ ЭП Службы штампов времени (Оператора Службы штампов времени) на момент формирования штампа времени действителен;
- сертификат Службы штампов времени (Оператора Службы штампов времени) содержит в расширении Extended Key Usage область использования – Установка штампа времени (1.3.6.1.5.5.7.3.8);

3.5.10.8 Процедура «Получение информации из реестра КУЦ».

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

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

Ответственным за предоставление информации из реестра сертификатов является Администратор КУЦ.

4. Нормативные ссылки

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

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

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

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

5. Порядок внесения изменений

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

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

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

6. Контроль и ответственность

6.1 Контроль выполнения требований Регламента

Пользователь КУЦ несёт ответственность за:

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

Доверенное лицо несёт ответственность за:

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

Оператор КУЦ несёт ответственность за:

- идентификацию и аутентификацию Пользователя КУЦ (Доверенного лица) – проверку представленных документов;
- формирование комплекта документов, выдаваемых КУЦ;
- выдачу Пользователю (Доверенному лицу) комплекта документов (две копии сертификата на бумажном носителе, ключа и сертификата на ключевом носителе, конверта с парольной фразой и пин-кодом, руководства по обеспечению безопасности ЭП, заключения КУЦ подлинности ЭП в ЭД);

- отправку комплекта документов заказным письмом (заключение КУЦ подлинности ЭП в ЭД), сохранение одного экземпляра в архиве КУЦ;
- передачу комплекта документов (две копии сертификата на бумажном носителе, ключа и сертификата на ключевом носителе, конверта с парольной фразой и пин-кодом, руководства по обеспечению безопасности ЭП) сотруднику службы Спецсвязи России и запись в журнале отправки писем;
- за правильность выполнения подпроцессов в соответствии с инструкцией Оператора;
- за конфиденциальность ключей ЭП.

Администратор КУЦ несёт ответственность за:

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

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

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

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

6.2 Ответственность работников за несоблюдение требований Регламента

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

7. Перечень приложений

Приложение №1 Матрица ответственности.

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

Приложение №3 Дополнительные выходы и дополнительные входы.

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

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

Приложение №6 Форма доверенности пользователя Удостоверяющего центра

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

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

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

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

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

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

Приложение №13 Формат сертификата ключа проверки электронной подписи.

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

Приложение №15 Ограничения использования сертификатов ключа проверки электронной подписи.

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

Матрица ответственности

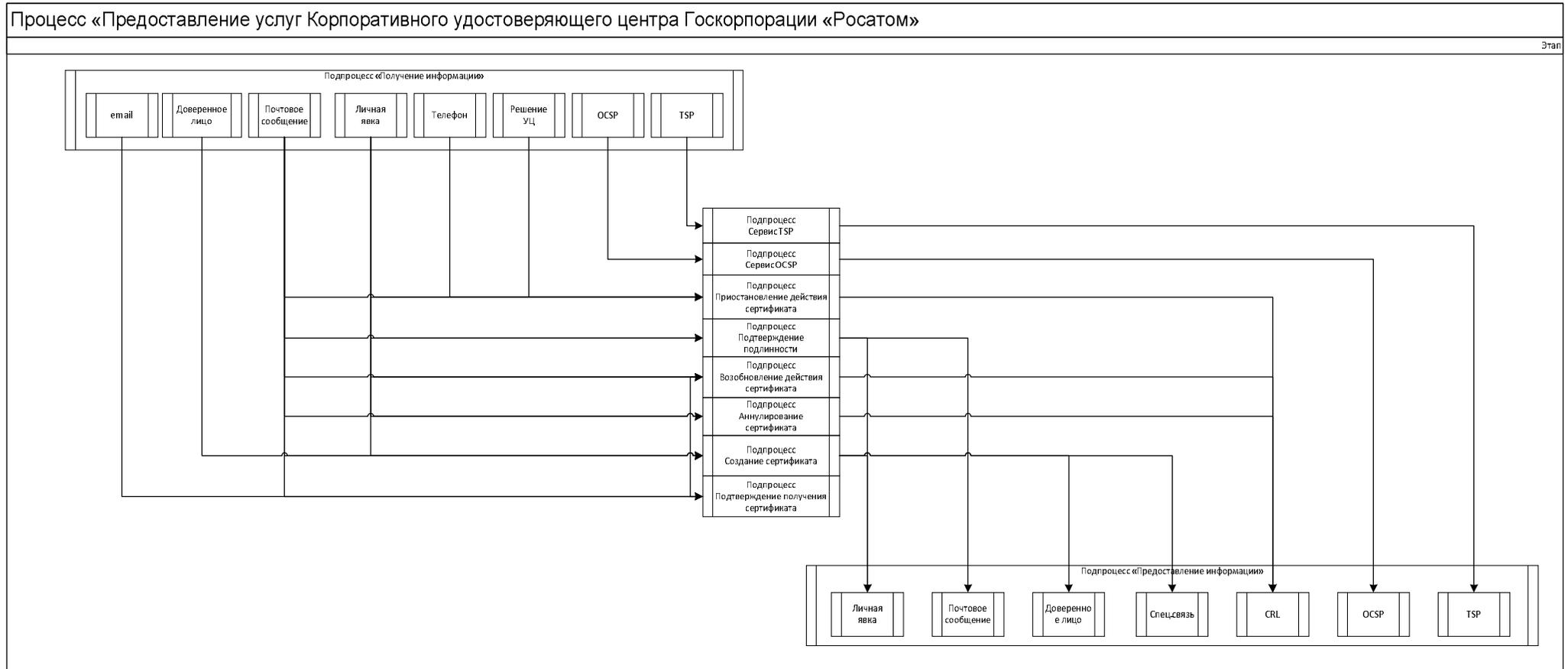
Подпроцессы в составе процесса	Участники процесса					
	Руководитель предприятия/ организации	Пользователь КУЦ	Доверенное лицо	Оператор КУЦ	Администратор КУЦ	Руководитель КУЦ
1. Подпроцесс «Предоставление информации в КУЦ»	О	О		Инф	К	К
1.1. Процедура «Предоставление информации по e-mail»		О		Инф	К	К
1.2. Процедура «Предоставление информации доверенным лицом»		О	О	Инф	К	К
1.3. Процедура «Предоставление информации почтовым сообщением»		О		Инф	К	К
1.4. Процедура «Предоставление информации при личной явке»		О		Инф	К	К
1.5. Процедура «Предоставление информации по телефону»		О		Инф		К
1.6. Процедура «Предоставление информации по решению КУЦ»		О		Инф	К	О
1.7. Процедура «Предоставление информации ОССП»					О	К
1.8. Процедура «Предоставление информации ТСП»					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 Спецсвязью России»		Инф		О	К	
2.5. Процедура «Получение информации CRL»		Инф			О	К
2.6. Процедура «Получение информации OCSP»		Инф			О	К
2.7. Процедура «Получение информации TSP»		Инф			О	К
3. Подпроцесс «Подтверждение получения сертификата ключа проверки электронной подписи»		О		Инф	К	К
4. Подпроцесс «Создание сертификата ключа проверки электронной подписи»				О	К	К
5. Подпроцесс «Аннулирование сертификата ключа проверки электронной подписи»				О	К	К
6. Подпроцесс «Возобновление действия сертификата ключа проверки электронной подписи»				О	К	К
7. Подпроцесс «Подтверждение подлинности ключа проверки электронной подписи»				О	О	К
8. Подпроцесс «Приостановление действия сертификата ключа проверки электронной подписи»				О	К	К
9. Подпроцесс «Сервис OCSP»					О	К
10. Подпроцесс «Сервис TSP»					О	К

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

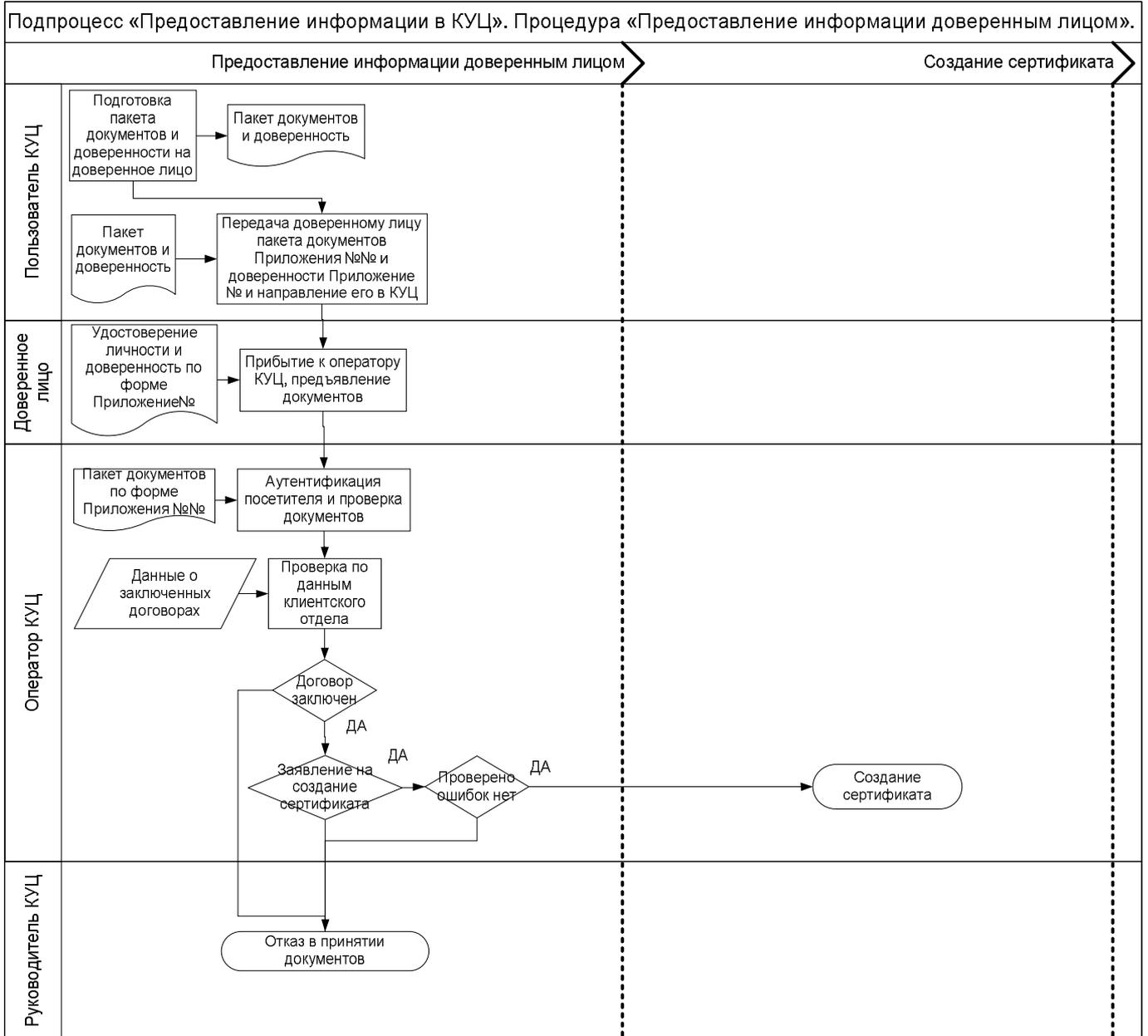
Сокращение	Название роли	Определение	Исполнитель Роли
М	Методолог	Формирует требования к организации деятельности в рамках подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/Организации
И	Интегратор	Интегрирует результаты подпроцесса/процедуры и отвечает за организацию подпроцесса/процедуры, 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

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

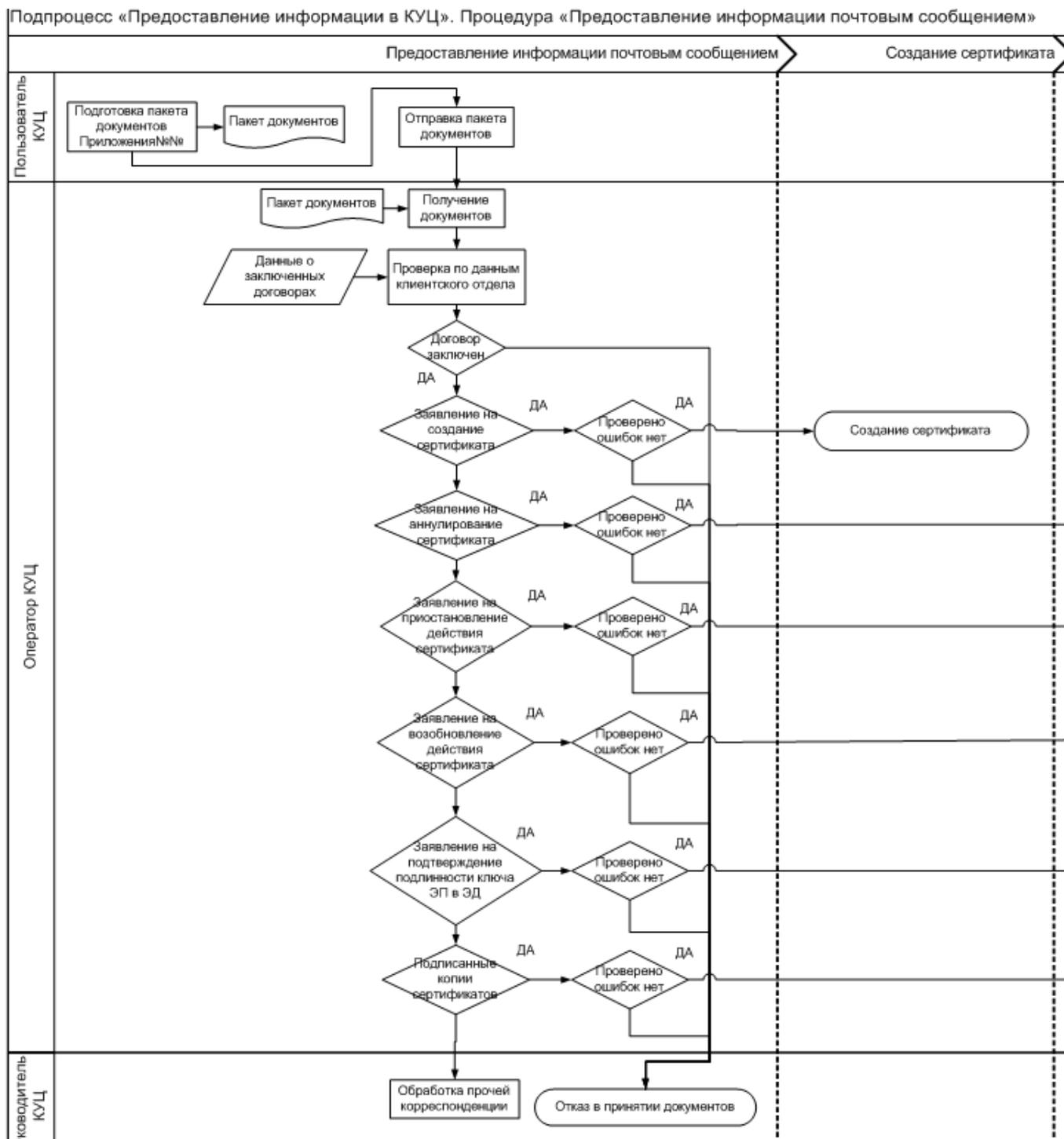


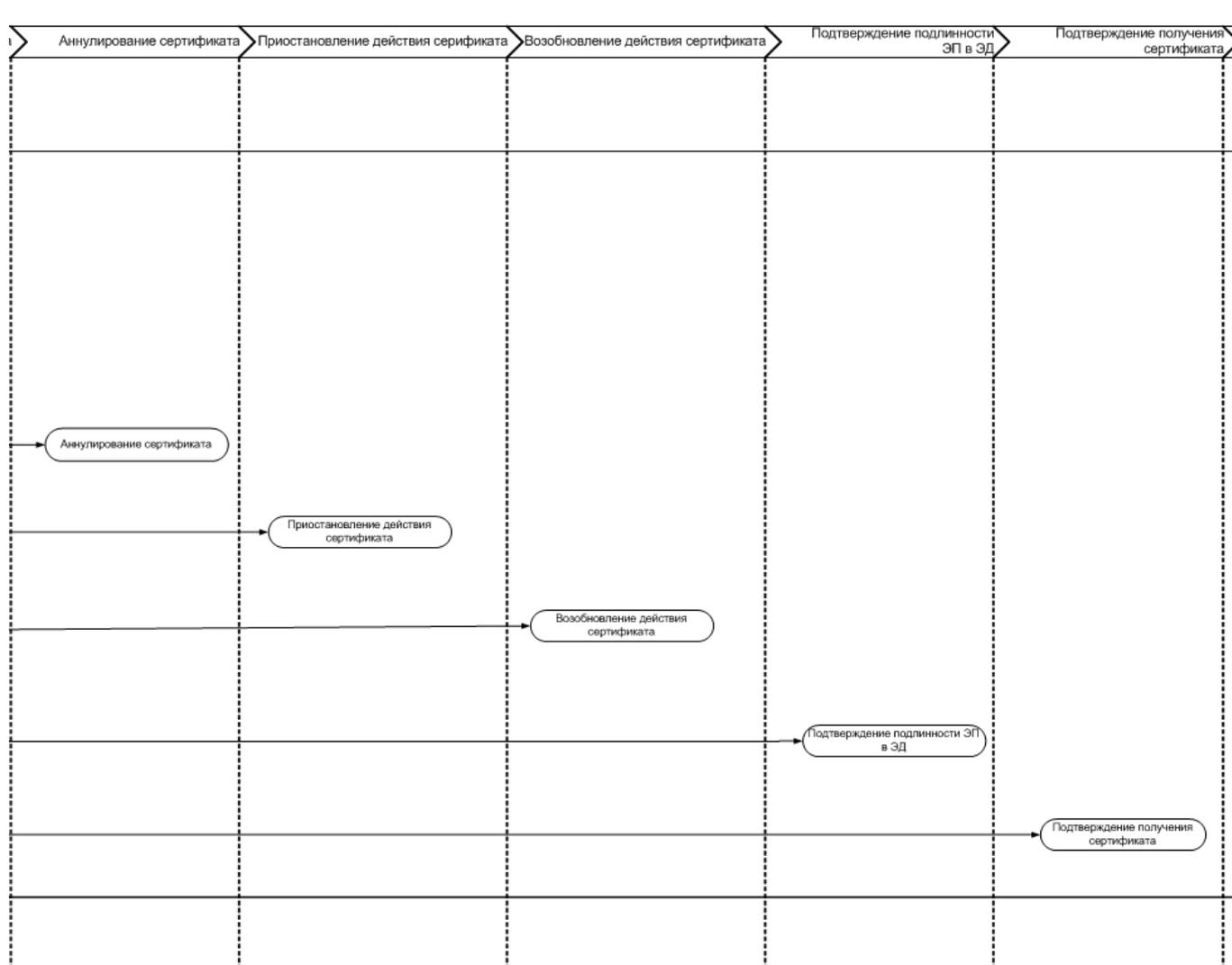
1. Подпроцесс «Предоставление информации в КУЦ»:

а) Схема процедуры «Предоставление информации доверенным лицом»:

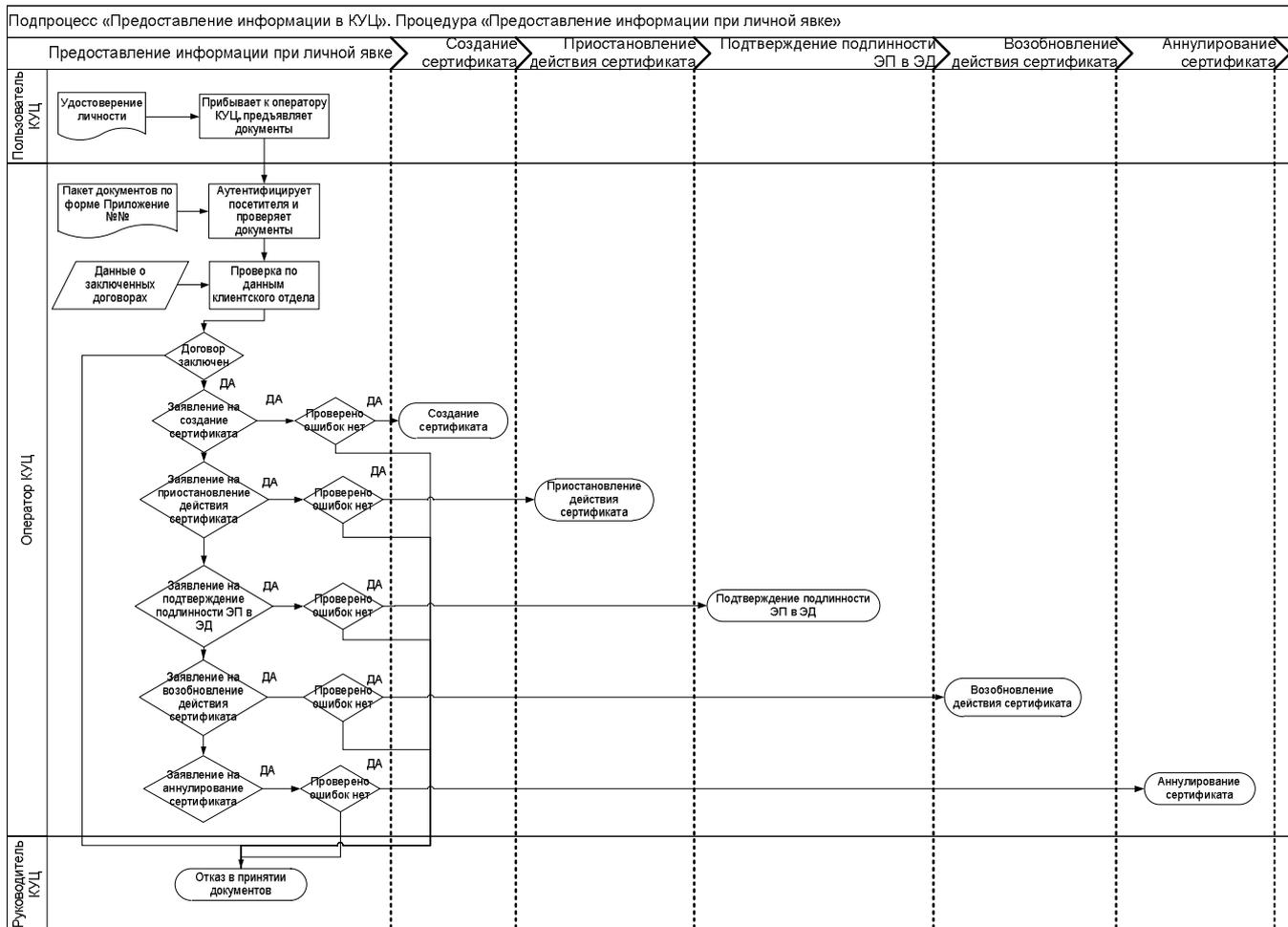


б) Схема процедуры «Предоставление информации почтовым сообщением»:

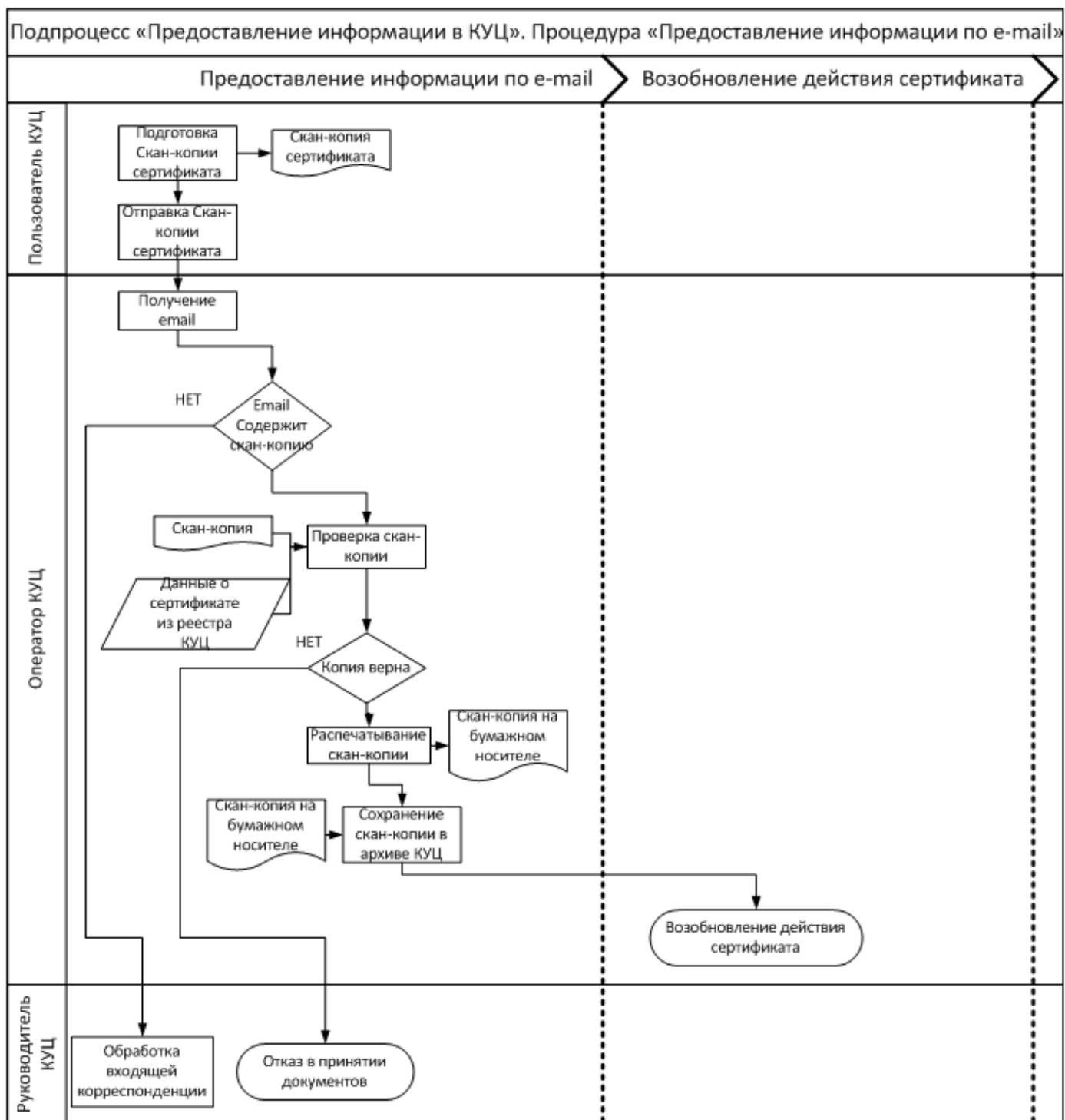




с) Схема процедуры «Предоставление информации при личной явке»:



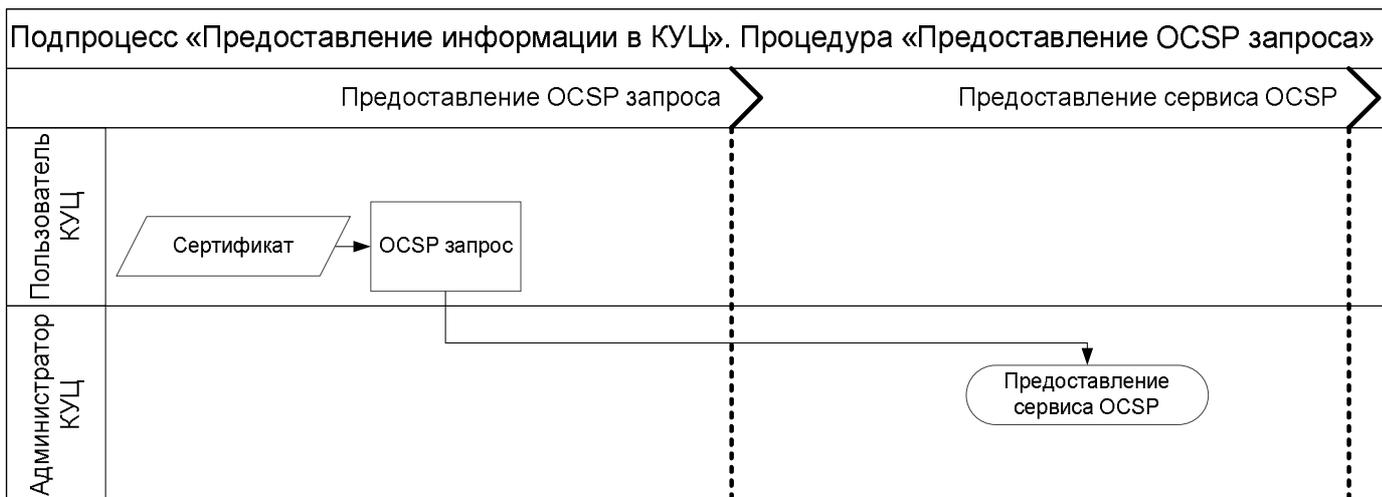
d) Схема процедуры «Предоставление информации по e-mail»:



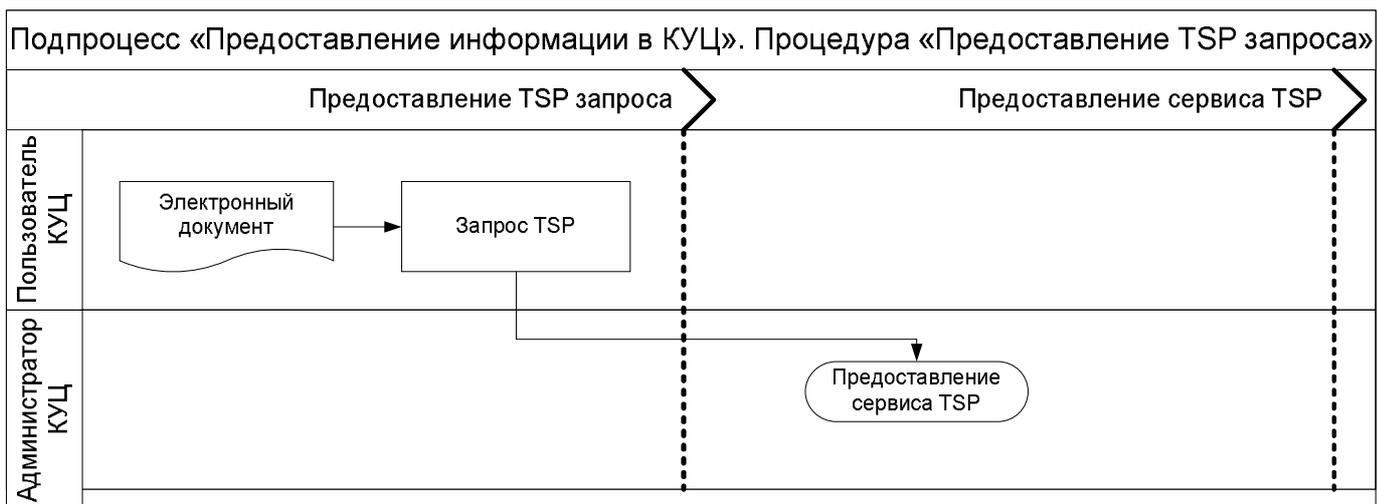
е) Схема процедуры «Предоставление информации по телефону»:



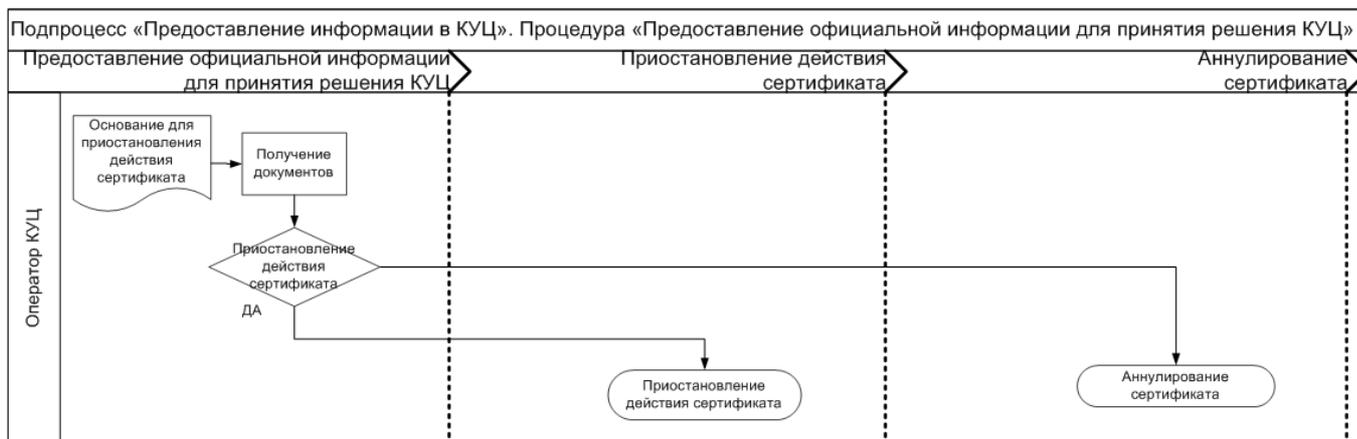
f) Схема процедуры «Предоставление OCSP запроса»:



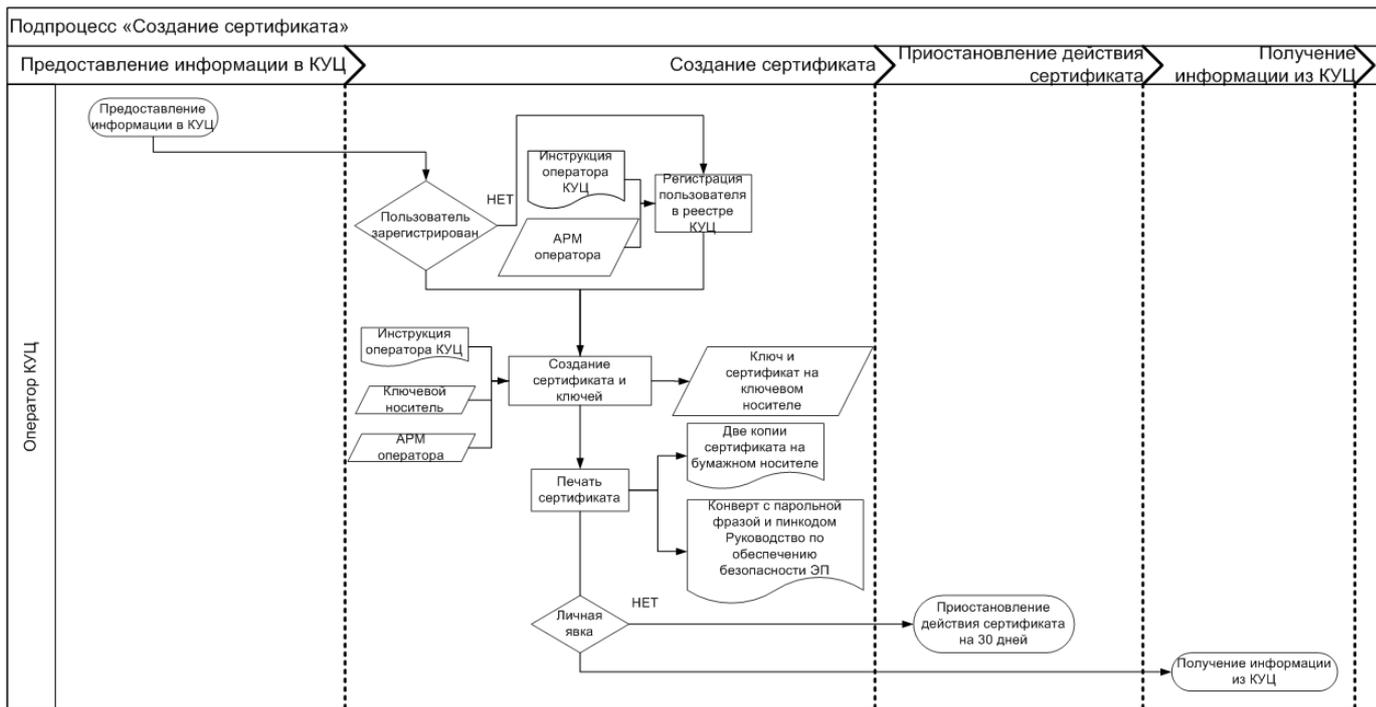
g) Схема процедуры «Предоставление TSP запроса»:



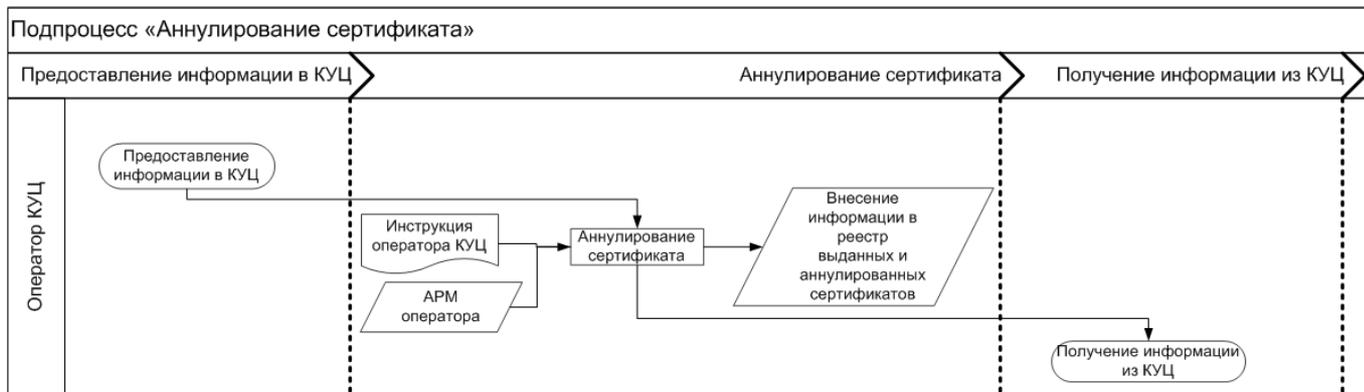
h) Схема процедуры «Предоставление официальной информации для принятия решения КУЦ»:



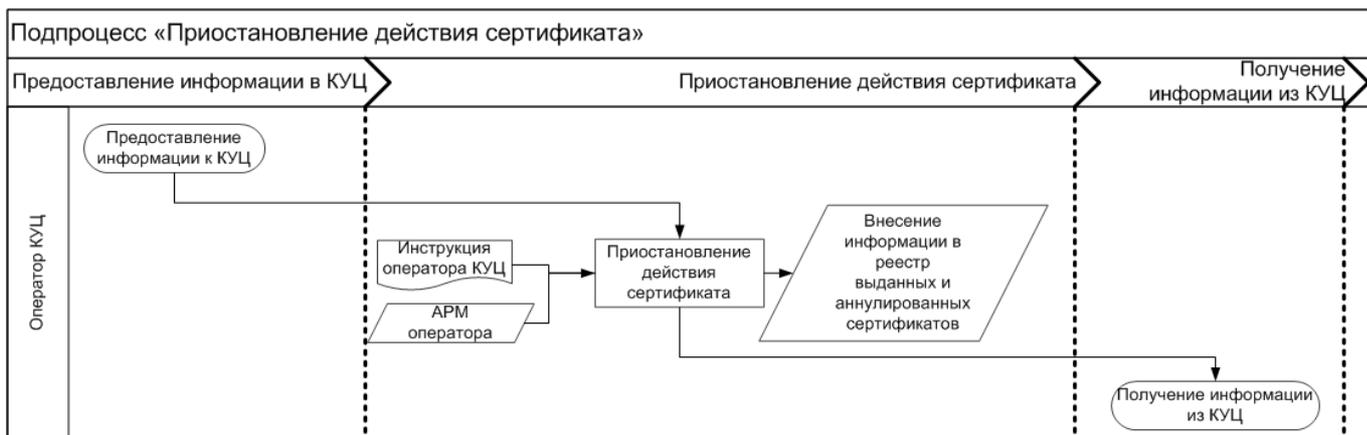
2. Схема подпроцесса «Создание сертификата»:



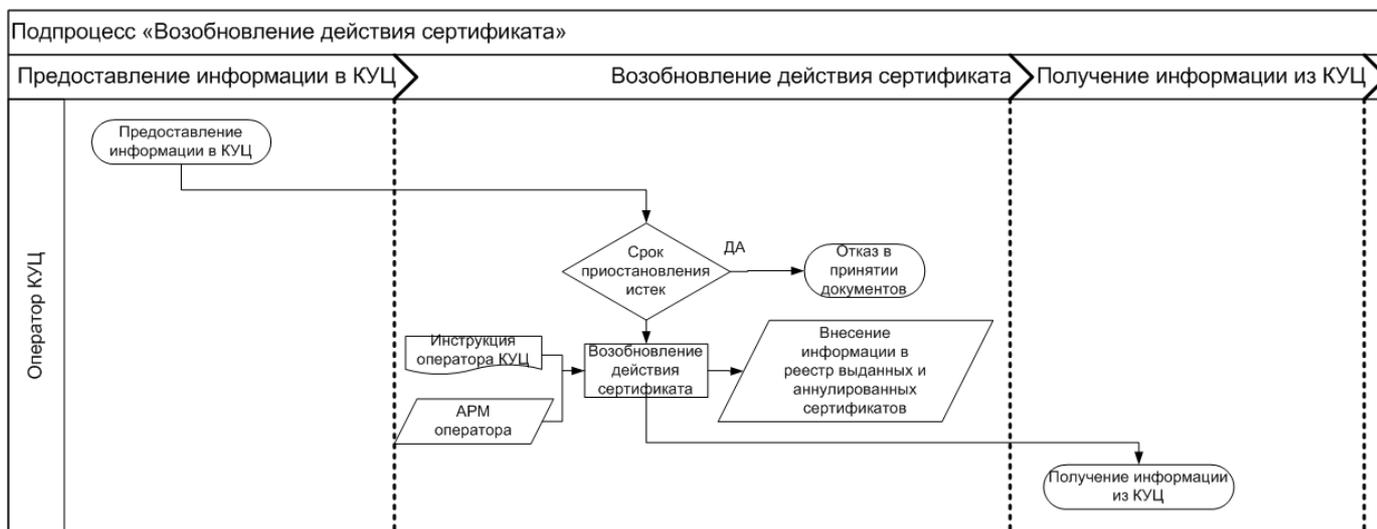
3. Схема подпроцесса «Аннулирование сертификата»:



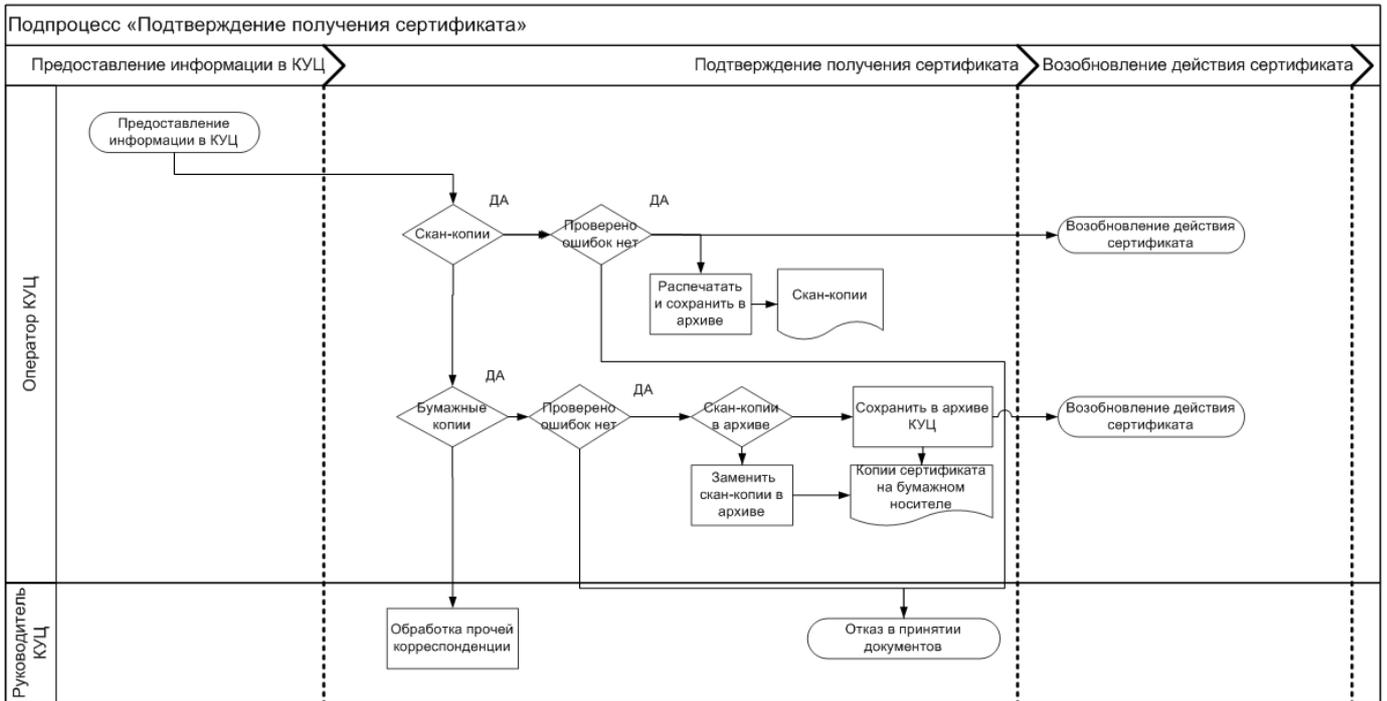
4. Схема подпроцесса «Приостановление действия сертификата»:



5. Схема подпроцесса «Возобновление действия сертификата»:



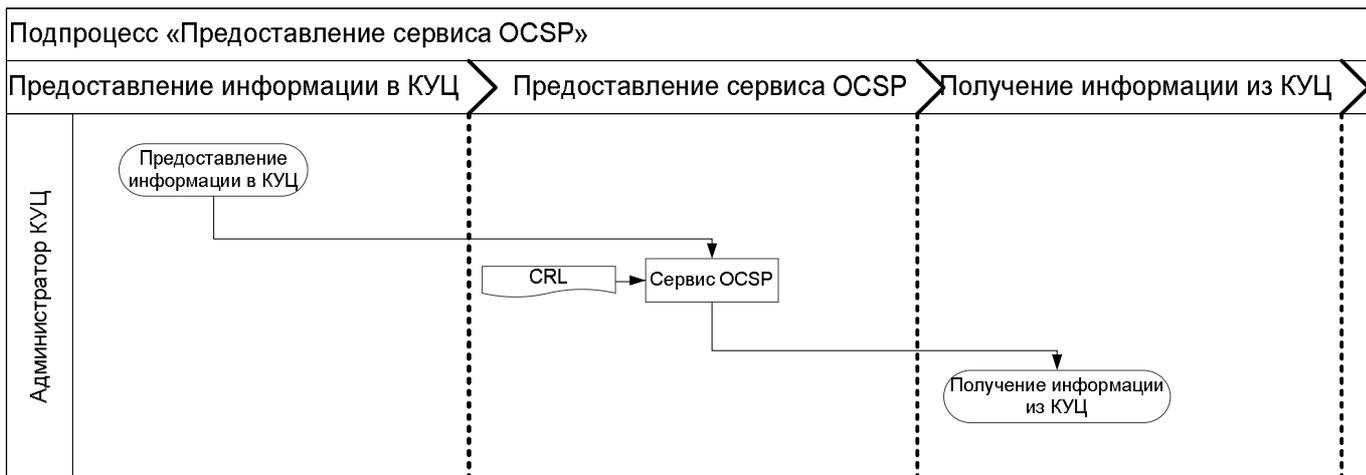
6. Схема подпроцесса «Подтверждение получения сертификата»:



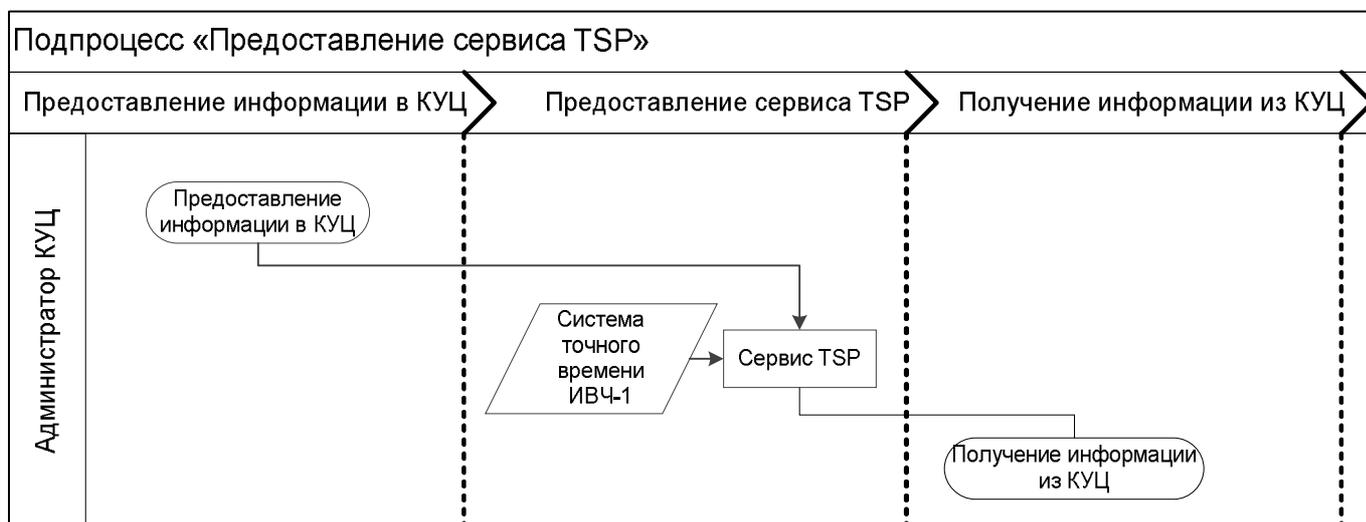
7. Схема подпроцесса «Подтверждение подлинности ЭП в ЭД»:



8. Схема подпроцесса «Предоставление сервиса OCSP»:

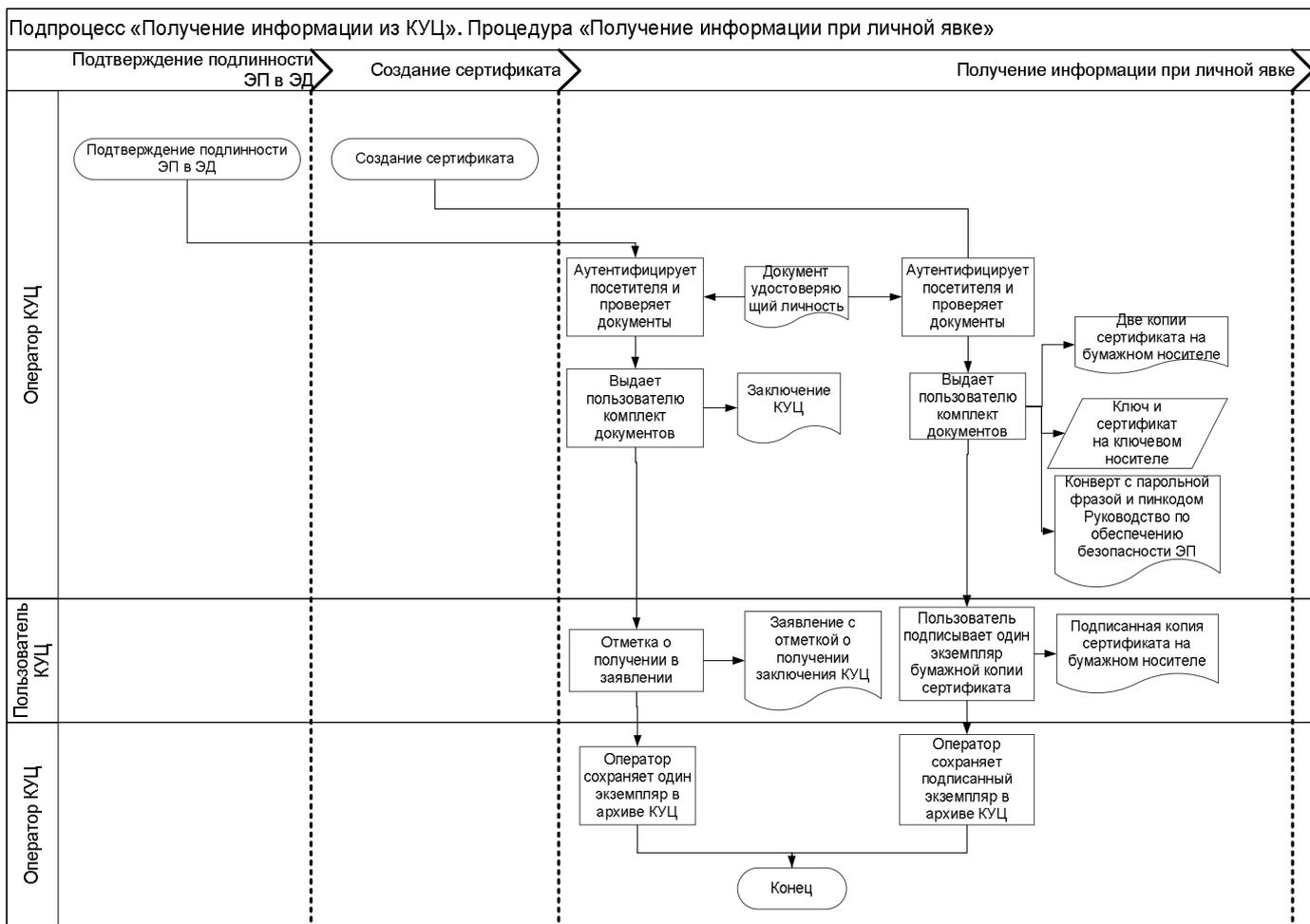


9. Схема подпроцесса «Предоставление сервиса TSP»:

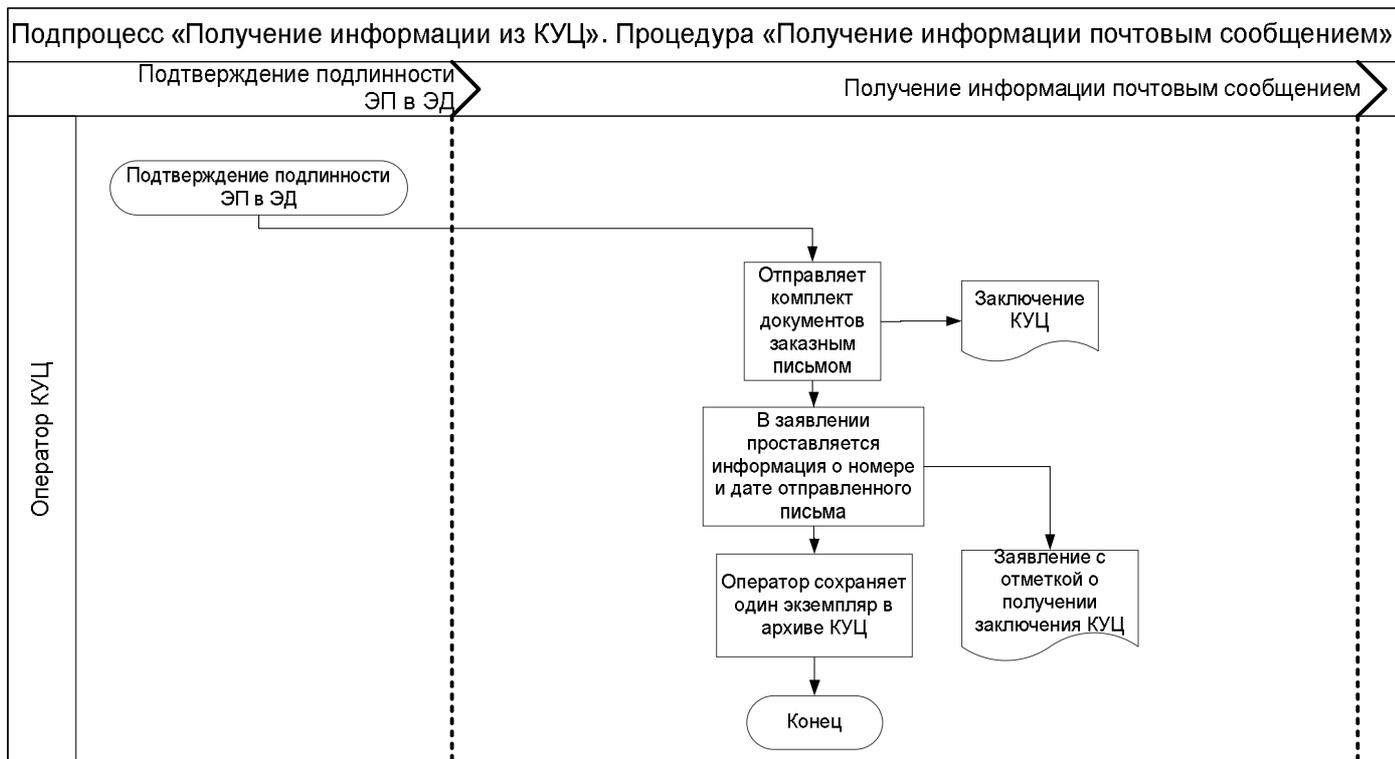


10. Подпроцесс «Получение информации из КУЦ»:

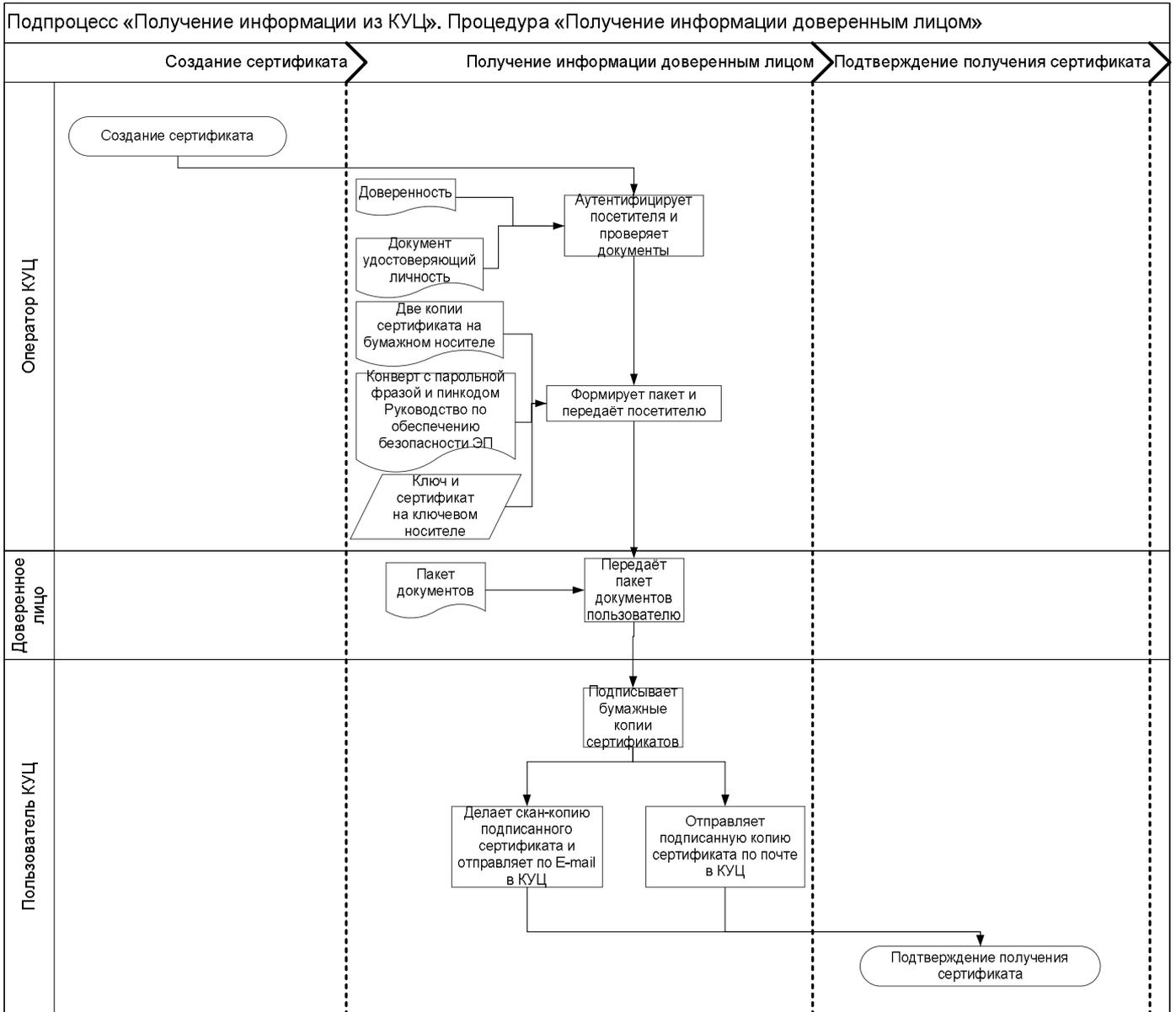
а) Схема процедуры «Получение информации при личной явке»:



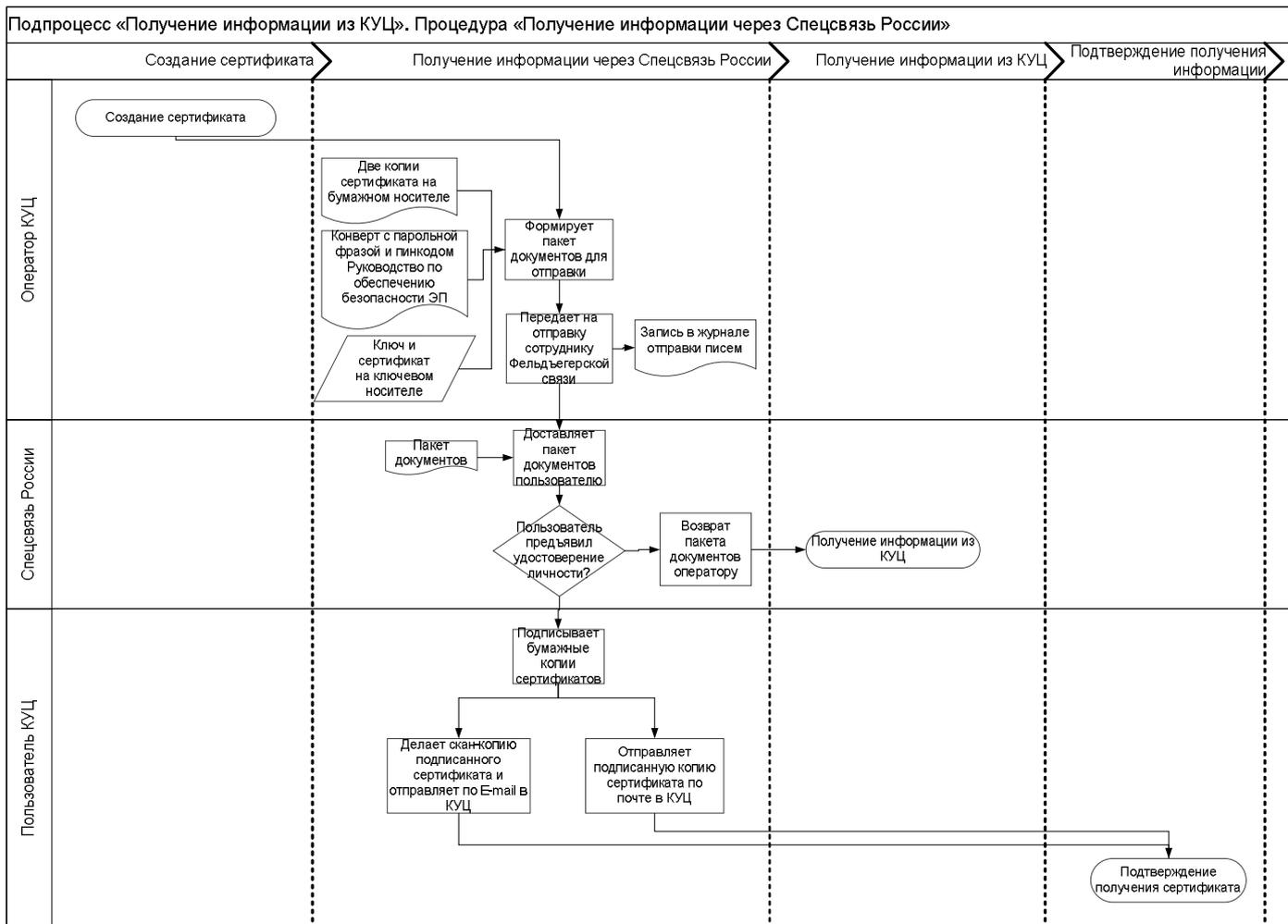
б) Схема процедуры «Получение информации почтовым сообщением»:



с) Схема процедуры «Получение информации доверенным лицом»:



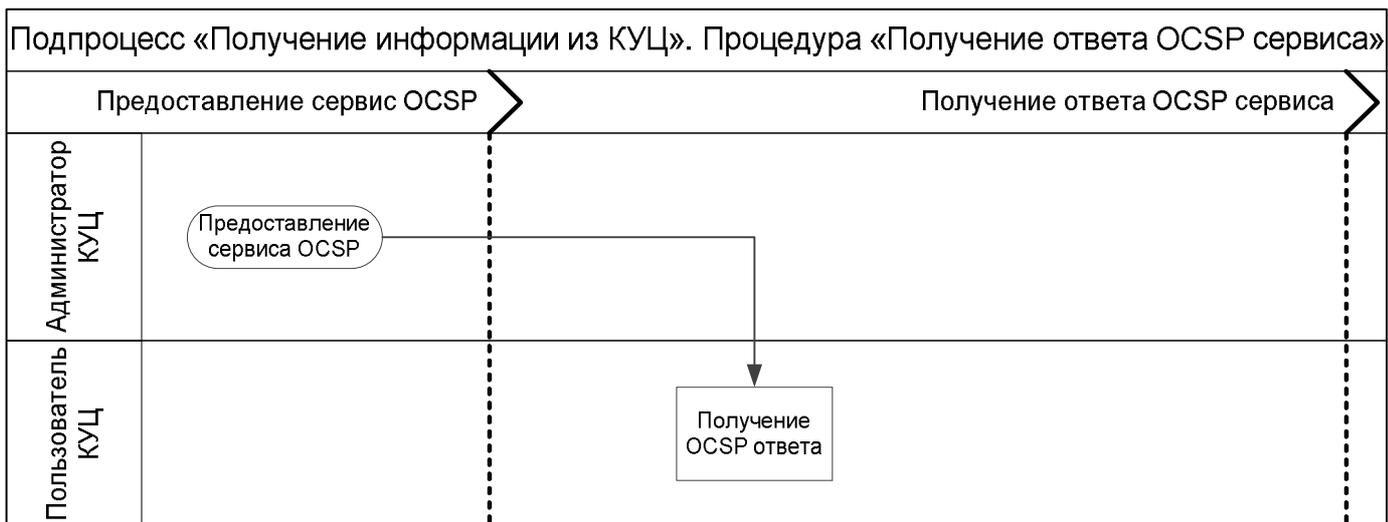
d) Схема процедуры «Получение информации через Спецсвязь России»:



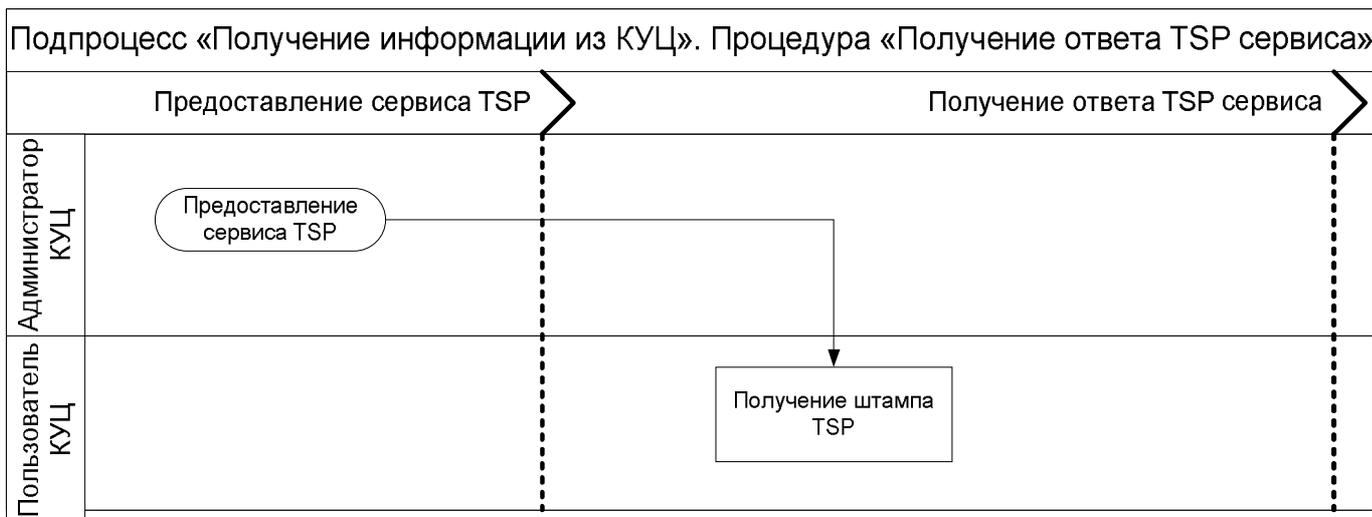
е) Схема процедуры «Получение информации из списков отозванных сертификатов»:



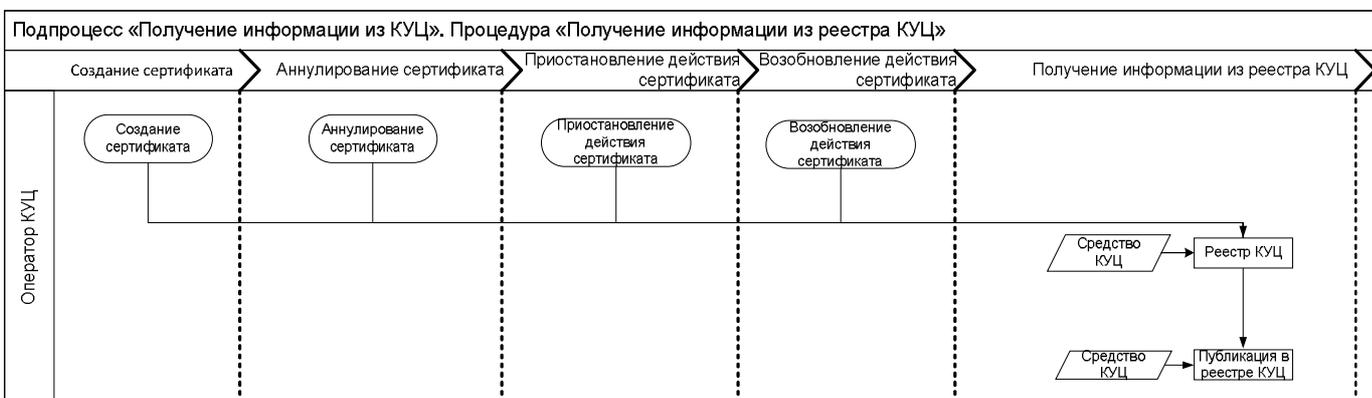
ф) Схема процедуры «Получение ответа OCSP сервиса»:



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 квалифицированных сертификатов ключей 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 (SubjectAlternativeName)» 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 должен 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	А	латинская заглавная буква А	99	П	кириллическая заглавная буква П
26	В	латинская заглавная буква В	100	Р	кириллическая заглавная буква Р
27	С	латинская заглавная буква С	101	С	кириллическая заглавная буква С
28	Д	латинская заглавная буква D	102	Т	кириллическая заглавная буква Т
29	Е	латинская заглавная буква E	103	У	кириллическая заглавная буква У
30	Ф	латинская заглавная буква F	104	Ф	кириллическая заглавная буква Ф
31	Г	латинская заглавная буква G	105	Х	кириллическая заглавная буква Х
32	Н	латинская заглавная буква H	106	Ц	кириллическая заглавная буква Ц
33	І	латинская заглавная буква I	107	Ч	кириллическая заглавная буква Ч
34	Ј	латинская заглавная буква J	108	Ш	кириллическая заглавная буква Ш
35	К	латинская заглавная буква K	109	Щ	кириллическая заглавная буква Щ
36	L	латинская заглавная буква L	110	Ъ	кириллическая заглавная буква Ъ
37	М	латинская заглавная буква M	111	Ы	кириллическая заглавная буква Ы
38	N	латинская заглавная буква N	112	Ь	кириллическая заглавная буква Ь
39	О	латинская заглавная буква O	113	Э	кириллическая заглавная буква Э
40	Р	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 № 8

Заявление на аннулирование сертификата ключа проверки электронной подписи

«_____» _____ 201__ г.

 наименование организации, включая организационно-правовую форму
 в лице _____,

 должность
 _____,

 фамилия, имя, отчество
 действующего на основании _____

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

Серийный номер сертификата	
Причина аннулирования сертификата	

Владелец сертификата ключа проверки электронной подписи _____ / _____ /
 (подпись) (ФИО)

Уполномоченное должностное лицо _____ / _____ /
 (подпись) (ФИО)

«___» _____ 201__ г. М.П.

Отметки удостоверяющего центра

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

_____ / _____ /
 «___» _____ 201__ г.

Приложение № 9

Заявление на приостановление действия сертификата ключа проверки электронной подписи

«_____» _____ 201__ г.

наименование организации, включая организационно-правовую форму

в лице _____,

должность

фамилия, имя, отчество

действующего на основании _____

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

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

Владелец сертификата ключа проверки электронной подписи

_____ / _____ /

(подпись)

(ФИО)

Уполномоченное должностное лицо

_____ / _____ /

(подпись)

(ФИО)

«__» _____ 201__ г.

М.П.

Отметки удостоверяющего центра

Отметка Оператора УЦ.

Данные, указанные в заявлении, проверены.

Сведения о приостановлении действия сертификата ключа проверки электронной подписи занесены в реестр УЦ

_____ / _____ /

«__» _____ 201__ г.

Приложение № 10

Заявление на возобновление действия сертификата ключа проверки электронной подписи

«_____» _____ 201__ г.

наименование организации, включая организационно-правовую форму

в лице _____,

должность

фамилия, имя, отчество

действующего на основании _____

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

Серийный номер сертификата	
----------------------------	--

Владелец сертификата ключа проверки электронной подписи

_____ / _____ /

(подпись)

(ФИО)

Уполномоченное должностное лицо

_____ / _____ /

(подпись)

(ФИО)

«___» _____ 201__ г.

М.П.

Отметки удостоверяющего центра

Отметка Оператора УЦ.

Данные, указанные в заявлении, проверены.

Сведения о возобновлении действия сертификата ключа проверки электронной подписи занесены в реестр УЦ

_____ / _____ /

«___» _____ 201__ г.

Приложение № 11

Заявление на подтверждение подлинности электронной подписи в электронном документе

« _____ » _____ 201__ г.

наименование организации, включая организационно-правовую форму

В лице _____,

должность

фамилия, имя, отчество

действующего на основании _____

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

1. Файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе на прилагаемом к заявлению носителе – рег. № _____;
2. Файл, содержащий подписанные ЭП данные и значение ЭП, либо файл, содержащий исходные данные и файл, содержащий значение ЭП, на прилагаемом к заявлению носителе – рег. № _____
3. Время, на момент наступления которого требуется подтвердить подлинность ЭП:

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

В Корпоративном удостоверяющем центре по адресу: г. Москва, 1-й Нагатинский проезд., д. 10, стр. 1, ком. 906	<input type="checkbox"/>
Почтовым сообщением по адресу (указать адрес и имя получателя):	<input type="checkbox"/>

Владелец сертификата ключа проверки электронной подписи _____ / _____ /
(подпись) (ФИО)

Уполномоченное должностное лицо _____ / _____ /
(подпись) (ФИО)

« ____ » _____ 201__ г. М.П.

Отметки удостоверяющего центра

Подготовлено заключение о подтверждении подлинности ЭП в электронном документе _____ / _____ /
« ____ » _____ 201__ г.

Заключение о подтверждении подлинности ЭП получено пользователем _____ / _____ /
« ____ » _____ 201__ г.

Приложение № 12

Форма копии сертификата на бумажном носителе

Сведения о сертификате:

Кому выдан: CN

Кем выдан: Rosatom GOST CA

Действителен с <дата вступления в силу> по <дата окончания>

Версия: 3 (0x2)

Серийный номер: <Серийный номер>

Издатель сертификата: CN = Rosatom GOST CA, O = Госкорпорация "Росатом", L = Москва, S = г. Москва, C = RU, E = ca@rosatom.ru, Street = ул. Большая Ордынка д. 24, = 007706413348, = 1077799032926

Срок действия:

Действителен с: <дата вступления в силу>

Действителен по: <дата окончания>

Владелец сертификата: CN, OU, O, L, S, C, E, INN, SNILS, OGRN

Открытый ключ:

Алгоритм открытого ключа:

Название: <название алгоритма>

Идентификатор: <идентификатор алгоритма>

Значение: <значение открытого ключа>

Расширения сертификата X.509

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа

Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

2. Расширение 2.5.29.37

Название: Улучшенный ключ

Значение: Временный доступ к Центру Регистрации (1.2.643.2.2.34.2)

3. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта

Значение: da 01 d1 46 47 58 69 b4 85 b3 1f cb 1e 22 cc 5f 9e 95 de 79

4. Расширение 2.5.29.35

Название: Идентификатор ключа центра сертификатов

Значение: Идентификатор ключа=46 e6 c6 29 7f 19 ed 18 05 94 b4 f4 4f 6c 00 cb b7 51 2c 2f Поставщик сертификата: <информация о поставщике сертификата>

5. Расширение 2.5.29.31

Название: Точки распространения списков отзыва (CRL)

Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: <перечень точек распространения СОС>

6. Расширение 1.3.6.1.5.5.7.1.1

Название: Доступ к информации о центрах сертификации

Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)

Дополнительное имя: <адрес размещения издающего сертификата>

7. Расширение 2.5.29.16

Название: Период использования закрытого ключа

Значение: Действителен с <дата вступления в силу> Действителен по <дата окончания>

8. Расширение 2.5.29.32

Название: Политики сертификата

Значение: [1]Политика сертификата: Идентификатор политики=1.2.643.100.113.1

9. Расширение 1.2.643.100.111

Значение: <Средство электронной подписи пользователя>

10. Расширение 1.2.643.100.112

Значение: <Средство электронной подписи издателя>

Подпись Удостоверяющего центра:

Алгоритм подписи:

Название: <название алгоритма>

Идентификатор: <идентификатор>

Значение: <значение открытого ключа издателя>

Подпись уполномоченного сотрудника УЦ: _____ / _____
" ____ " _____ 201__ г.

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

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

Приложение № 13

Формат сертификата ключа проверки электронной подписи

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

Приложение № 14

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

Пользователь КУЦ обязан:

- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием средств квалифицированной электронной подписи;
- сдать средства квалифицированной электронной подписи и ключи электронной подписи, эксплуатационную и техническую документацию к ним в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств квалифицированной электронной подписи;
- немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи средств квалифицированной электронной подписи, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений
- обеспечивать конфиденциальность ключей электронной подписи, в частности не допускать использование принадлежащих ему ключей электронной подписи без его согласия;
- уведомлять КУЦ, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированной электронной подписи и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с действующим Федеральным законодательством.
- не использовать ключ электронной подписи и немедленно обратиться в КУЦ для прекращения действия сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;
- использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены).
- обновлять сертификат ключа проверки электронной подписи в соответствии с установленным регламентом.
- принять меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным средством квалифицированной электронной подписи, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на средства квалифицированной электронной подписи, технические средства, на которых эксплуатируется средства квалифицированной электронной подписи и защищаемую информацию.

Пользователю КУЦ запрещается:

- оставлять без контроля вычислительные средства, на которых эксплуатируется средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;
- записывать на ключевые носители постороннюю информацию;
- использовать нестандартные, изменённые или отладочные версии операционных систем (ОС).
- использовать ОС, отличную от предусмотренной штатной работой.
- использовать возможность удалённого управления, администрирования и модификации ОС и её настроек.
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации.
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ
- подключать к компьютеру с установленным средством квалифицированной электронной подписи дополнительные устройства и соединители, не предусмотренные штатной комплектацией.
- изменять настройки, установленные программой установки средства квалифицированной электронной подписи или администратором.
- обрабатывать на ПЭВМ, оснащённой средством квалифицированной электронной подписи, информацию, содержащую государственную тайну.
- осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

Пользователь КУЦ несёт ответственность за:

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

Приложение № 15

Ограничения использования сертификатов ключей проверки электронной подписи

1. Квалифицированный сертификат Госкорпорации «Росатом»

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

В сертификате указываются следующие ограничения:

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

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
- Пользователь Центра Регистрации, NTTP, 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, НТТР, 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, NTTP, TLS клиент (1.2.643.2.2.34.6)
- Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости (1.2.643.5.1.24.2.30)

Срок действия сертификата - 1 год и 3 месяца.

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

Приложение № 16

Перечень областей использования сертификатов, зарегистрированных в КУЦ

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

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

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

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

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

У Т В Е Р Ж Д А Ю

Заместитель директора по
информационным технологиям
АО «Гринатом»



С.Н. Данилов

(по дов. № 22/309/2018-ДОВ от 28.12.18)

М.П.

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»

Редакция №3

Москва 2019 г.

Оглавление

1. Назначение и область применения	3
2. Термины, определения и сокращения	5
3. Описание процесса.....	9
3.1. Цель процесса.....	9
3.2. Задачи процесса.....	9
3.3. Участники группы процессов и их роли	9
3.4. Основные выходы процесса.....	12
3.5. Основные входы процесса	16
3.6. Описание подпроцессов.....	21
4. Нормативные ссылки	32
5. Порядок внесения изменений	33
6. Контроль и ответственность.....	33
7. Перечень приложений.....	34
Приложение №1. Матрица ответственности	36
Приложение №2. Схема процесса	38
Приложение №3. Дополнительные выходы и дополнительные входы.....	51
Приложение №4. Форма приказа о назначении Администраторов безопасности и лиц их замещающих.....	52
Приложение №5. Форма Заявления на услугу Администратора безопасности	53
Приложение №6. Перечень лиц, допускаемых к самостоятельной работе с СКЗИ.....	54
Приложение №7. Форма Приказа о предоставлении прав подписей	55
Приложение №8.1 Заявление на СКЗИ (с передачей СКЗИ)	56
Приложение №8.2 Заявление на СКЗИ (без передачи СКЗИ)	57
Приложение №9. Схема организации криптографической защиты конфиденциальной информации (шаблон)	58
Приложение №10. Книга лицевых счетов	59
Приложение №11. Доверенность доверенного лица на получение СКЗИ в ОКЗ	62
Приложение №12. Сопроводительное письмо к СКЗИ.....	63
Приложение №13. Акт повреждения упаковки	64
Приложение №14. Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации).....	65
Приложение №15. Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ.....	67
Приложение №16. Технический (аппаратный) журнал.....	73
Приложение №17. Акт готовности СКЗИ к эксплуатации.....	74
Приложение №18. Учебные материалы.....	76
Приложение №19. Анкета для опроса пользователей.....	107
Приложение №20. Заключение о сдаче зачетов	112
Приложение №21. Заключение о возможности эксплуатации СКЗИ.....	114
Приложение №22. Журнал выполнения регламентных работ.....	115
Приложение №23. Порядок проведения расследований фактов нарушения условий использования СКЗИ.....	117
Приложение №24. Акт уничтожения СКЗИ	136
Приложение №25. Приказ о проведении проверки	137
Приложение №26. План-график проведения проверок.....	138
Приложение №27. Информационное письмо о проведении проверки.....	139
Приложение №28. Сводная таблица по объекту проверки	140
Приложение №29. Программа проверки.....	150
Приложение №30. Акт проверки.....	156
Приложение №31. План устранения недостатков	164

1. Назначение и область применения

Настоящий 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» (далее – Регламент), разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты (далее – ОКЗ).

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

Требования настоящего Регламента распространяются на организации-обладатели конфиденциальной информации (далее - ООКИ), использующие 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 Регламент использует ссылки на следующие документы, необходимые для управления процессом «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»:

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	Действует	Лицензия	Данилов С.Н.

<p>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)</p>			
<p>Федеральный закон Российской Федерации от 06.04.11 г. № 63-ФЗ "Об электронной подписи"</p>	<p>Действует</p>	<p>Федеральный закон</p>	<p>Данилов С.Н.</p>
<p>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»</p>	<p>Действует</p>	<p>Приказ</p>	<p>Данилов С.Н.</p>
<p>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)»</p>	<p>Действует</p>	<p>Приказ</p>	<p>Данилов С.Н.</p>

Отраслевые требования по информационной безопасности Госкорпорации «Росатом» №1/910-П-дсп от 23.09.2014	Действует	Требование	Данилов С.Н.
---	-----------	------------	--------------

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 Регламента»

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)	<p>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;</p> <p>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;</p> <p>средства электронной подписи;</p>

	<p>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;</p> <p>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;</p> <p>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;</p> <p>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;</p>
--	---

	<p>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;</p> <p>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.</p>
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 Регламента.

3.3. Участники группы процессов и их роли

№ п.п.	Участники	Основные роли
--------	-----------	---------------

1	Руководитель ООКИ	<ul style="list-style-type: none"> • 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 регламента 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»; • 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)	<ul style="list-style-type: none"> • Разрабатывает и поддерживает в актуальном состоянии схему криптографической защиты информации; • Определяет требования к защищенности различных информационных систем в соответствии с действующей нормативно-методической документацией;

		<ul style="list-style-type: none"> • Составляет заключение о возможности эксплуатации СКЗИ; • Формирует комплект поставки СКЗИ; • Учитывает СКЗИ в ОКЗ; • Отправляет СКЗИ в ООКИ.
3	Администратор безопасности ОКЗ АО «Гринатом»	<ul style="list-style-type: none"> • 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»	<ul style="list-style-type: none"> • Согласовывает Приказ о проведении проверки требований Регламента; • Согласовывает Приказ о проведении расследования условий использования СКЗИ.
5	Начальник Управления информационной безопасности АО «Гринатом»	<ul style="list-style-type: none"> • 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 Заключение по результатам расследований фактов нарушения условий использования СКЗИ.
6	Руководитель Органа криптографической защиты АО «Гринатом»	<ul style="list-style-type: none"> • 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

		<p>доступом, не содержащей сведений, составляющих государственную тайну;</p> <ul style="list-style-type: none"> • Утверждает Заключение комиссии Органа криптографической защиты АО «Гринатом» по результатам расследования фактов нарушения условий использования СКЗИ.
7	Проверяющий	<ul style="list-style-type: none"> • Подготавливает документы для проведения проверок выполнения требований Регламента; • Осуществляет проверки выполнения требований Регламента; • 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

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ 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
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

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ 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 (для обладателя конфиденциальной информации)	Предприятие, АО «Гринатом»	Организация
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

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ 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 ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ	Предприятие, АО «Гринатом»	Организация
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	Предприятие, АО «Гринатом»	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация)
	каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ		

3.5. Основные входы процесса

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
1	Отраслевые требования по информационной безопасности ГК «Росатом» №1/910-П-дсп от 23.09.2014	ГК «Росатом»	Корпорация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
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
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	Предприятие	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
	самостоятельной работе с СКЗИ		
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
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

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ 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
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

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ 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
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	АО «Гринатом»	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
	государственную тайну в ООКИ		
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 Отраслевыми требованиями по информационной безопасности №1/910-П-дсп от 23.09.2014.

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 печатывает 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):

- Оформляет доверенность на себя на получение СКЗИ из банка;
- Получает в банке СКЗИ по доверенности;

- Подписывает акт приема-передачи банковского СКЗИ по форме, установленной банком.

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 получают 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 «Отраслевым требованиям по информационной безопасности Госкорпорации «Росатом» безопасности №1/910-П-дсп от 23.09.2014 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 получают из банка):

- Ставит на учет носители информации в качестве ключевых;
- Производит генерацию ключевой информации Пользователей и 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 Банк;
- Получает зарегистрированные сертификаты из Банка;
- Делает отметку в Журнале учета (для обладателя конфиденциальной информации) о сроках действия сертификата.

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 Регламента».

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):

- 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.

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 Регламента»):

- Устраняет недостатки, выявленные в ходе проверки выполнения требований Регламента;
- Проставляет отметки об устранении недостатков в Плане устранения недостатков, выявленных в ходе проверки выполнения требований Регламента;
- Направляет в ОКЗ АО «Гринатом» План устранения недостатков, выявленных в ходе проверки выполнения требований Регламента, 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 shredders.

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 отказывается 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 Регламента».

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)»;
- 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);

- Отраслевые требования по информационной безопасности Госкорпорации «Росатом» безопасности №1/910-П-дсп от 23.09.2014;
- Постановление №313 от 16.04.2012 г. Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

5. Порядок внесения изменений

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

6. Контроль и ответственность

6.1 Регламент обязаны соблюдать все следующие участники процесса:

Руководитель ООКИ;
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 Регламента.

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

7. Перечень приложений

Приложение №1.	Матрица ответственности.
Приложение №2.	Схема процесса.
Приложение №3.	Дополнительные выходы и дополнительные входы.
Приложение №4.	Форма приказа о назначении Администраторов безопасности и лиц их замещающих
Приложение №5.	Форма Заявления на услугу Администратора безопасности
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 СКЗ И (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

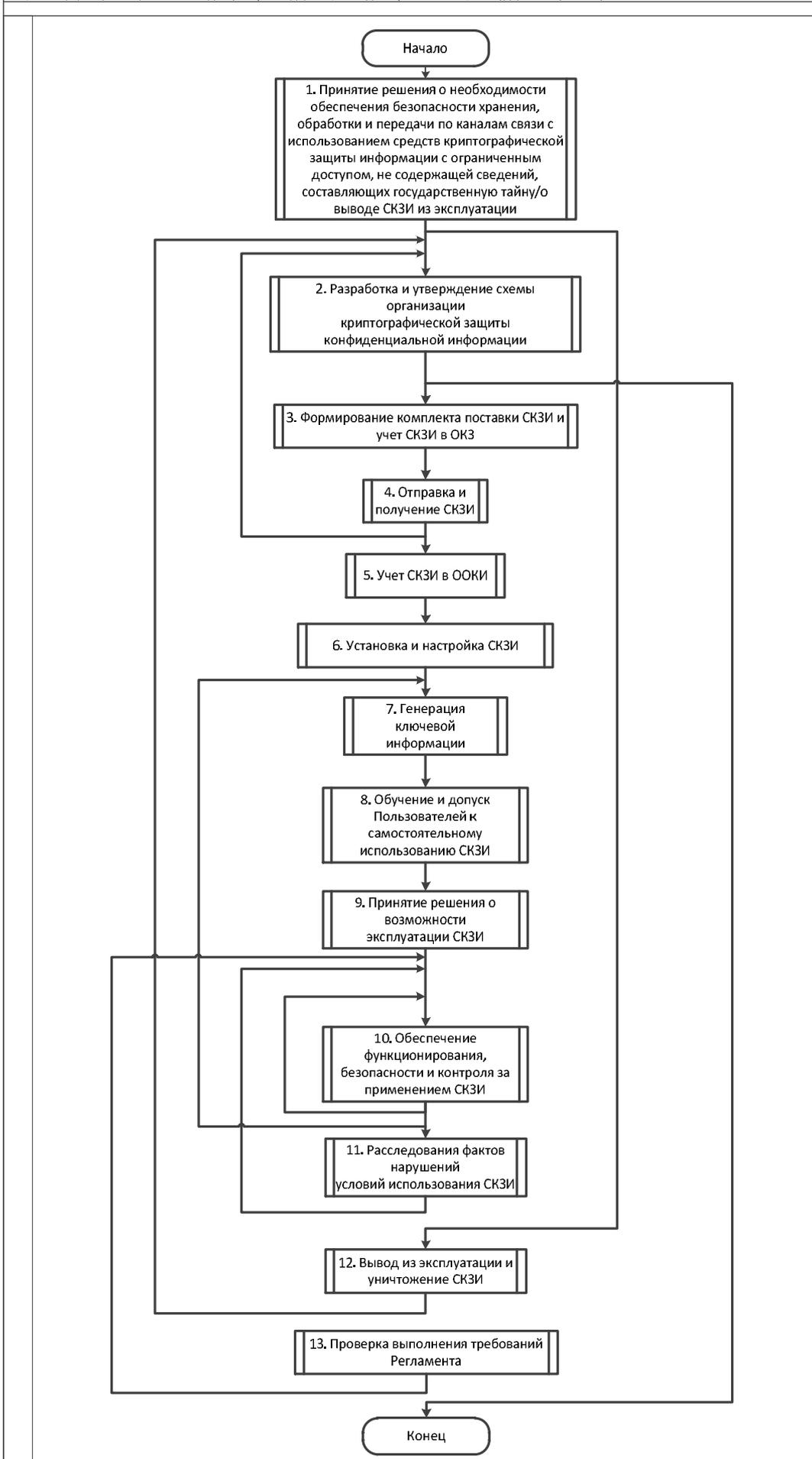
Подпроцессы в составе процесса	Участники процесса						
	Руководитель ООКИ	Аналитик	АБ	Начальник Управления информационно-безопасности АО «Гринатом»	Руководитель Органа криптографической защиты АО «Гринатом»	Руководитель АО «Гринатом»	Проверяющий
Подпроцесс «Принятие решения о необходимости обеспечения 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 Регламента»	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

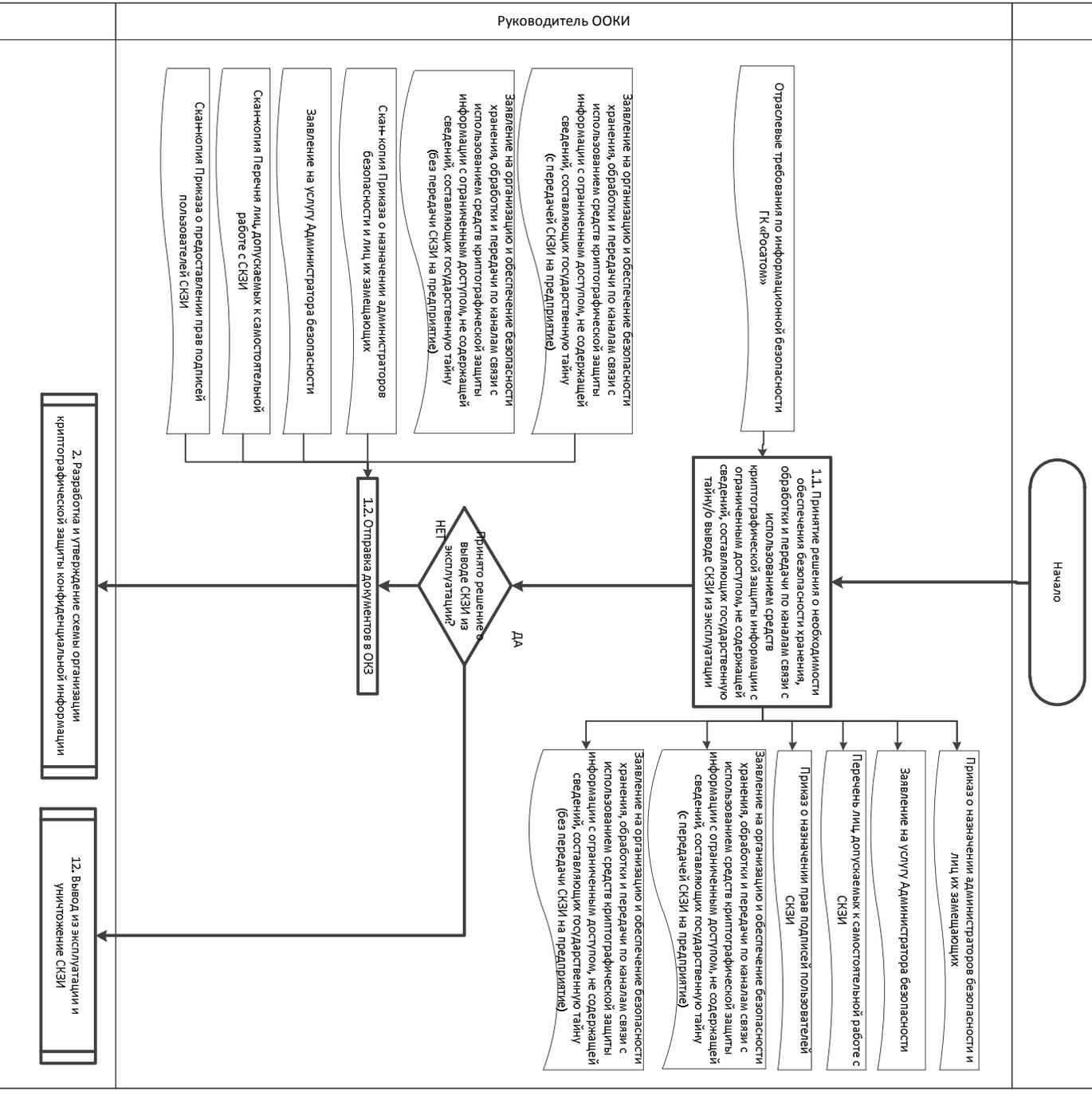
И	Интегратор	Интегрирует результаты подпроцесса/процедуры и отвечает за организацию подпроцесса/процедуры, включая взаимодействие участников	Структурное подразделение Корпорации/Дивизиона/Организации
К	Контролер	Осуществляет контроль выполнения и достижения результатов подпроцесса/процедуры	Структурное 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

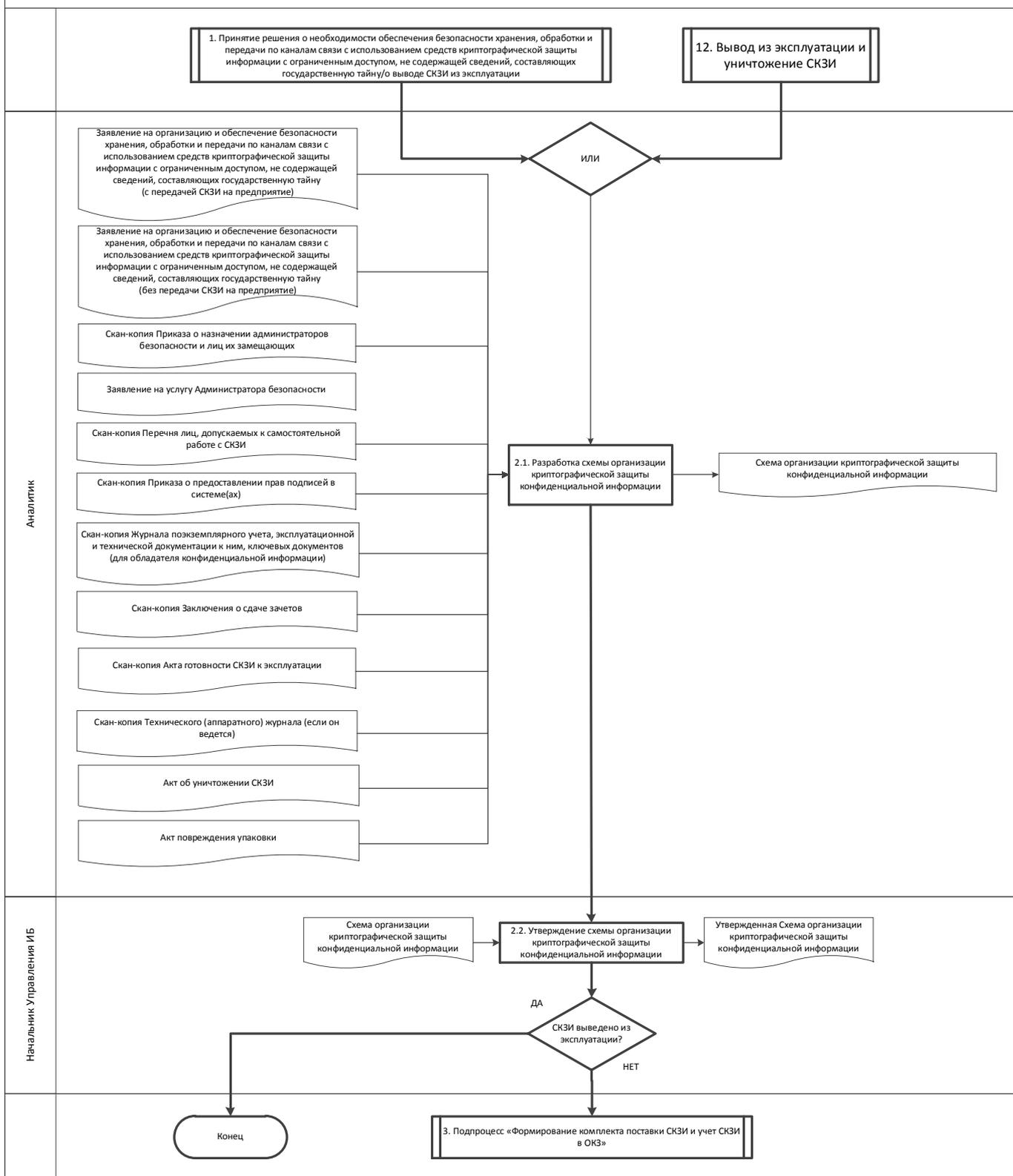
Процесс «Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»



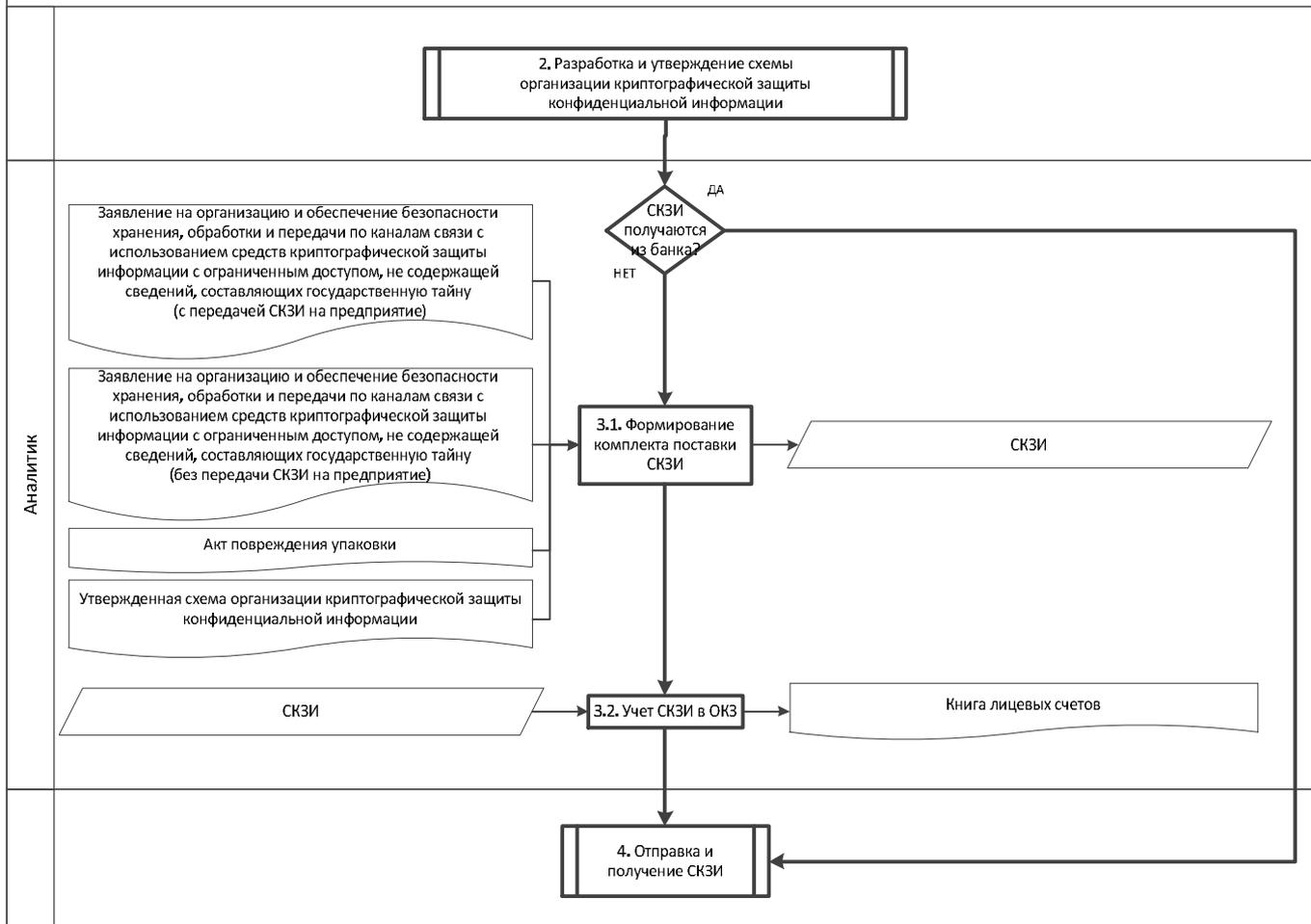
1. Подпроцесс «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации»



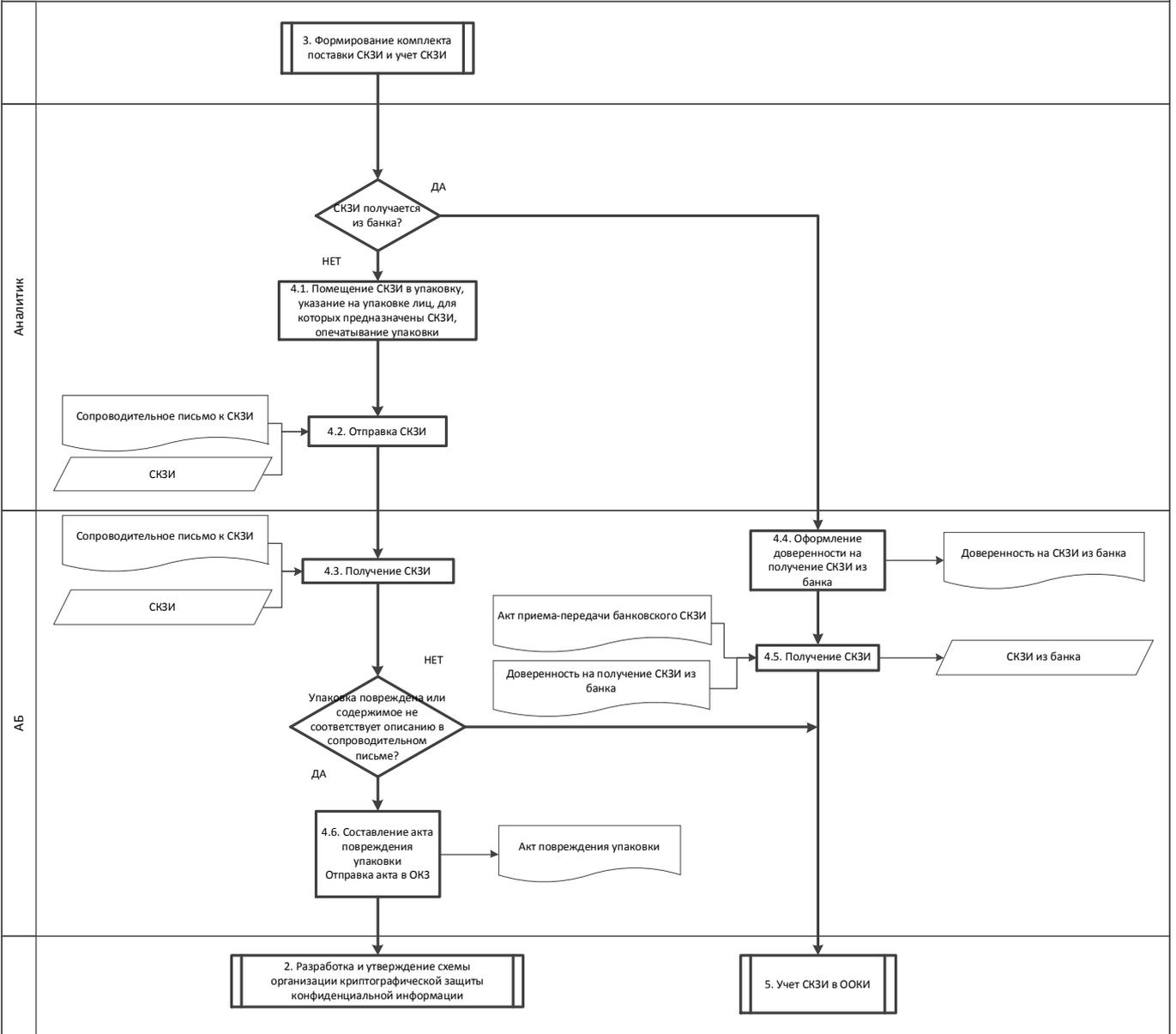
2. Подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации»



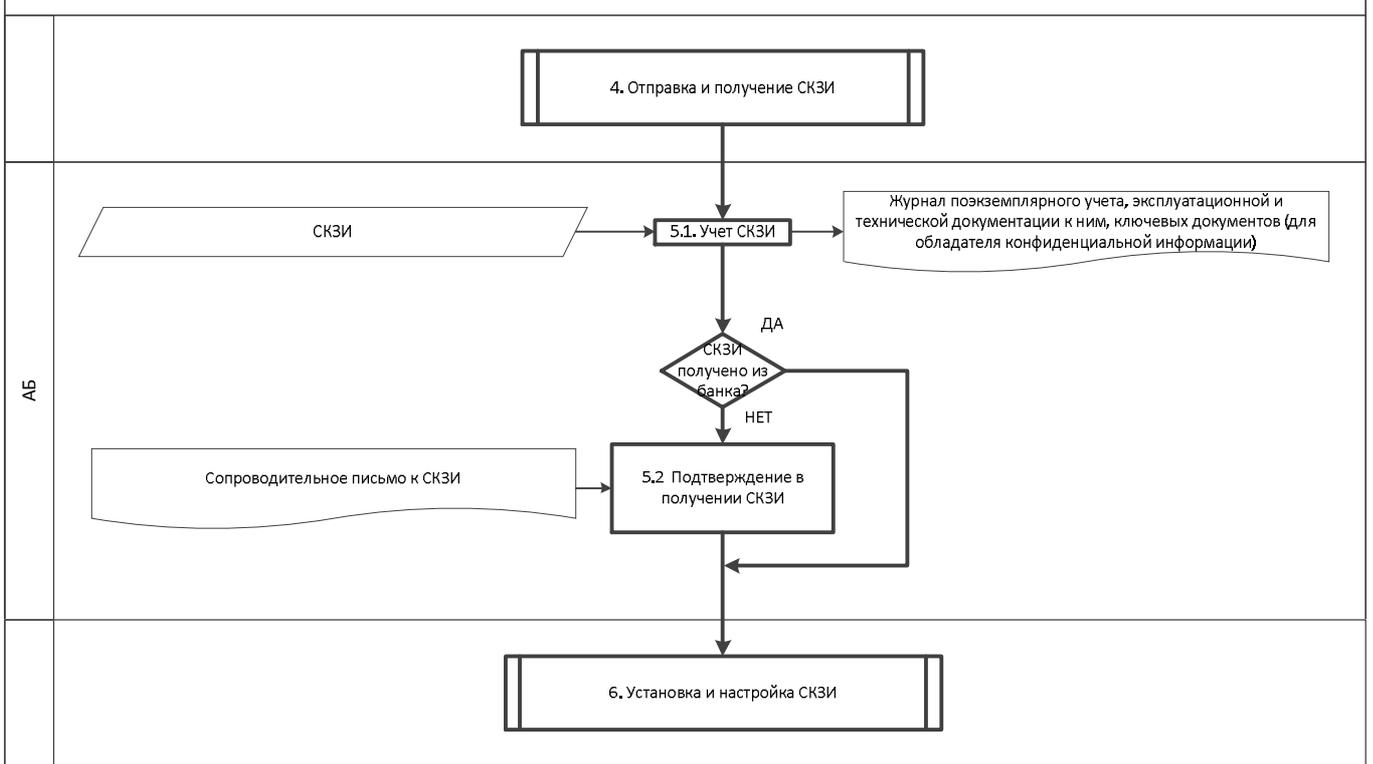
3. Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ в ОКЗ»



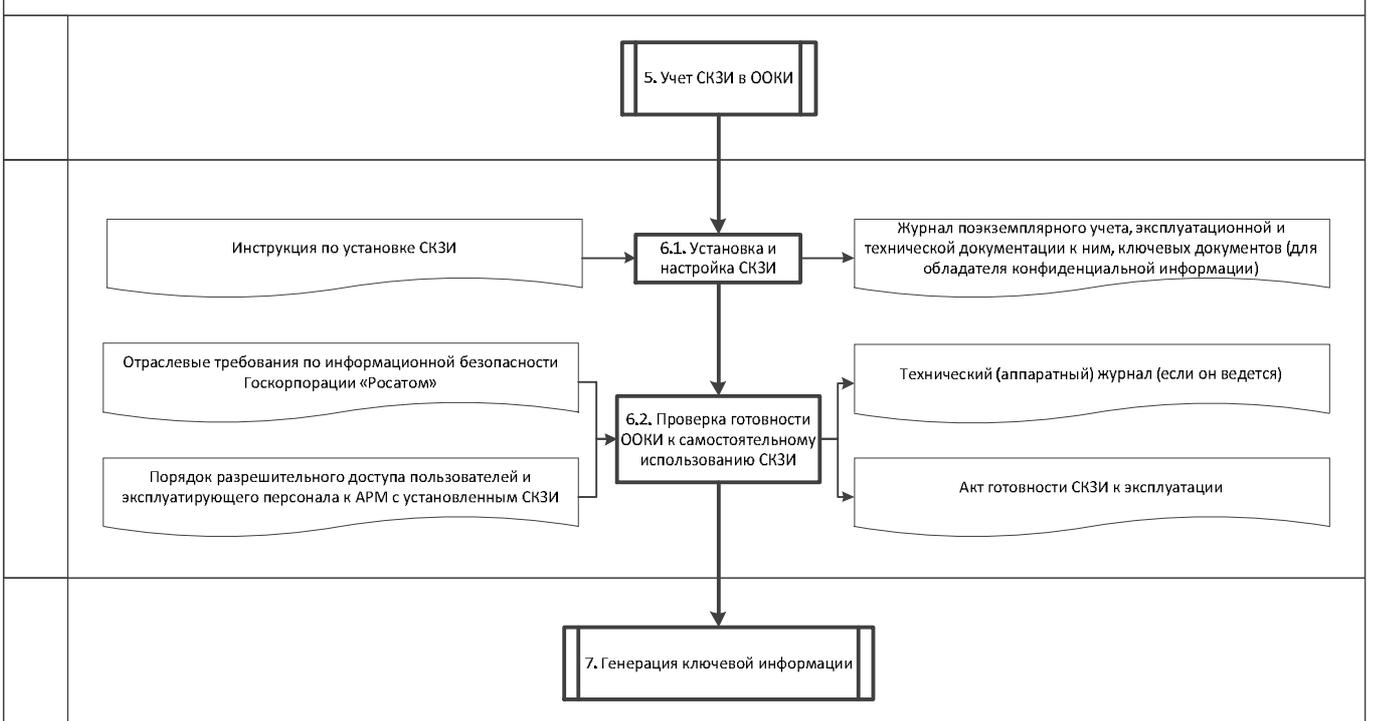
4. Подпроцесс «Отправка и получение СКЗИ»



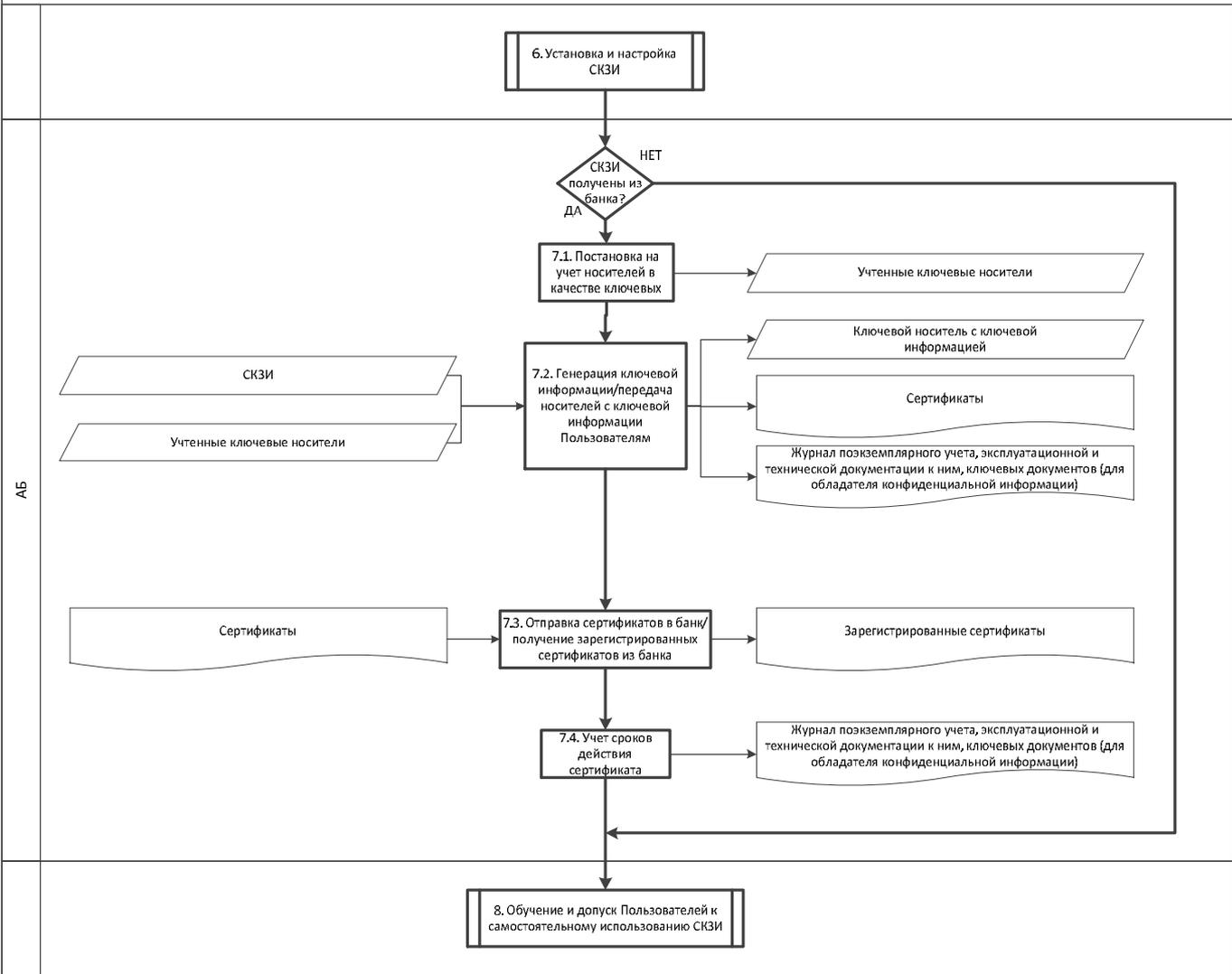
5. Подпроцесс «Учет СКЗИ в ООКИ»



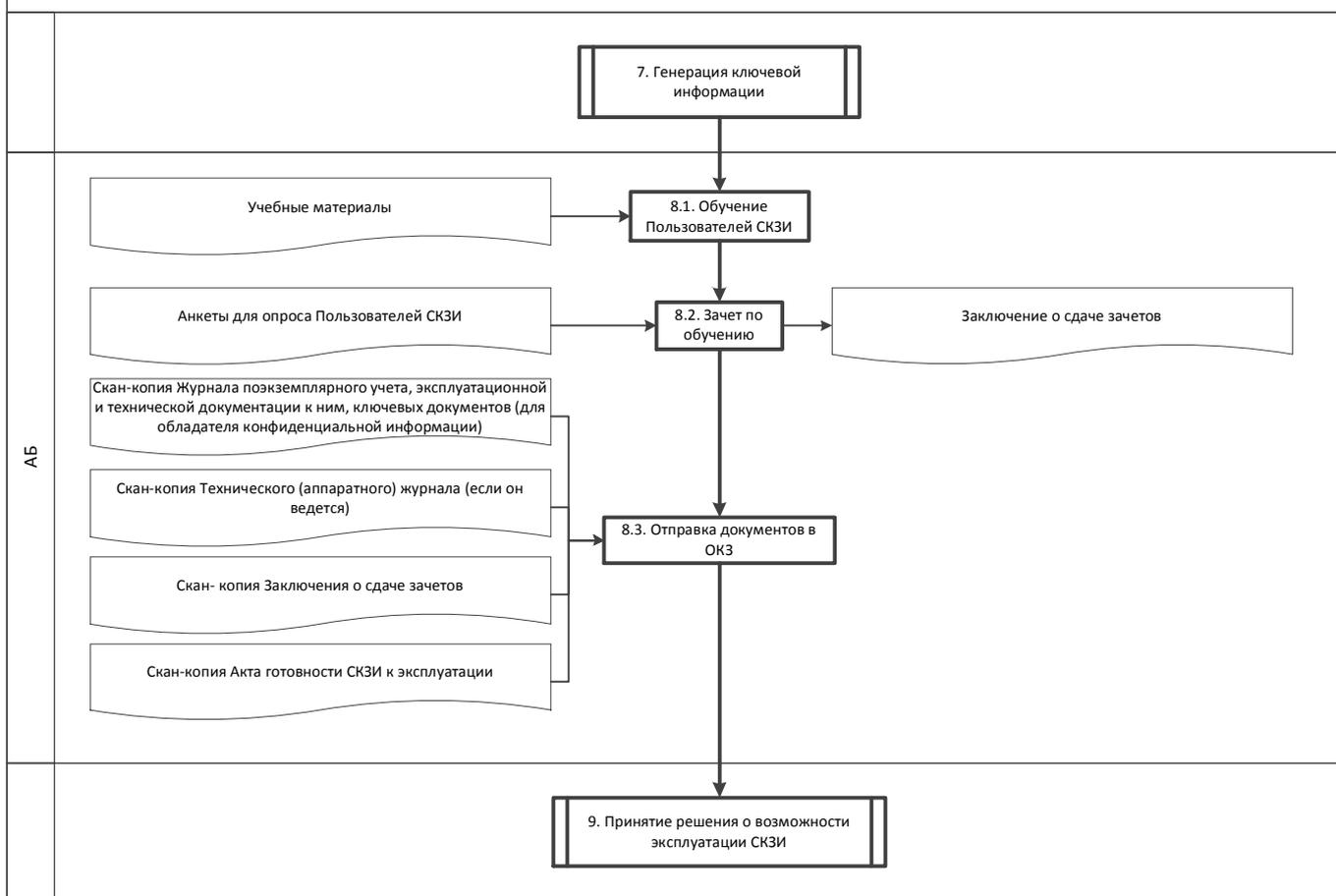
6. Подпроцесс «Установка и настройка СКЗИ»



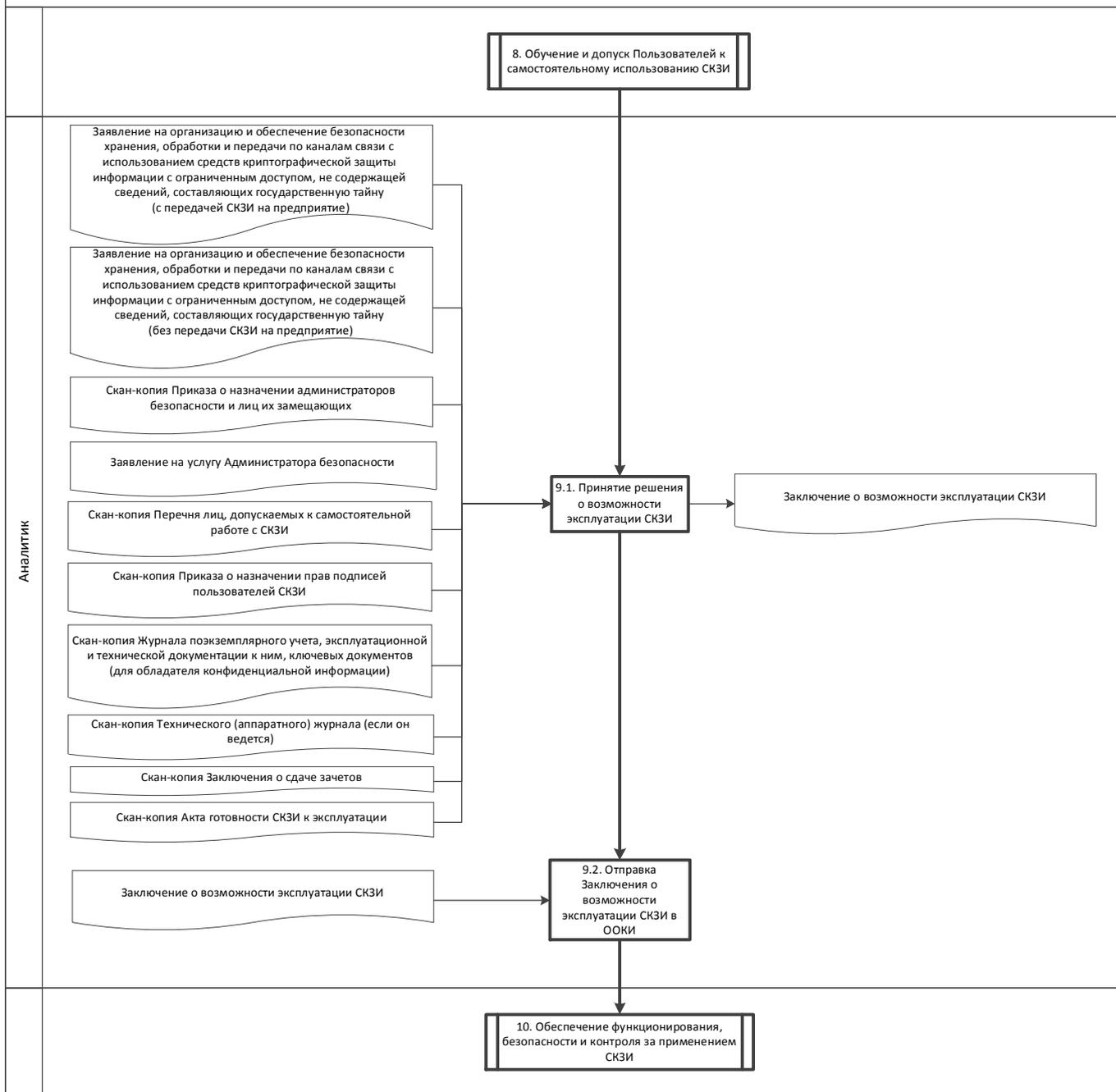
7. Подпроцесс «Генерация ключевой информации»



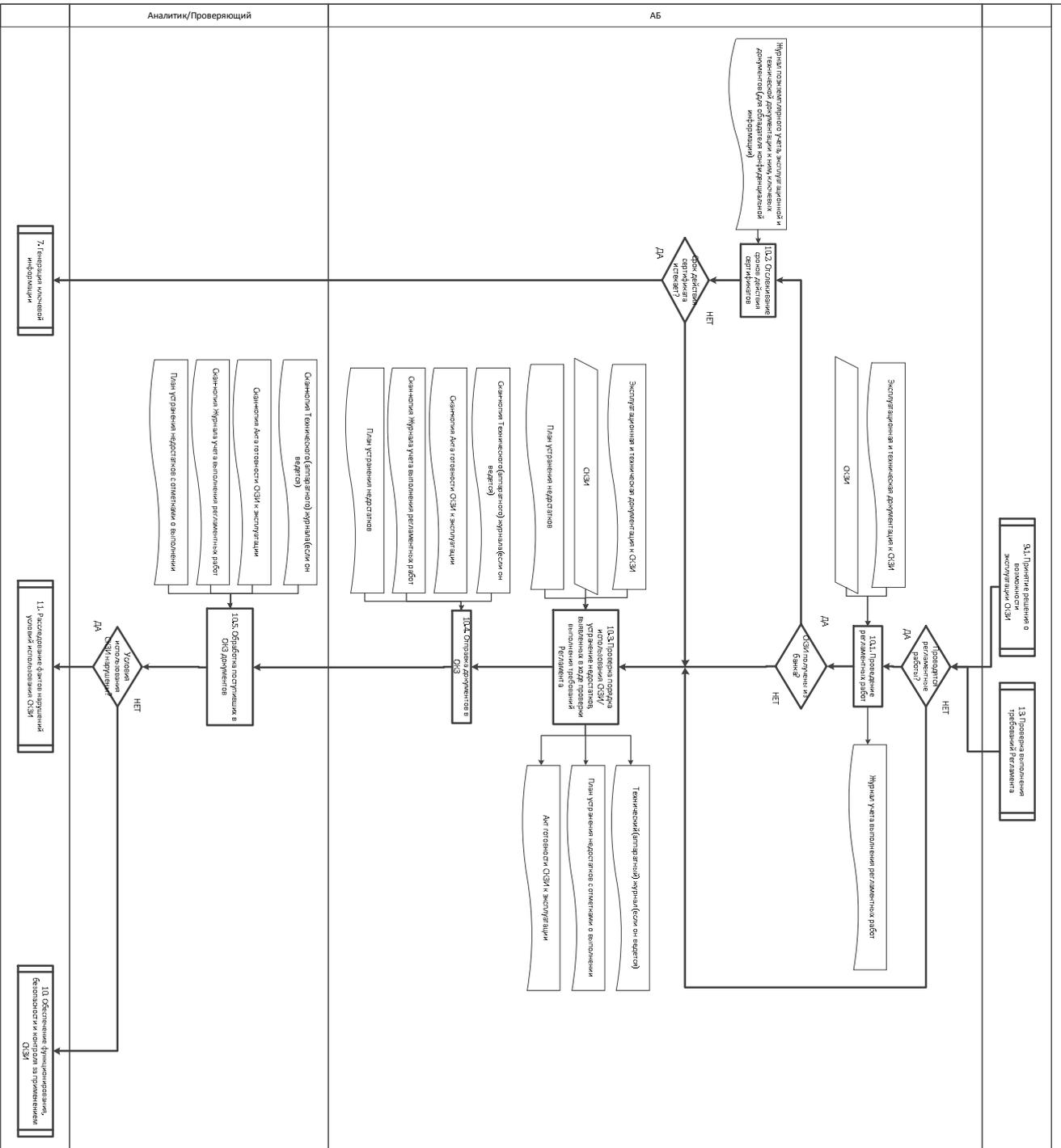
8. Подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ»



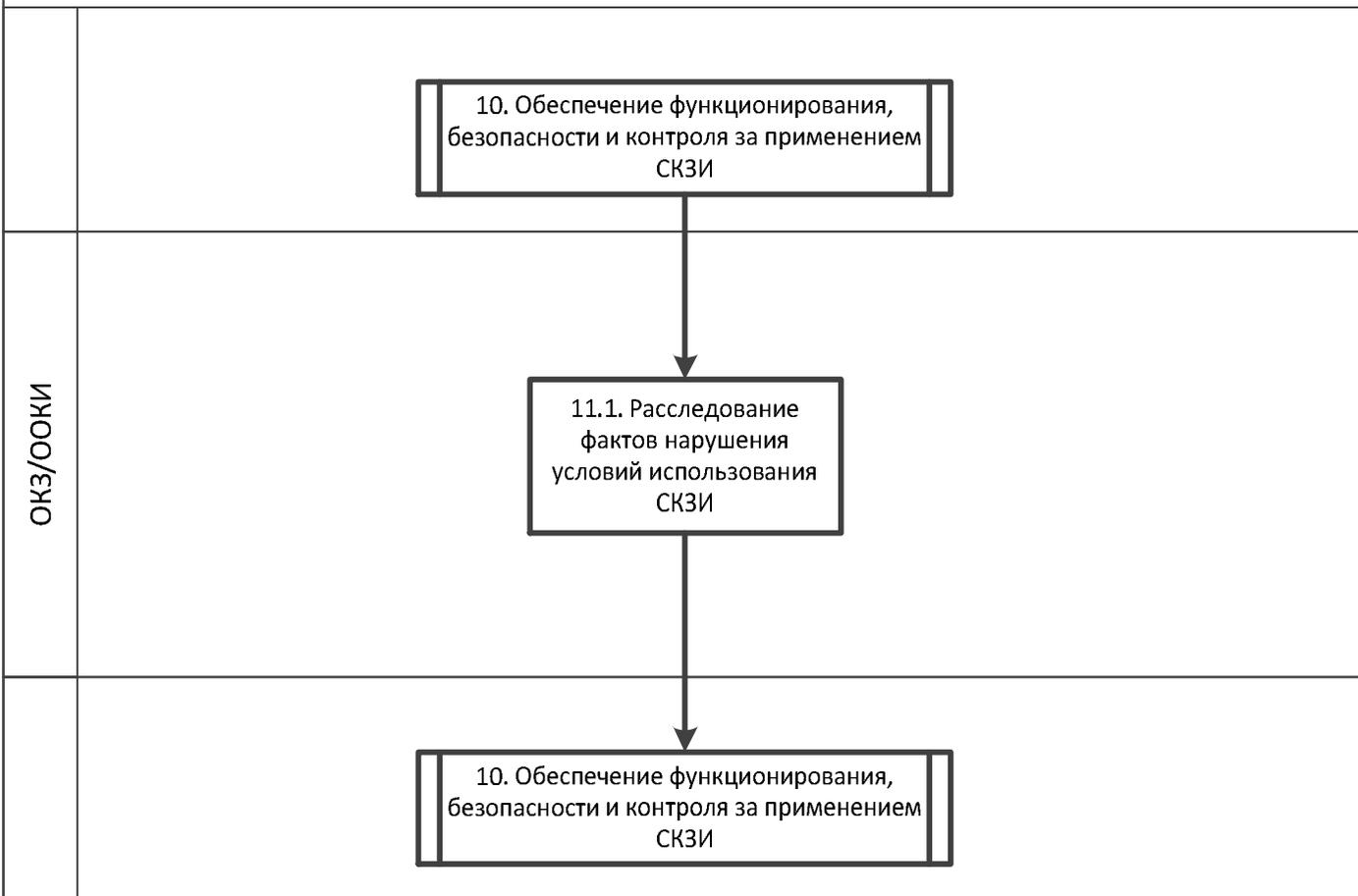
9. Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»



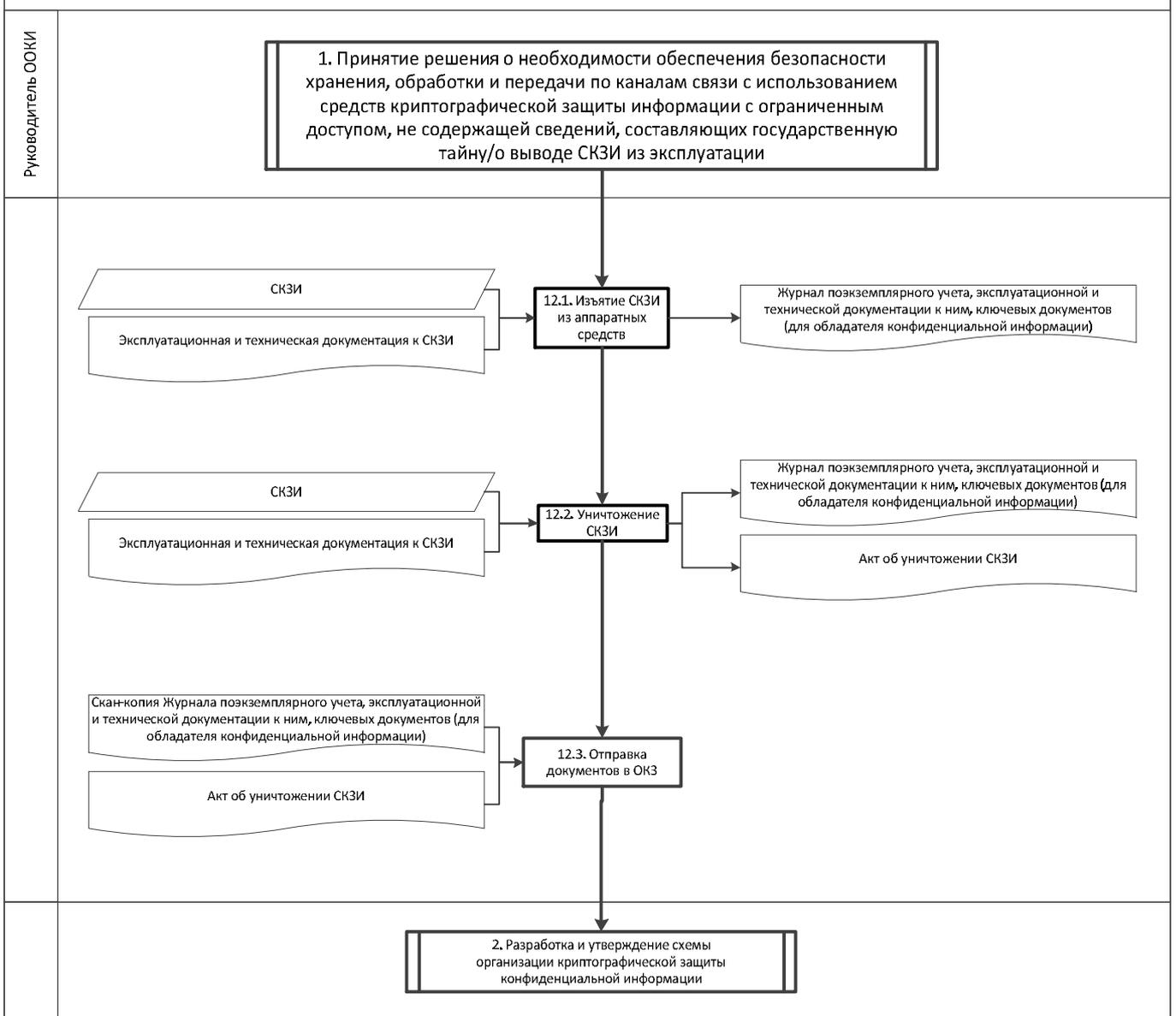
10. Подпроцесс «Обеспечение функционирования безопасности контроля за применением СЭИ»



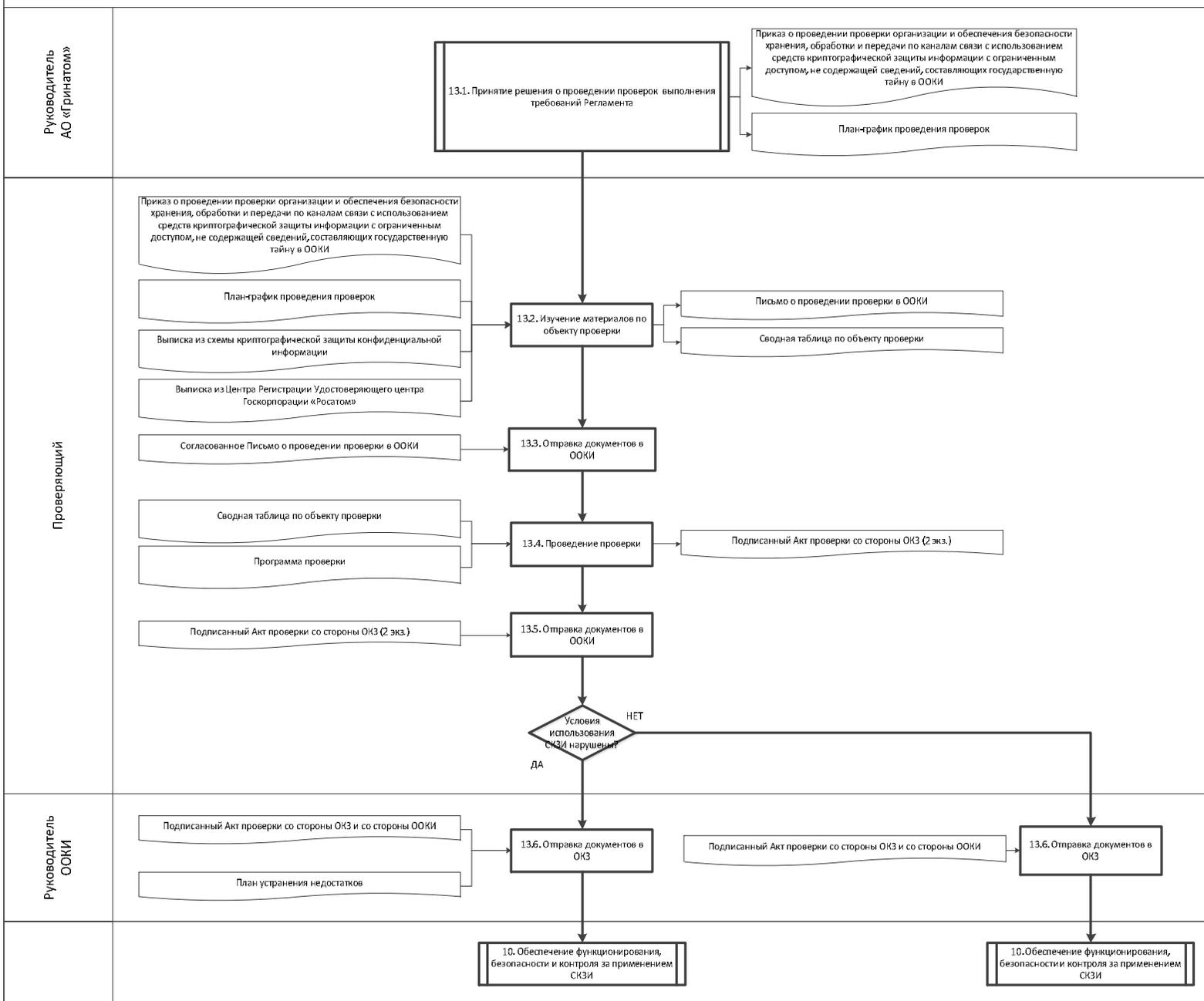
11. Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»



12. Подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ»



13. Подпроцесс «Проверка выполнения требований Регламента»



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, а также контроль за соблюдением требований по безопасности 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 №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.
(дата)

наименование организации, включая организационно-правовую форму

В лице _____,
должность _____

фамилия, имя, отчество

действующего на основании _____

просит ОКЗ АО «Гринатом»:

1. 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 «Отраслевыми требованиями по информационной безопасности Госкорпорации «Росатом» №1/910-П-дсп от 23.09.2014 в организации, _____ расположенной _____ по _____ адресу

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

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

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.
(дата)

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 «Отраслевыми требованиями по информационной безопасности Госкорпорации «Росатом» №1/910-П-дсп от 23.09.2014 в организации, расположенной по адресу

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

№ п/п	Пользователь СКЗИ (должность, Ф.И.О.)	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

Администратор безопасности

_____/_____
(подпись) (ФИО)

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО
ДОЛЖНОСТНОГО ЛИЦА>

_____/_____
(подпись) (ФИО)

М.П.

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

			№ п/п
			Краткое наименование предприятия
			Полное наименование предприятия
			Заявление о присоединении №
			Администратор безопасности (ФИО, Приказ/ <small>СФН 22</small>)
			Пользователь СКЗИ (ФИО полностью)
			Тип используемого СКЗИ
			Серийный номер СКЗИ
			Автоматизированная/информационная система
			Учетный/серийный номер системного блока АРМ на
			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
			Рег. номер лицевого счета / <small>ЖПЧ</small>
			Дата регистрации лицевого счета / <small>ЖПЧ</small>
			Рег. номер Приказа о лицах допускаемых к
			Дата регистрации Приказа о лицах, допускаемых к <small>работе с</small>
			Рег. номер Приказа о предоставлении прав подписей
			Дата регистрации Приказа о предоставлении прав подписей <small>в программах/системах</small>
			Заключение о возможности эксплуатации СКЗИ
			Примечание

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		

- ЛИСТ -

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

№ 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 дей-ствие	Дата вы-вода из дей-ствия	Отметка об уничтожении СКЗИ, ключевых документов		При-мечание
				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 разос-ланы (переда-ны)	Дата и номер сопроводительного письма	Дата и номер под-тверж-дения или распис-ка в по-луче-нии	Дата и номер сопроводительного письма	Дата и номер под-твер-ждения			Дата унич-тоже-ния	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 _____

уполномочивает _____ (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

Общий центр обслуживания Госкорпорации «Росатом»



ГРИНАТОМ

АО «Гринатом»
115230, Москва
1-й Нагатинский проезд, д.10, стр.1
+7 499 949 49 19
info@greenatom.ru
www.greenatom.ru

«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. № _____ - _____ от
____.____.____)

Исп.:

Тел.:

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 распiska в получении	Ф.И.О. сотрудника в органа криптографической защиты, пользователей СКЗИ, производивших подключение (установку)	Дата подключения (установки) подписи лиц, производивших 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 распiska 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
2017 г.

Оглавление

1. Общие положения	3
2. Требования к размещению технических средств установленными СКЗИ	3
3. Требования к программному и аппаратному обеспечению	3
4. Защита информации от НСД	4

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;
 - несанкционированно 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 BIOS 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 №17. Акт готовности СКЗИ к эксплуатации

Акт № _____

готовности СКЗИ « _____ » версии _____ к эксплуатации
(наименование СКЗИ)

г. _____ « ____ » _____ 20 ____ г.

Администратор безопасности _____ ,
(Фамилия И.О., e-mail)

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

(Наименование организации, фактический адрес)

к эксплуатации СКЗИ на соответствие Отраслевым требованиям по информационной безопасности №1/910-П-дсп от 23.09.2014 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.

Контроль	Выполнено/не выполнено, подпись
Установлено сертифицированное антивирусное ПО: _____ <small>(наименование/версия)</small>	_____ <small>(подпись)</small>
Установлено сертифицированное СЗИ от НСД: _____ <small>(наименование/версия)</small> ОС настроена в соответствии с отраслевыми требованиями по информационной безопасности №1/910-П-дсп от 23.09.2014	_____ <small>(подпись)</small>
Установлено СКЗИ в соответствии с документацией, поставляемой в комплекте. Проверено выполнение требований документа «Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ»	_____ <small>(подпись)</small>

СКЗИ « _____ » версии _____ установлено:

№ п/п	№ помещения и рабочего места	Уч. № ПЭВМ	ПЭВМ опечатана печатью №	Операционная система

Вывод:

Оборудование АРМ соответствует Отраслевым требованиям по информационной безопасности №1/910-П-дсп от 23.09.2014 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 « _____ » версии « _____ » .
(Наименование СКЗИ)

_____/_____
(подпись) (Ф.И.О.)

Управление информационной безопасности



ГРИНАТОМ

Обучение пользователей правилам работы со средствами криптографической защиты информации

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.

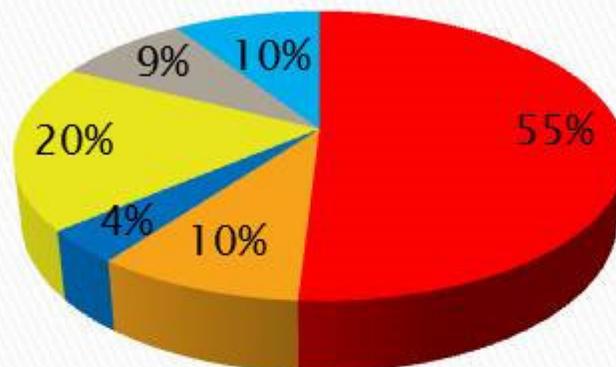
У компании «Гринатом» 6 ценностей:

- ✓ **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.



Влияние осведомленности пользователей на уровень информационной безопасности



- Ошибки персонала
- Вирусы
- Обиженные сотрудники
- Нечестные сотрудники
- Проблемы электропитания
- 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 принятие 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 (технологических 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, установка 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)



GRINATOM

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, простой 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



Типичные причины нарушений пользователей

- Использование нелегального программного обеспечения

Действие:

использование нелегального 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 непроизводительных 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 ловушки 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



GRINATOM

Приказ от 16.04.2014 №1/375-П



РОСАТОМ

п. 3.1.9 Средства вычислительной техники предоставляемые работнику для выполнения служебных обязанностей не предназначены для хранения и обработки личной информации

п. 4.2 Пользователь обязан:

- ▶ п. 4.2.1: Использовать ИРС только в целях исполнения своих должностных обязанностей;

п. 4.3 Пользователю запрещается:

- ▶ п. 4.3.9: Использовать предоставленные в пользование средства вычислительной техники и ИРС для хранения и обработки информации, не имеющей отношения к выполнению своих должностных или иных обязанностей.



РОСАТОМ

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 с 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.



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;
- ▶ Установка 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



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 BIOS 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.



Приказ от 09 февраля 2005 г. № 66

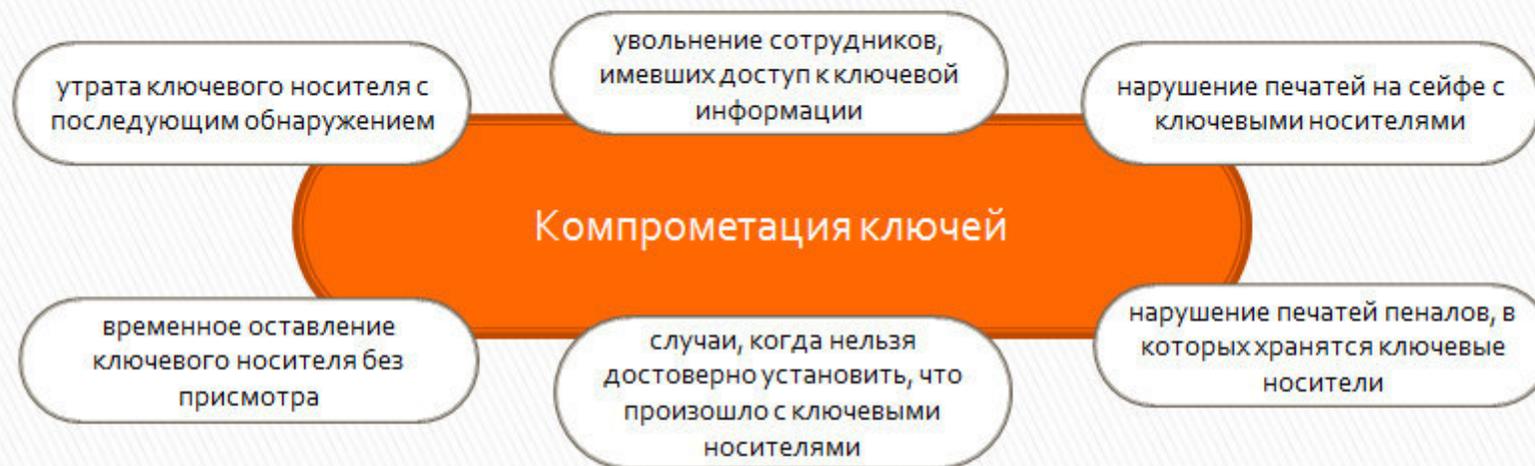


пп. 46 СКЗИ эксплуатируются в соответствии с правилами пользования ими...

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.





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 16.04.2014 №1/375-П
 п. 4.3 Пользователю запрещается:
п. 4.3.8 Оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты от несанкционированного доступа

Заблокировать компьютер:



или
Ctrl-Alt-Del + Enter



GRINATOM

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
специальными

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 16.04.2014 №1/375-П



РОСАТОМ

п.3.1.10 С целью соблюдения принципа персональной ответственности за свои действия, каждому пользователю, допущенному к работе с конкретным ИРС, используется индивидуальный уникальный идентификатор (учетная запись) и пароль, а в отдельных случаях – закрытый ключ аутентификации пользователя и его сертификат открытого ключа. Индивидуальный пароль служит для проверки подлинности (аутентификации) пользователя при доступе к ИРС и должен сохраняться им в тайне. Определенной категории работников, в случае производственной необходимости, могут быть присвоены несколько уникальных имен (учетных записей). Использование при работе несколькими пользователями одного и того же имени пользователя («группового имени») запрещено.



ГРИНАТОМ

Ответственность пользователя СКЗИ за разглашение конфиденциальной информации

Трудовой кодекс РФ

ст.81 ТК РФ
Расторжение трудового договора по инициативе работодателя

Кодекс РФ об административных правонарушениях

ст.13.14 КОАП РФ
Наложение адм. штрафа от **500 до 1000 руб.** (на граждан) и от **4000 до 5000 руб.** (на должностных лиц)

Уголовный кодекс РФ

ст.183 п.2 УК РФ
Наказывается штрафом в размере до **1 млн. руб.** или лишением свободы сроком до **трех лет**



Ответственность организации

Кодекс РФ об административных правонарушениях

ст.13.11-13.14 КОАП РФ
Штраф до 25 000 руб. с конфискацией,
приостановление деятельности
организации на срок до 90 суток

Уголовный кодекс РФ

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__ г¹

Начальник отдела
криптографической защиты
АО «Гринатом»

М.П.

_____/_____
(подпись) (ФИО)

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.

ПОРЯДОК

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

Оглавление

1. Назначение и область применения.....	3
2. Термины, определения и сокращения.....	3
3. Порядок работ	4
3.1. Организация Расследования	4
3.2. Порядок формирования Комиссии	4
3.3. Порядок работы Комиссии	4
3.4. Оформление и учет материалов расследования, организация устранения причин нарушения условий использования СКЗИ	6
4. Нормативные ссылки	8
5. Внесение изменений в Порядок	9
6. Контроль и ответственность	9
Приложение №1. Форма Приказа о проведении Расследования	10
Приложение №2. Форма заключения по результатам Расследования	11
Приложение №3. Форма плана работы Комиссии	134
Приложение №4. Форма описи документов	135

1. Назначение и область применения

Настоящий Порядок проведения расследований² 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 Регламента 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» (далее – Регламент ОКЗ).

3. Порядок работ

² 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.

3.1. 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 командированы в ООКИ, в которой произошло подлежащее Расследованию нарушение 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, имени, 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 Регламенту 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 отчетов 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

<ДОЛЖНОСТЬ ПРЕДСЕДАТЕЛЯ
КОМИССИИ (РУКОВОДИТЕЛЯ
ОКЗ), НАИМЕНОВАНИЕ
ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

«__» _____ 20__ г.

ОЗНАКОМЛЕН

<ДОЛЖНОСТЬ
РУКОВОДИТЕЛЯ УПРАВЛЕНИЯ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
АО «ГРИНАТОМ»>

_____/_____
(подпись) (Ф.И.О)

«__» _____ 20__ г.

ЗАКЛЮЧЕНИЕ

**комиссии Органа криптографической защиты АО «Гринатом»
по результатам расследования фактов
нарушения условий использования СКЗИ в
<ПОЛНОЕ 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.

ОЗНАКОМЛЕН

<ДОЛЖНОСТЬ
РУКОВОДИТЕЛЯ ООКИ>

_____/_____
(подпись) (Ф.И.О)

«__» _____ 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, устанавливающих 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»

Председатель Комиссии

(подпись) / (Ф.И.О)

(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, устанавливающих СКЗИ носителей, эксплуатационной и технической документации.

Члены комиссии:

_____/_____
(подпись) (Ф.И.О)

_____/_____
(подпись) (Ф.И.О)



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

Общий центр обслуживания Госкорпорации «Росатом»



ГРИНАТОМ

АО «Гринатом»
115230, Москва
1-й Нагатинский проезд, д.10, стр.1
+7 499 949 49 19
info@greenatom.ru
www.greenatom.ru

«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	
<p>Приказ о назначении администраторов безопасности и лиц, их замещающих (далее – Приказ):</p> <ul style="list-style-type: none"> – 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. 	
<p>Уровень квалификации администратора безопасности для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ:</p> <ul style="list-style-type: none"> – 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	
<p>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:</p> <ul style="list-style-type: none"> – 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; 	

<ul style="list-style-type: none"> – 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 	
<ul style="list-style-type: none"> – Металлические хранилища для хранения ключевых документов, эксплуатационной и технической документации, устанавливающих 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; 	

<ul style="list-style-type: none"> – 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 	
<ul style="list-style-type: none"> – 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 	
<ul style="list-style-type: none"> – Документация ОКЗ 	
<ul style="list-style-type: none"> – Наличие утвержденного перечня лиц, допускаемых к самостоятельной работе с СКЗИ и его актуальность 	
<ul style="list-style-type: none"> – 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	
<p>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:</p> <ul style="list-style-type: none"> – 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; 	

<ul style="list-style-type: none"> – 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. 	
<p>Шкафы (ящики, хранилища) индивидуального пользования:</p> <ul style="list-style-type: none"> – 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 	
<p>Окна спецпомещений пользователей СКЗИ:</p> <ul style="list-style-type: none"> – 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 	

<p>последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения пользователей СКЗИ посторонних лиц;</p> <p>– наличие на окнах спецпомещений пользователей СКЗИ приспособлений для предотвращения просмотра извне спецпомещений пользователей СКЗИ</p>	
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 учетной 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 регламента 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».

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, устанавливающих 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. Заключение 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: <ul style="list-style-type: none"> • выписка из Схемы организации криптографической защиты конфиденциальной информации; • выписка из Центра Регистрации Удостоверяющего центра Госкорпорации «Росатом». Уточнение перечня объектов, подлежащих проверке: <ul style="list-style-type: none"> • перечень СКЗИ; • перечень сертификатов ключей проверки электронной подписи. 	
1.2.	Подготовка сводной таблицы по объекту проверки.	
2	Проведение проверки	
2.1	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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
(п. ____, ____ Перечня ДСП)
Экз № ____

УТВЕРЖДАЮ

ОЗНАКОМЛЕН

<ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ
ПРОВЕРКИ, НАИМЕНОВАНИЕ
ОРГАНИЗАЦИИ>

<ДОЛЖНОСТЬ
УПОЛНОМОЧЕННОГО ЛИЦА,
НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

_____/_____
(подпись) (Ф.И.О)

«__» _____ 20__ г.

«__» _____ 20__ г.

АКТ

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

<Наименование организации>

СОГЛАСОВАНО

СОГЛАСОВАНО

<ДОЛЖНОСТЬ ЧЛЕНА КОМИССИИ,
НАИМЕНОВАНИЕ
ОРГАНИЗАЦИИ>

<ДОЛЖНОСТЬ ЧЛЕНА КОМИССИИ,
НАИМЕНОВАНИЕ
ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

_____/_____
(подпись) (Ф.И.О)

«__» _____ 20__ г.

«__» _____ 20__ г.

В соответствии с Приказом АО «Гринатом»³ 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.

³ 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. |
| | Обеспечение безопасности информации с | |
| 2. CLB.18 | 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)

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:



От Исполнителя:
Заместитель директора по
информационным технологиям
АО «Гринатом»

(Handwritten signature)
С.Н. Данилов

(по дов. № 22/309/2018-ДОВ от 28.12.18)

Перечень и стоимость услуг Исполнителя

г. Москва

« 01 » декабря 2019 года

Стоимость Услуг, оказываемых Исполнителем по настоящему Договору, составляет:

№	Код вида Услуги	Наименование вида Услуги	Стоимость Услуги с НДС, руб.	В том числе НДС, руб.
1.	CLB.11 (УКЭП)	Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ЭП	4 364,44 единовременно за один сертификат	727,41
2.	CLB.11 (УНЭП)	Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском неквалифицированного сертификата ЭП	4 053,84 единовременно за один сертификат	675,64
3.	CLB.18 (КриптоПро CSP клиентская)	Обеспечение безопасности информации с использованием средств криптографической защиты информации (СКЗИ «КриптоПро CSP» клиентская лицензия в собственности АО «Гринатом»)	1 097,68 в квартал за одно СКЗИ	182,95

4.	CLB.18 (КриптоПро CSP серверная)	Обеспечение безопасности информации с использованием средств криптографической защиты информации (СКЗИ «КриптоПро CSP» серверная лицензия в собственности АО «Гринатом»)	4 283,64 в квартал за одно СКЗИ	713,94
5.	CLB.18 (S-Terra CSP VPN Client)	Обеспечение безопасности информации с использованием средств криптографической защиты информации (СКЗИ «S-Terra CSP VPN Client» в собственности АО «Гринатом»)	1 679,98 в квартал за одно СКЗИ	280,00
6.	CLB.18 (ViPNet Client)	Обеспечение безопасности информации с использованием средств криптографической защиты информации (СКЗИ «ViPNet Client» в собственности АО «Гринатом»)	1 176,37 в квартал за одно СКЗИ	196,06
7.	CLB.18 (СКЗИ заказчика)	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 (СКЗИ – собственность Заказчика)	844,38 в квартал за одно СКЗИ	140,73
8.	GEN.23 (Москва)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом»	3 034,51 в квартал за одно рабочее место с СКЗИ	505,75
9.	GEN.23 (Ангарск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Ангарск	1 424,88 в квартал за одно рабочее место с СКЗИ	237,48

10.	GEN.23 (Владимир)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Владимир	485,50 в квартал за одно рабочее место с СКЗИ	80,92
11.	GEN.23 (Глазов)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Глазов	828,50 в квартал за одно рабочее место с СКЗИ	138,08
12.	GEN.23 (Дмитровград)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Дмитровград	839,09 в квартал за одно рабочее место с СКЗИ	139,85
13.	GEN.23 (Зеленогорск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Зеленогорск	1 292,94 в квартал за одно рабочее место с СКЗИ	215,49
14.	GEN.23 (Ковров)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Ковров	538,27 в квартал за одно рабочее место с СКЗИ	89,71
15.	GEN.23 (Нижний Новгород)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Нижний Новгород	1 372,10 в квартал за одно рабочее место с СКЗИ	228,68

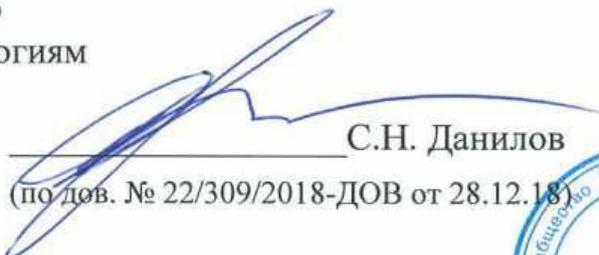
16.	GEN.23 (Новосибирск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Новосибирск	1 066,00 в квартал за одно рабочее место с СКЗИ	177,67
17.	GEN.23 (Новоуральск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Новоуральск	997,38 в квартал за одно рабочее место с СКЗИ	166,23
18.	GEN.23 (Подольск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Подольск	1 176,80 в квартал за одно рабочее место с СКЗИ	196,13
19.	GEN.23 (Санкт-Петербург)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Санкт-Петербург	1 197,94 в квартал за одно рабочее место с СКЗИ	199,66
20.	GEN.23 (Саров)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Саров	2 522,59 в квартал за одно рабочее место с СКЗИ	420,43
21.	GEN.23 (Северск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Северск	1 108,19 в квартал за одно рабочее место с СКЗИ	184,70

22.	GEN.23 (Электросталь)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Электросталь	1 029,06 в квартал за одно рабочее место с СКЗИ	171,51
23.	GEN.23 (Мурманск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Мурманск	2 360,45 в квартал за одно рабочее место с СКЗИ	393,41
24.	GEN.23 (Краснокаменск)	Услуга Администратора безопасности Органа криптографической защиты АО «Гринатом» в городе Краснокаменск	1 158,55 в квартал за одно рабочее место с СКЗИ	193,09
25.	CLB.21 (серверная часть системы)	Контроль (оценка) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем (если уровень доверия к серверной части Системы ранее не определен)	32 541,66 в квартал за одну информационную систему	5 423,61
26	CLB.21 (клиентская часть системы)	Контроль (оценка) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем (если уровень доверия к серверной части Системы определен ранее)	13 262,08 в квартал за одну информационную систему	2 210,35

27	CLB.26	Подключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»	1 406,81 в квартал за один абонентский пункт	234,47
----	--------	---	--	--------

От Исполнителя:

Заместитель директора по
информационным технологиям
АО «Гринатом»


С.Н. Данилов
(по дов. № 22/309/2018-ДОВ от 28.12.18)



Приложение №6
к Договору присоединения № 22/2143-Д от 06 июля 2012 г.

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



С.Н. Данилов
(по дов. № 22/309/2018-ДОВ от 28.12.18)

Регламент процесса

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

Редакция №1

Москва 2019 г.

ОГЛАВЛЕНИЕ

1. Назначение и область применения.....	3
2. Термины, определения и сокращения.....	5
3. Описание процесса.....	7
3.1. Цель процесса.....	8
3.2. Задачи процесса.....	8
3.3. Участники группы процессов и их роли.....	8
3.4. Основные выходы процесса.....	9
3.5. Основные входы процесса.....	11
3.6. Описание процесса.....	12
4. Нормативные ссылки.....	15
5. Порядок внесения изменений.....	16
6. Контроль и ответственность.....	17
7. Перечень приложений.....	17
Приложение №1. Матрица ответственности.....	18
Приложение №2. Схема процесса.....	20
Приложение №3. Дополнительные выходы и дополнительные входы.....	21
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.....	22
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.....	23
Приложение №6. Форма Заключения Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе.....	25

1. Назначение и область применения

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

Настоящий Регламент 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». Регламент имеет статус локального.

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

Документ	Статус	Тип документа	Ответственный
Лицензия ФСБ России ЛСЗ №0014254 Рег.№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	Данилов С.Н.

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	Данилов С.Н.
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	Данилов С.Н.
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	Данилов С.Н.
Отраслевые требования по информационной безопасности Госкорпорации «Росатом» №1/910-П-дсп от 23.09.2014	Действует	Требование	Данилов С.Н.

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;

	<p>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;</p> <p>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.</p>
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

- выявление рисков информационной безопасности при заключении договоров на эксплуатацию Систем;
- 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	<ul style="list-style-type: none"> • выявляет риски информационной безопасности при заключении договоров на эксплуатацию Систем; • 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»	<ul style="list-style-type: none"> • 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 (Корпораци я / Дивизион/ Организаци я)
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

	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 (доп. соглашений) на Системы	ООКИ	Организация
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 Требованиям к средствам удостоверяющего центра»));
- документацию о наличии дополнительных служб удостоверяющего центра (службы онлайн-овой 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, используемые 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);
- Отраслевые требования по информационной безопасности Госкорпорации «Росатом» безопасности №1/910-П-дсп от 23.09.2014;
- Постановление №313 от 16.04.2012 г. Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- Единые отраслевые методические указания по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утв. Приказом от 22.10.2015 №1/1009-П.

5. Порядок внесения изменений

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

6. Контроль и ответственность

6.1 Регламент обязаны соблюдать все следующие участники процесса

Руководитель ОКЗ;
Проверяющий.

6.2. Ответственность работников за несоблюдение требований Регламента

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

7. Перечень приложений

Приложение №1.	Матрица ответственности.
Приложение №2.	Схема процесса.
Приложение №3.	Дополнительные выходы и дополнительные входы.
Приложение №4.	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 №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

(нужное подчеркнуть)

« _____ » _____ 201__ г.

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.

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	Общесистемное программное обеспечение, установленное на АРМ

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

Общий центр обслуживания Госкорпорации «Росатом»



ГРИНАТОМ

АО «Гринатом»
115230, Москва
1-й Нагатинский проезд, д.10, стр.1
+7 499 949 49 19
info@greenatom.ru
www.greenatom.ru

«ДОЛЖНОСТЬ
УПОЛНОМОЧЕННОГО ЛИЦА»
«НАИМЕНОВАНИЕ
ОРГАНИЗАЦИИ»

«И.О.ФАМИЛИЯ»

от _____ № _____
На № _____ от _____

О передаче СКЗИ

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 OSCP (документацию на службу онлайн-проверки статусов сертификатов и службы штампов времени);
копию документации о поддержке формата усовершенствованной подписи;
копию сертификата соответствия ФСБ России на средства криптографической защиты информации, используемые 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 приведения 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**



АКЦИОНЕРНОЕ ОБЩЕСТВО «ГРИНАТОМ»

Лицензия ФСБ России рег. ЛСЗ № 0014254 Рег. №15686 Н
от 19 января 2017 года.

СОГЛАСОВАНО

УТВЕРЖДАЮ

<ДОЛЖНОСТЬ ПРОВЕРЯЮЩЕГО>

<ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ
ОРГАНА КРИПТОГРАФИЧЕСКОЙ
ЗАЩИТЫ>

_____/_____
(подпись) (Ф.И.О)

_____/_____
(подпись) (Ф.И.О)

«__» _____ 20__ г.

«__» _____ 20__ г.

М.П.

**ЗАКЛЮЧЕНИЕ
ОРГАНА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ
АО «ГРИНАТОМ»**

по результатам оценки уровня доверия к защищенной с использованием
шифровальных (криптографических) средств
«НАИМЕНОВАНИЕ СИСТЕМЫ»

Москва

20__ г.

1. ВВОДНАЯ ЧАСТЬ

1.1. Основание для исследования

Заявление от ... г. на контроль (оценку) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

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

Наименование Системы

1.3. Вопросы для исследования

1.3.1. Исследование договора на эксплуатацию «НАИМЕНОВАНИЕ СИСТЕМЫ» между организацией-обладателем конфиденциальной информации и Банком на наличие рисков информационной безопасности;

1.3.2. Наличие в договоре рисков для клиента в области информационной безопасности;

1.3.3. Юридическая значимость документов в «НАИМЕНОВАНИЕ СИСТЕМЫ»;

1.3.4. Доверие криптографическим сервисам «НАИМЕНОВАНИЕ СИСТЕМЫ»;

1.3.5. Доверия к СФК, средствам обработки и отображения данных;

1.3.6. Доверие к технологии, реализующей инфраструктуру ключевой системы;

1.3.7. Доверие к участникам процессов обработки данных.

2. ИССЛЕДОВАТЕЛЬСКАЯ ЧАСТЬ

2.1. Материально-технические средства (приборы, оборудование и пр.), применяемые при подготовке заключения

- Программное обеспечение;
- Средства защиты информации;
- Средства криптографической защиты информации;
- Проект договора/подписанный договор на «НАИМЕНОВАНИЕ СИСТЕМЫ»;
- Лицензии на лицензируемые виды деятельности;
- Сертификаты соответствия;
- Свидетельства об аккредитации;
- Эксплуатационная документация.
- Локальные нормативные акты

2.2. Нормативная и справочная документация

- [1] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
- [2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- [3] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- [4] Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями).
- [5] Федеральный закон от 04.05.2011 № 99-ФЗ (ред. от 21.07.2014) «О лицензировании отдельных видов деятельности» (04.05.2011).
- [6] Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» (в редакции постановления Правительства Российской Федерации от 20.07.2012 № 740).
- [7] Постановление Правительства Российской Федерации от 15.05.2010 № 330 «Об утверждении Положения об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов её проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения».
- [8] Постановление Правительства Российской Федерации от 03.02.2012 № 79 «Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации».
- [9] Постановление Правительства Российской Федерации от 16.04.2012 № 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)»;
- [10] Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- [11] ГОСТ Р ИСО 15489-1—2007 Управление документами. Общие требования.

- [12] Национальный стандарт Российской Федерации ограниченного распространения ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».
- [13] «Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждённое Председателем Гостехкомиссии России 25.11.1994.
- [14] «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждённые приказом Гостехкомиссии России от 30.08.2002 № 282.
- [15] «Методические рекомендации по технической защите информации, составляющей коммерческую тайну», утверждённые заместителем директора ФСТЭК России 25.12.2006.
- [16] «Пособие по организации технической защиты информации, составляющей коммерческую тайну», утверждённое заместителем директора ФСТЭК России 25.12.2006.
- [17] Приказ ФАПСИ 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».
- [18] Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- [19] Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Составы 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».
- [20] Приказ Госкорпорации «Росатом» от 28.03.2011 № 1/238-П «Об утверждении Единой политики защиты коммерческой тайны в атомной отрасли».
- [21] Приказ Госкорпорации «Росатом» от 20.06.2012 № 1/540-П «Об оценке видов информации ограниченного доступа при создании, модернизации и эксплуатации автоматизированных систем в защищённом исполнении и прикладных информационных систем».
- [22] Приказ Госкорпорации «Росатом» от 23.09.2014 № 1/910-П-дсп. «Об утверждении Отраслевых требований по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию, составляющую коммерческую тайну, служебную информацию ограниченного распространения (с пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации «Росатом» и её организациях».
- [23] Приказ Госкорпорации «Росатом» от 13.10.2015 № 1/978-П «Об утверждении Единых отраслевых методических указаний по управлению расчётно-кассовым обслуживанием в Госкорпорации «Росатом» и её организациях».

- [24] Приказ Госкорпорации «Росатом» от 22.10.2015 №1/1009-П «Об утверждении Единых отраслевых методических указаний по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях.

2.3. Методы исследования

- Анализ представленной в ответ на запрос от «___» _____ 20__ г. документации;
- Изучение и обобщение информации в представленной документации на «НАИМЕНОВАНИЕ СИСТЕМЫ».
- Опрос специалистов АО «Гринатом»;

2.4. Риски для клиента в области информационной безопасности в договоре

2.5. Результаты исследований на предмет юридической значимости документов в «НАИМЕНОВАНИЕ СИСТЕМЫ»

2.6. Результаты исследований на предмет доверия криптографическим сервисам «НАИМЕНОВАНИЕ СИСТЕМЫ»

Критерий оценки	Наличие	Срок действия	Номер	Приложение №
Используются средства криптографической защиты информации				
Сертификаты соответствия ФСБ России на средства криптографической защиты информации с актуальным сроком действия				
Документация на СКЗИ				
СКЗИ соответствует «Требованиям к средствам электронной подписи» (приложение № 1 к приказу ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»)				
Соответствуют требованиям ГОСТ 28147-89				
Соответствуют требованиям ГОСТ Р 34.11-94				
Соответствуют требованиям ГОСТ Р 34.11-2012				
Соответствуют требованиям ГОСТ Р 34.10-2001				

Соответствуют требованиям ГОСТ Р 34.10-2012				
Класс защиты применяемых шифровальных (криптографических) средств не менее КС1				
Класс защиты применяемых шифровальных (криптографических) средств не менее КС2				
Используются сертифицированные ключевые носители				
Используются ключевые носители типа Токен или Смарт-карты				
Используются ключевые носители типа Сменный Flash-носитель или Жесткий диск ПЭВМ				

2.7. Результаты исследований на предмет доверия к СФК, средствам обработки и отображения данных

Критерий оценки	Наличие	Срок действия	Номер	Приложение №
Защита информации производится средствами операционной системы				
Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ				
Копия формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника)				
Заключение о корректности встраивания СКЗИ в «НАИМЕНОВАНИЕ СИСТЕМЫ»				
Документация на систему ДБО				
Зафиксирована версия Программного обеспечения «НАИМЕНОВАНИЕ СИСТЕМЫ» и ОС				
Наличие аттестата соответствия на соответствие требованиям по информационной безопасности				
Используется сертифицированное антивирусное ПО				
Установлено сертифицированное СЗИ от НСД				
Сертификат соответствия ФСБ на СПДС				
Аттестат соответствия ФСТЭК на АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация				

2.8. Результаты исследований на предмет доверия к технологии, реализующей инфраструктуру ключевой системы

Критерий оценки	Наличие	Срок действия	Номер	Приложение №
-----------------	---------	---------------	-------	--------------

Лицензия ФСБ России на соответствующие виды деятельности				
Лицензия на программное обеспечение				
Средство, реализующие инфраструктуру ключевой системы сертифицировано в соответствии с системой сертификации РОСС RU.0001.030001 по классу КС2				
Средство, реализующие инфраструктуру ключевой системы сертифицировано в соответствии с системой сертификации РОСС RU.0001.030001 по классу КС3				
Документация на СКЗИ				
Документы, регламентирующие жизненный цикл ключевой системы				
Свидетельство об аккредитации				
Документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации)				
Средство автоматизации удостоверяющего центра 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 Требованиям к средствам удостоверяющего центра»)				
Наличие дополнительных служб удостоверяющего центра (службы онлайн-проверки статусов сертификатов и службы штампов времени)				
Поддержка формата усовершенствованной подписи				

2.9. Результаты исследований на предмет доверия к участникам процессов обработки данных

Критерий оценки	Наличие	Срок действия	Номер	Приложение №
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				

3. ВЫВОДЫ И РЕКОМЕНДАЦИИ

«НАИМЕНОВАНИЕ СИСТЕМЫ» обеспечивает _____ уровень доверия к криптографическим сервисам.

Приложение:

Приложение №1. Лицензия ФСБ России на соответствующие виды деятельности.

Приложение №2. Лицензия на программное обеспечение.

Приложение №3. Сертификаты соответствия в соответствии с системой сертификации РОСС RU.0001.030001 по классу КС2 или КС3 на средство, реализующем инфраструктуру ключевой системы.

Приложение №4. Документация на СКЗИ (копия формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника)).

Приложение №5. Документация, регламентирующая жизненный цикл ключевой системы;

Приложение №6. Свидетельство об аккредитации.

Приложение №7. Документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации).

Приложение №8. 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»)).

Приложение №9. Документация о наличии дополнительных служб удостоверяющего центра (службы онлайн-овой проверки статусов сертификатов и службы штампов времени).

Приложение №10. Документация о поддержке формата усовершенствованной подписи.

Приложение №11. Сертификаты соответствия ФСБ России на средства криптографической защиты информации, использующиеся в Системе (класс защиты применяемых шифровальных (криптографических) средств).

Приложение №12. Документация на СКЗИ (копия формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника)).

Приложение №13. Сертификаты соответствия на ключевые носители.

Приложение №14. 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.

Приложение №15. Локальные нормативные акты, определяющие права и роли работников в «НАИМЕНОВАНИЕ СИСТЕМЫ».

Приложение №7
к Договору присоединения № 22/2143-Д от 06 июля 2012 г.

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



С.Н. Данилов
(по дов. № 22/309/2018-ДОВ от 28.12.18)

М.П.

Регламент процесса

Организация и обслуживание защищённой сети комплекса «ViPNet-Гринатом»

Редакция №2

Москва 2019 г.

Содержание

1. Назначение и область применения.....	3
2. Термины, определения и сокращения.....	6
3. Описание процесса «Подключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»	7
3.1. Цель процесса	7
3.2. Задачи процесса	8
3.3. Участники процесса и их роли.....	8
3.4. Основные выходы процесса.....	8
3.5. Основные входы процесса.....	9
3.6. Описание подпроцессов	10
4. Описание процесса «Подключение/отключение и обслуживание ViPNet Coordinator в сети комплекса «ViPNet-Гринатом»	12
5. Описание процесса «Предоставление доступа к сетевому информационному ресурсу организации»	13
6. Нормативные ссылки.....	14
7. Порядок внесения изменений	16
8. Контроль и ответственность	16
9. Перечень приложений	16
Приложение №1. Матрица ответственности.....	17
Приложение №2. Схема процесса	18
Приложение №3. Заявление на подключение/отключение услуги	21
Приложение №4. Таблица связей в «Деловой почте» ViPNet-Гринатом.....	22
Приложение №5. Приказ о назначении ответственного и замещающих лиц по работе с абонентским пунктом ViPNet «Канцелярия»	23
Приложение №6. Заявление на установление межсетевого взаимодействия.....	24
Приложение №7. Соглашение об установлении межсетевого взаимодействия.....	25
Приложение №8. Заявление на предоставление канала связи до локальных ресурсов	31

1. Назначение и область применения

Настоящий регламент процесса Организация и обслуживание защищённой сети комплекса «ViPNet-Гринатом» (далее – Регламент), разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты (далее – ОКЗ).

Настоящий Регламент 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 Регламента 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 Регламент 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.
Единые отраслевые методические указания по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию, составляющую коммерческую тайну, служебную информацию ограниченного распространения (с	Действует	Требование	Волков С.П.

<p>пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации «Росатом» и её организациях №1/4-П-дсп от 09.01.2019</p>			
<p>Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»</p>	Действует	Требование	Волков С.П.
<p>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).</p>	Действует	Требование	Волков С.П.
<p>Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности"</p>	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 сетевому информационному ресурсу организации»
Подпроцесс:
«Организация межсетевого взаимодействия (кроссертификация)»
«Предоставление канала связи до локальных ресурсов»
«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

Термин	Определение
	независимо от их организационно-правовой формы и формы собственности, индивидуальные предприниматели и физические лица
Администратор сети ViPNet	Работник ОКЗ, осуществляющий предоставление услуги Организация и обслуживание защищённой сети комплекса «ViPNet-Гринатом»
ViPNet Coordinator (Координатор)	Универсальный сервер защищённой сети ViPNet
Кроссертификация	Организация межсетевое взаимодействие с обменом ключевой информацией и справочниками

Сокращение	Расшифровка
АБ	Администратор безопасности ОКЗ
ОКЗ	Орган криптографической защиты
Пользователь	Работник организации-обладателя конфиденциальной информации, для которого подано заявление на подключение и обслуживания Деловой почты
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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация, / Дивизион/ Организация)
2	Таблица связей в «Деловой почте» ViPNet-Гринатом - в случае, если организация вне периметра атомной отрасли	АО «Гринатом»	Организация
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 для автоматизированных систем, обрабатывающих информацию, составляющую коммерческую тайну, служебную информацию ограниченного распространения (с пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации	ГК «Росатом»	Корпорация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
	«Росатом» и её организациях №1/4-П-дсп от 09.01.2019		
2	Заявление на подключение/отключени е 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
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 Единым отраслевым методическим указаниям по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию, составляющую коммерческую тайну, служебную информацию ограниченного распространения (с пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации «Росатом» и её организациях №1/4-П-дсп от 09.01.2019;

– Направляет в адрес ОКЗ АО «Гринатом» Заявление на подключение/отключение и обслуживание защищенной электронной почты «Деловая почта» 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, согласует заполненную таблицу связей в «Деловой почте» ViPNet-Гринатом (Приложение №4) с отделом информационной безопасности департамента защиты государственной тайны и информации Госкорпорации «Росатом» (далее – ДЗГТИ).
- Создает 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.

* 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 Регламенте 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»

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 сетевому информационному ресурсу организации»

5.1 Подпроцесс «Организация межсетевого взаимодействия (кроссертификация)»

Реализуется в случае, если необходимо создать связи пользователю с абонентами внешних сетей, предоставить зашифрованный доступ к ресурсам доверенной сети.

Требуется:

- Заявление на установление межсетевого взаимодействия, Приложение №6 к Регламенту;
- Подписанное «Соглашение об установлении межсетевого взаимодействия», Приложение № 7 к Регламенту.

5.2 Подпроцесс «предоставление канала связи до локальных ресурсов»

Реализуется в случае, если необходимо предоставить зашифрованный доступ к ресурсам доверенной сети или ресурсам в сети ViPNet-Гринатом.

- Согласование межсетевого взаимодействия со смежными управлениями и владельцами ресурсов
 - Добавление связей с туннелирующим координатором
 - Добавление необходимых связей узлам
 - Взаимодействие с владельцем предоставляемых (туннелируемых) посредством сети «ViPNet-Гринатом» ресурсов
 - 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);
- Единые отраслевые методические указания по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию, составляющую коммерческую тайну, служебную информацию ограниченного распространения (с пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации «Росатом» и её организациях №1/4-П-дсп от 09.01.2019;
- 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, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

7. Порядок внесения изменений

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

8. Контроль и ответственность

8.1 Регламент обязаны соблюдать все следующие участники процесса:

- Руководитель ООКИ;
- Администратор сети ViPNet;
- Администратор ОКЗ;
- Пользователь АП.

8.2. Ответственность работников за несоблюдение требований Регламента.

За несоблюдение Регламента 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

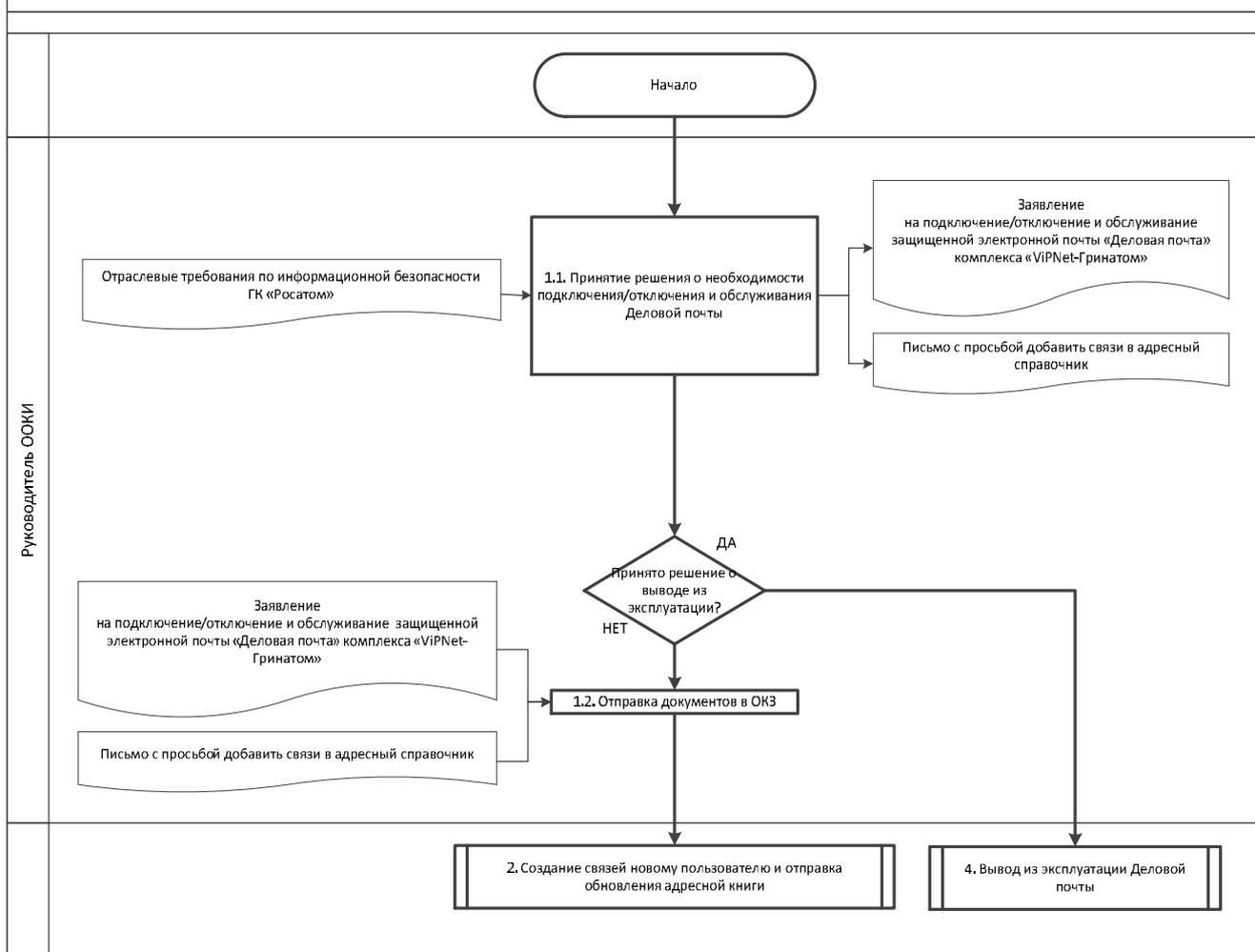
Сокращение	Название роли	Определение	Исполнитель Роли
О	Ответственный	Несет ответственность за достижение результата по подпроцессу/процедуре в своей предметной области	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
Утв	Утверждающий	Утверждает - 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

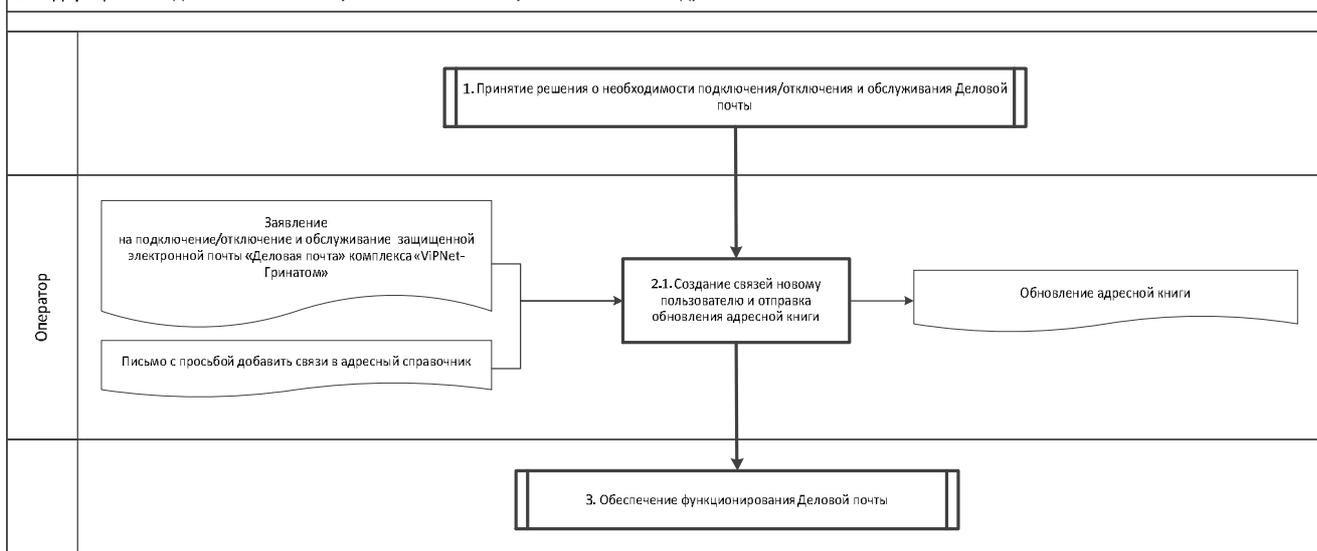
Процесс «Подключение и обслуживание защищенной электронной почты «Деловая почта» комплекса «VirNet-Гринатом»



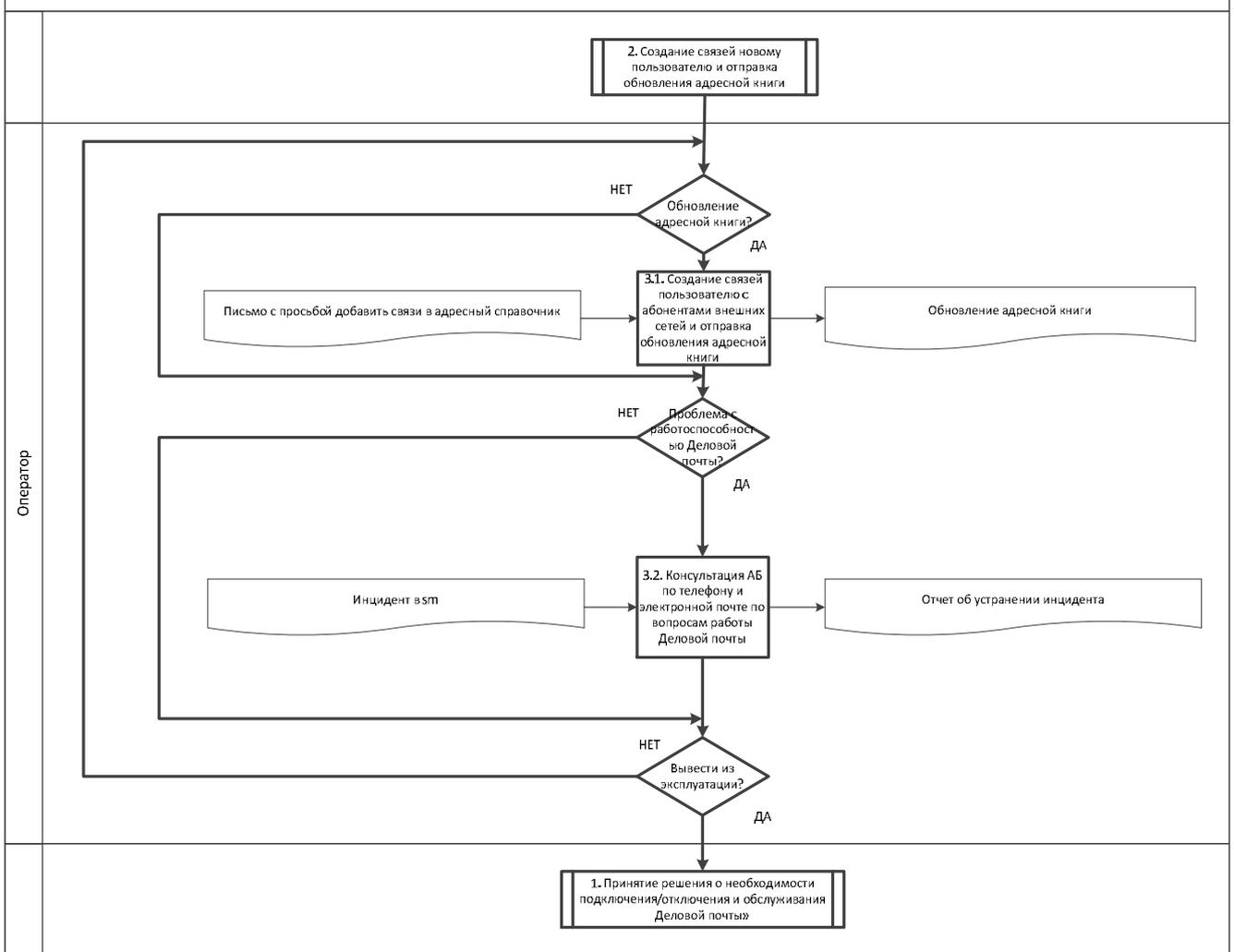
1. Подпроцесс «Принятие решения о необходимости подключения/отключения и обслуживания Деловой почты»



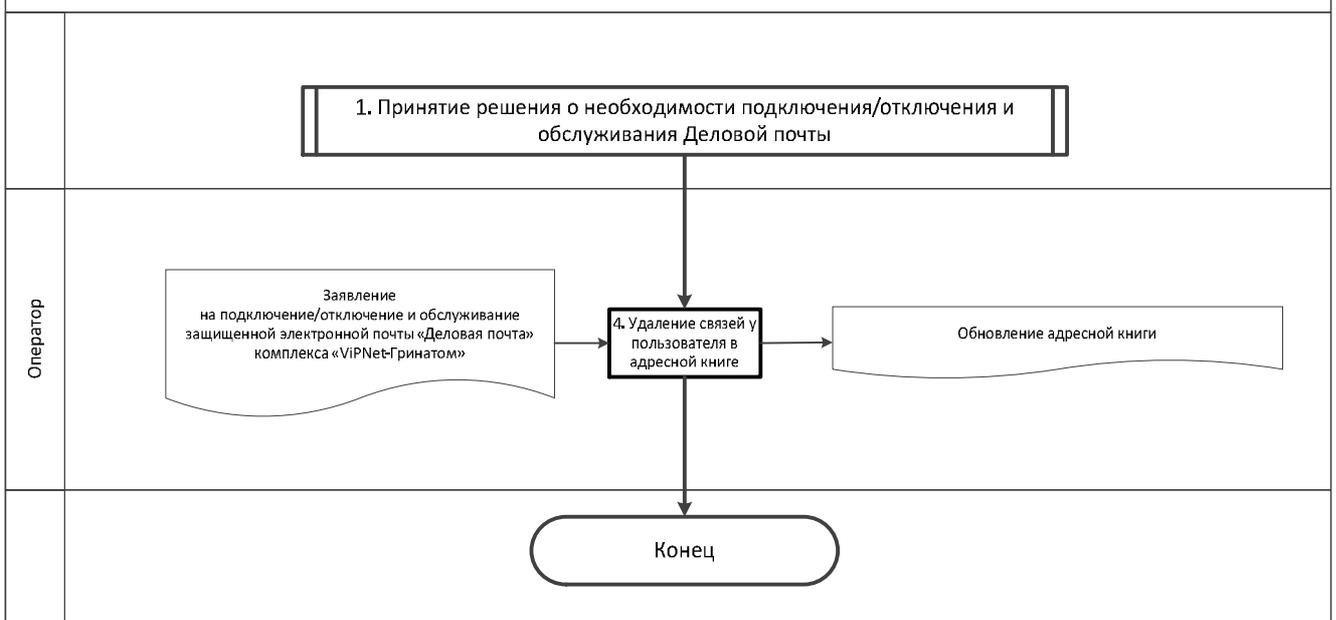
2. Подпроцесс «Создание связей новому пользователю и отправка обновления адресной книги»



3. Подпроцесс «Обеспечение функционирования Деловой почты»



4. Подпроцесс «Вывод из эксплуатации Деловой почты»



Приложение №3. Заявление на подключение/отключение услуги

Заявление на подключение и обслуживание защищенной электронной почты «Деловая почта» 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:

- подключению и обслуживанию защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом»;
- отключению от защищенной электронной почты «Деловая почта» комплекса «ViPNet-Гринатом».

№ 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)
1						
2						

(должность администратора безопасности)

(подпись)

(ФИО)

(должность уполномоченного должностного лица)

(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

(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 создается 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 срока 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»	Полное наименование:
Краткое наименование: АО «Гринатом»	Краткое наименование:
Место нахождения: 119017, Россия, Москва, ул. Большая Ордынка, д. 24	Место нахождения:
Почтовый адрес: 115230, г. Москва, 1-й Нагатинский проезд, д.10, строение 1	Почтовый адрес:
ОГРН: 1097746819720	ОГРН:
ИНН: 7706729736	ИНН:
Телефон: +7 (499) 949-49-19	Телефон:

ФИО Ответственного ДЛ

М.П.

М.П.

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, межсетевого экран и абонентские пункты.

Шлюзовой ViPNet-Координатор – сетевой узел, через который проходит весь межсетевого 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.

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 «Гринатом» (№ 11296)	АО	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 06 июля 2012 г.

У Т В Е Р Ж Д А Ю

Заместитель директора по
информационным технологиям

АО «Гринатом»



С.Н. Данилов

(по дов. № 22/309/2018-ДОВ от 28.12.18)

Регламент процесса
«Предоставление услуг
Корпоративного удостоверяющего центра Госкорпорации «Росатом»
с использованием информационной системы Органа криптографической
защиты»

Редакция № 1.0

Москва 2019 г.

Содержание

1.	Назначение и область применения.....	3
2.	Термины, определения и сокращения.....	4
3.	Описание процесса.....	6
3.1	Цель процесса	6
3.2	Задачи процесса.....	6
3.3.	Участники группы процессов и их роли.....	8
3.4	Описание подпроцессов	8
3.4.1.	Подпроцесс «Обработка обращения»	8
3.4.2.	Подпроцесс «Создание подписки на обеспечение сертификатом».....	9
3.4.3.	Подпроцесс «Корректировка подписки на обеспечение сертификатом».....	10
3.4.4.	Подпроцесс «Сокращение подписки на обеспечение сертификатом»..	11
3.4.5.	Подпроцесс «Перевыпуск сертификата».....	12
3.4.6.	Подпроцесс «Аннулирование сертификата».....	12
3.4.7.	Подпроцесс «Создание сертификата УКЭП»	13
3.4.8.	Подпроцесс «Вручение сертификата УКЭП»	13
3.4.9.	Подпроцесс «Создание сертификата УНЭП»	14
3.4.10.	Подпроцесс «Вручение сертификата УНЭП»	15
3.4.11.	Подпроцесс «Контроль действия сертификата»	15
4.	Нормативные ссылки.....	16
5.	Порядок внесения изменений	16
6.	Контроль и ответственность	16
6.1	Контроль выполнения требований Регламента	16
6.2	Ответственность работников за несоблюдение требований Регламента..	17
7.	Перечень приложений	18
	Приложение №1	19
	Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом».....	19
	1. Формат квалифицированного сертификата ключа проверки электронной подписи.....	31
	2. Формат неквалифицированного сертификата ключа проверки электронной подписи.....	32
	Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи	33
	Шаблоны сертификатов ключей проверки электронной подписи	34

1. Назначение и область применения

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

Общая информация о КУЦ:

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

Руководитель предприятия/организации;

Пользователь КУЦ;

Администратор безопасности;

Сотрудник HR;

Оператор КУЦ;

Администратор КУЦ;

Регламент распространяется в форме электронного документа по адресу:
URL= <http://crypto.rosatom.ru/dokumentatsiya/reglamenty/reglament-kuts/>

Регламент 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

2. 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

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;
- установления сроков действия сертификатов;
- аннулирования сертификатов, выданных КУЦ;
- приостановления и возобновления действия сертификатов, выданных КУЦ;
- выдачи по обращению заявителя средств ЭП, содержащих ключи ЭП и ключи проверки ЭП, созданные КУЦ;

- ведения реестра выданных и аннулированных сертификатов (далее - реестр сертификатов), в том числе включающего в себя информацию, содержащуюся в сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов и об основаниях таких прекращения или аннулирования;
- создания по обращениям заявителей ключей ЭП и ключей проверки ЭП;
- проверки уникальности ключей проверки ЭП в реестре сертификатов;
- осуществления по обращениям участников электронного взаимодействия проверки ЭП;
- информирования в письменной форме заявителей об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки;
- обеспечения актуальности информации, содержащейся в реестре сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- предоставления безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информации, содержащейся в реестре сертификатов, в том числе информации об аннулировании сертификатов ключей проверки ЭП;
- обеспечения конфиденциальности созданных КУЦ ключей ЭП;
- осуществления иной, связанной с использованием ЭП деятельности.

3.3. Участники группы процессов и их роли

№	Участники	Основные роли
1	Пользователь КУЦ	<ul style="list-style-type: none"> • Обладает учётной записью в домене ГК • Создает обращение • Получает сертификаты
2	Уполномоченное лицо предприятия	<ul style="list-style-type: none"> • Согласовывает и подписывает электронные заявки в ИС ОКЗ на создание и сокращение подписок предприятия;
3	Сотрудник HR	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Создание сертификата УКЭП • Создание сертификата УНЭП
6	Администратор КУЦ	<ul style="list-style-type: none"> • 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 ГК 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 пользователя 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 получения 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 пользователя КУЦ, в объеме, необходимом для выпуска сертификата УКЭП и регистрации его в ЕСИА. Данный шаг может быть произведен 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 подписи 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»

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 Требованиям к средствам удостоверяющего центра".

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

5. Порядок внесения изменений

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

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

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

6. Контроль и ответственность

6.1 Контроль выполнения требований Регламента

За несоблюдение Регламента 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 Регламента

За несоблюдение Регламента 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 своей предметной области
Инф	Информируемый	Получает информацию о ходе/результате подпроцесса /процедуры

7. Перечень приложений

Приложение №1. Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

Приложение № 2. Формат сертификатов ключа проверки электронной подписи

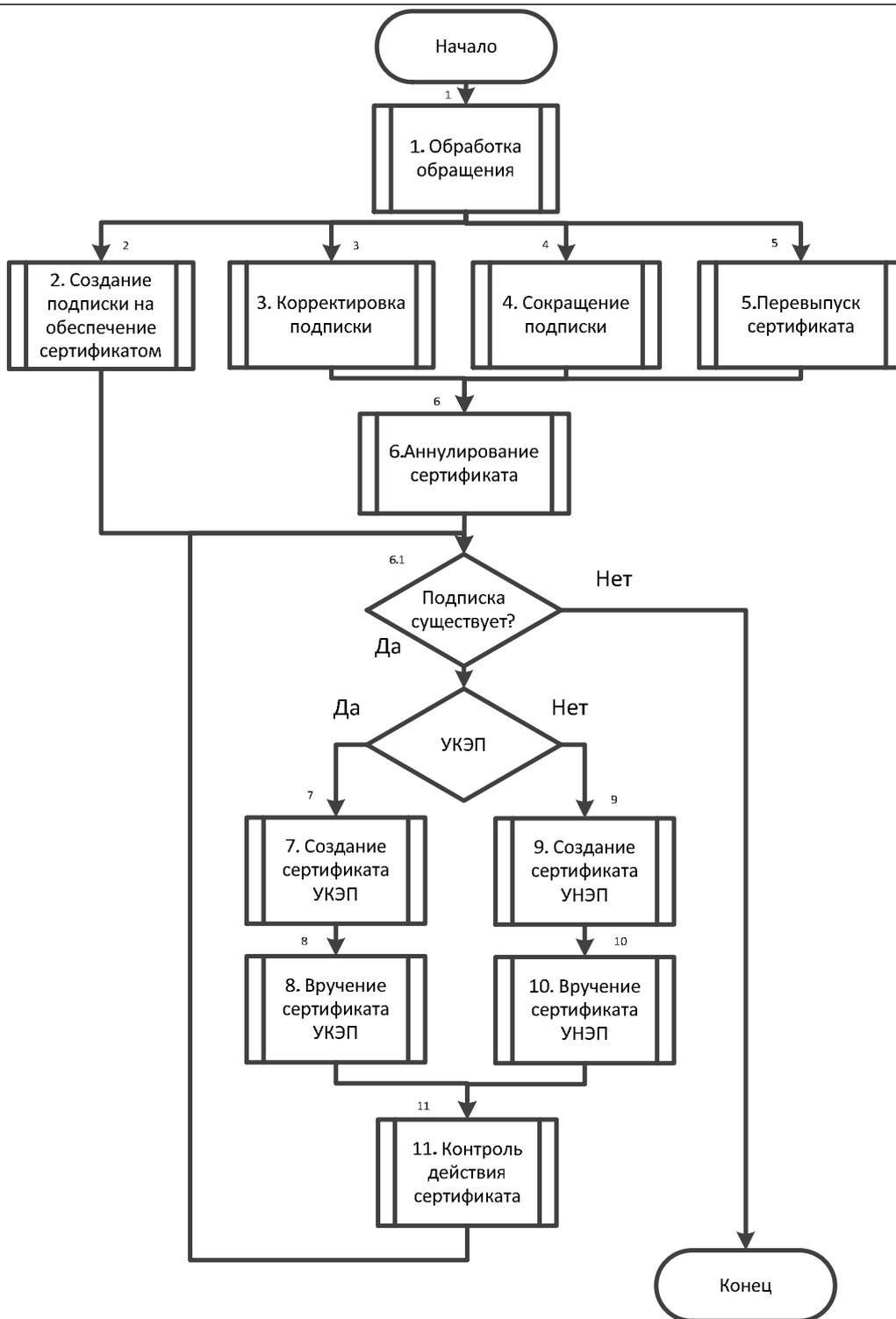
Приложение № 3. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

Приложение № 4. Шаблоны сертификатов ключей проверки электронной подписи

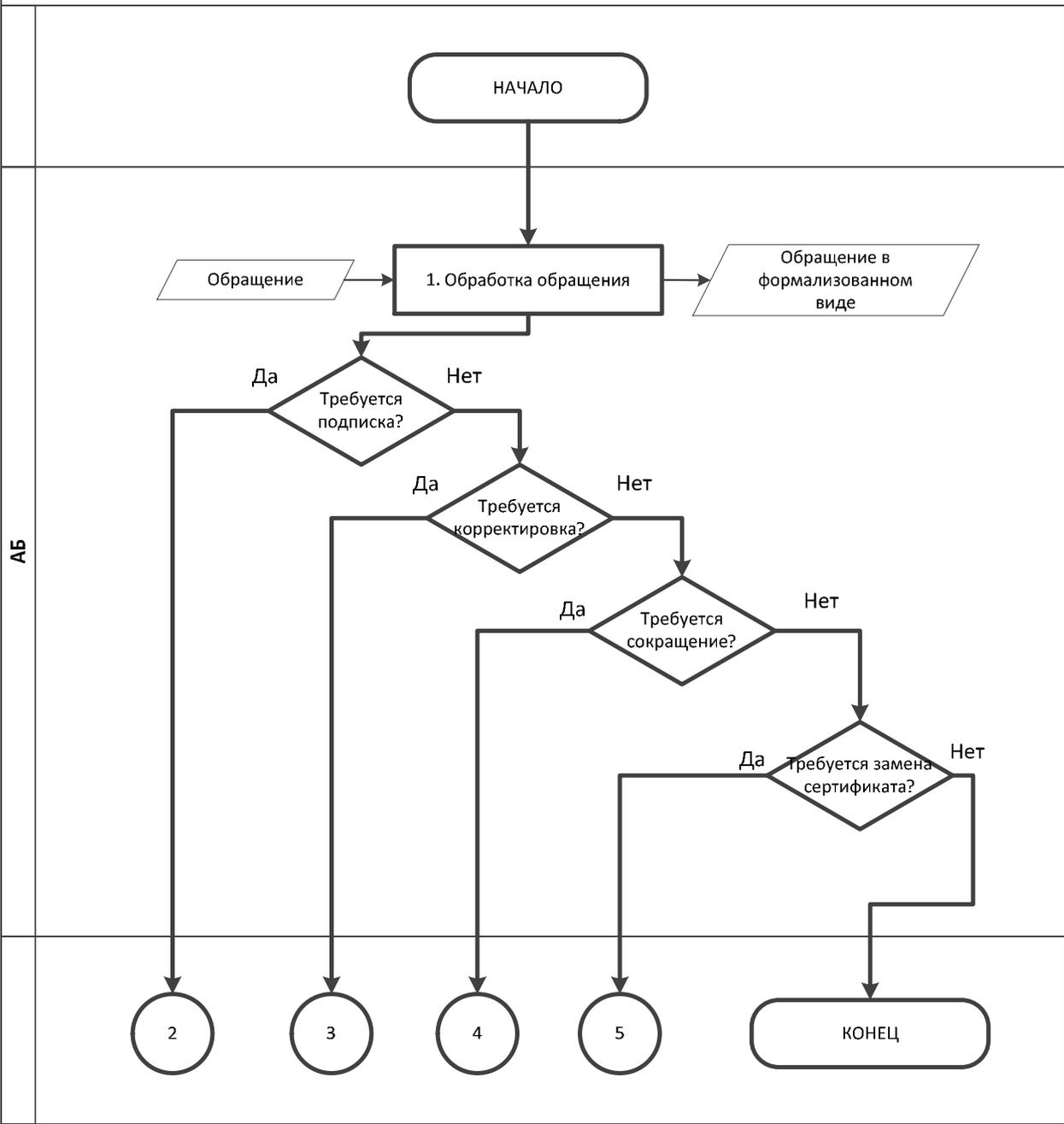


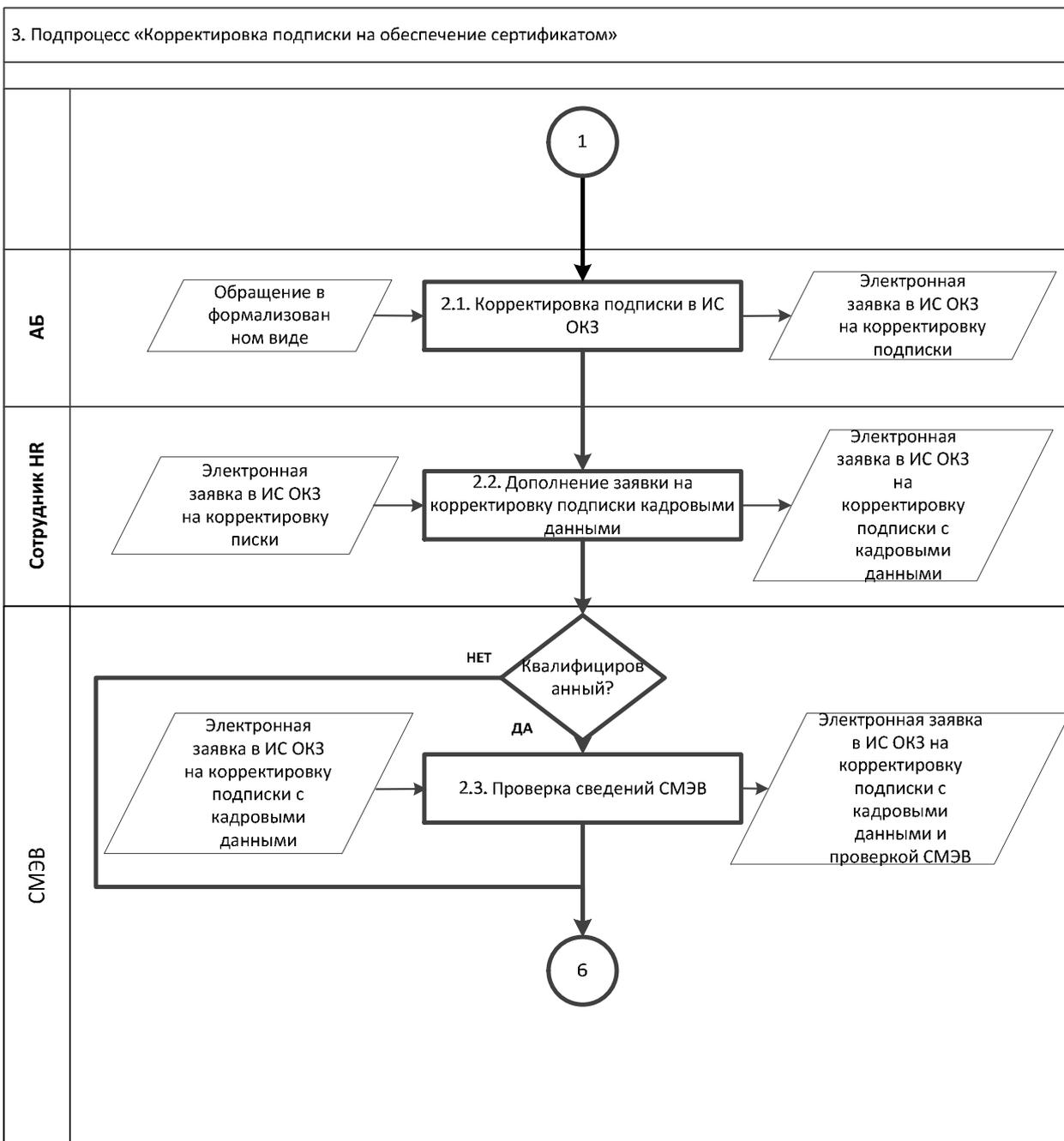
Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

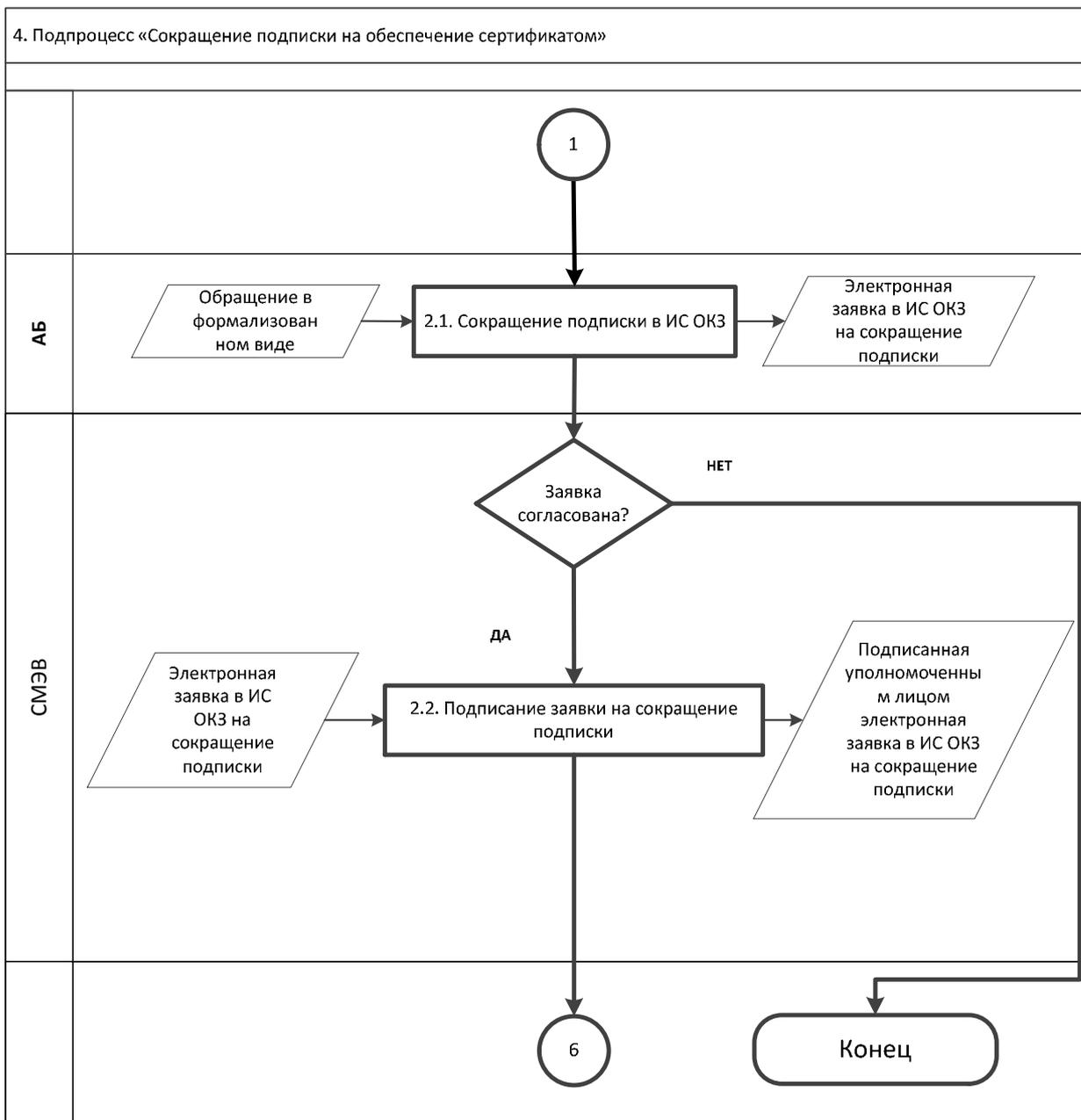
Процесс «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с использованием информационной системы Органа криптографической защиты»

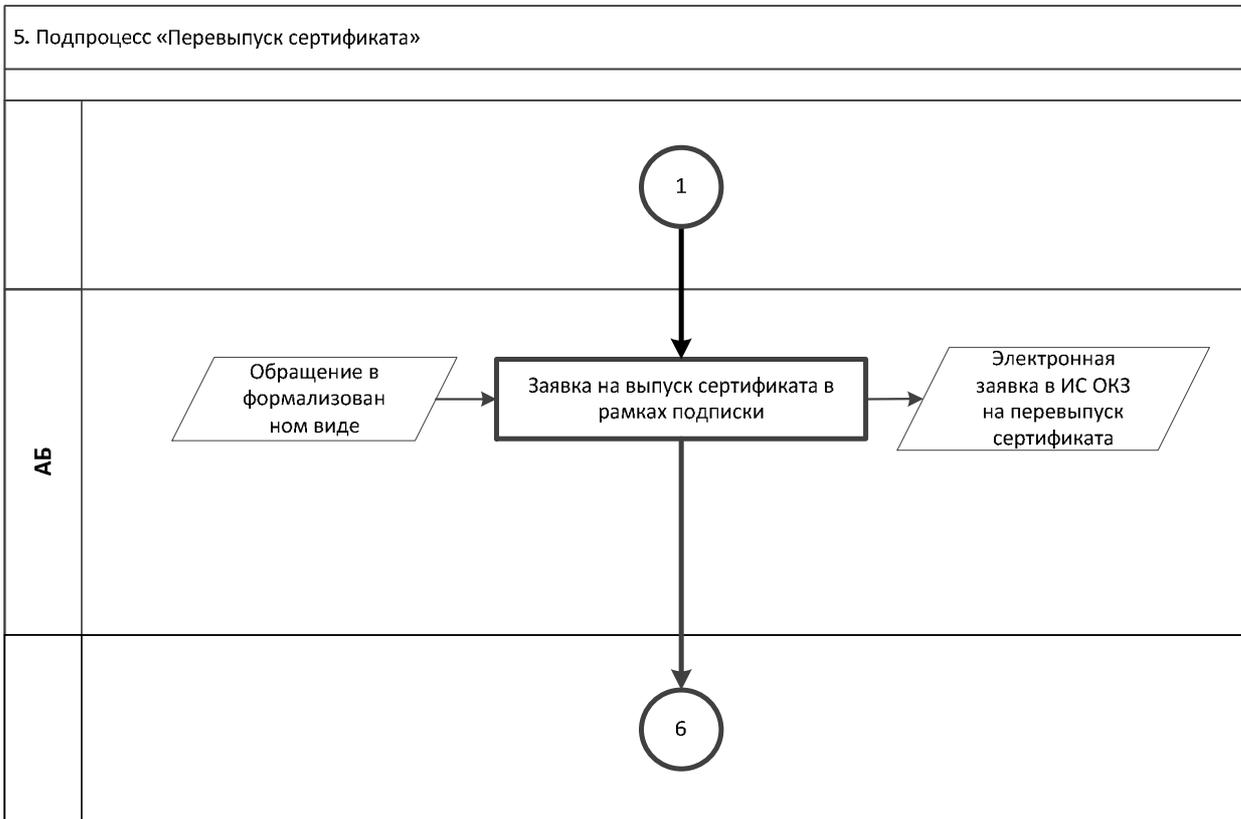


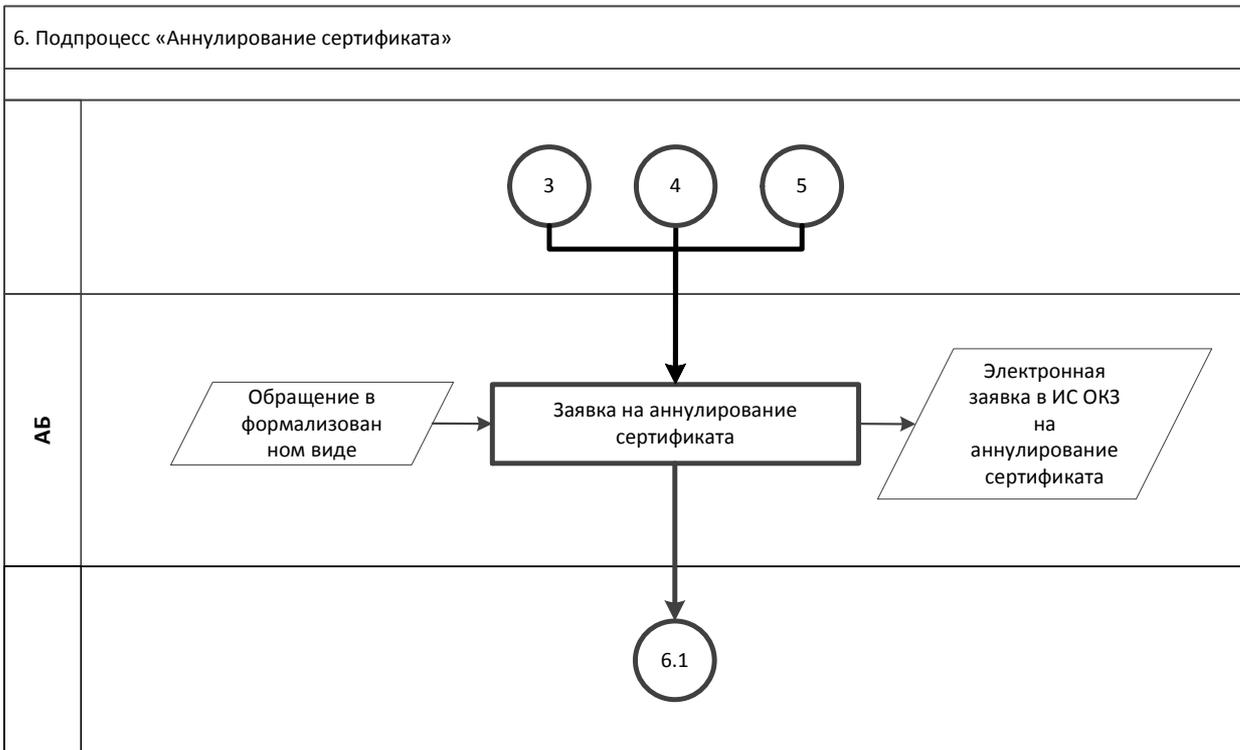
1. Подпроцесс «Обработка обращения»

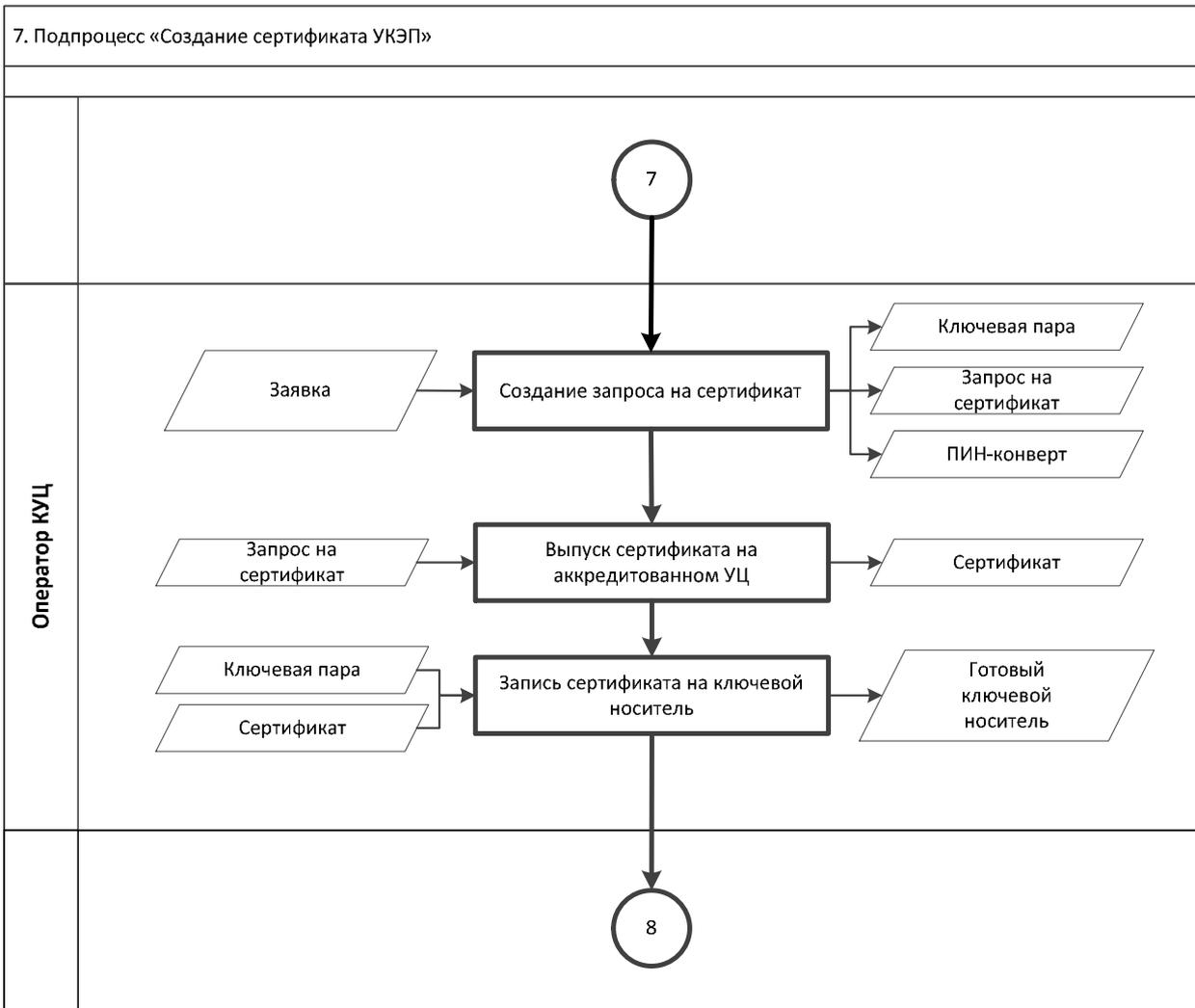


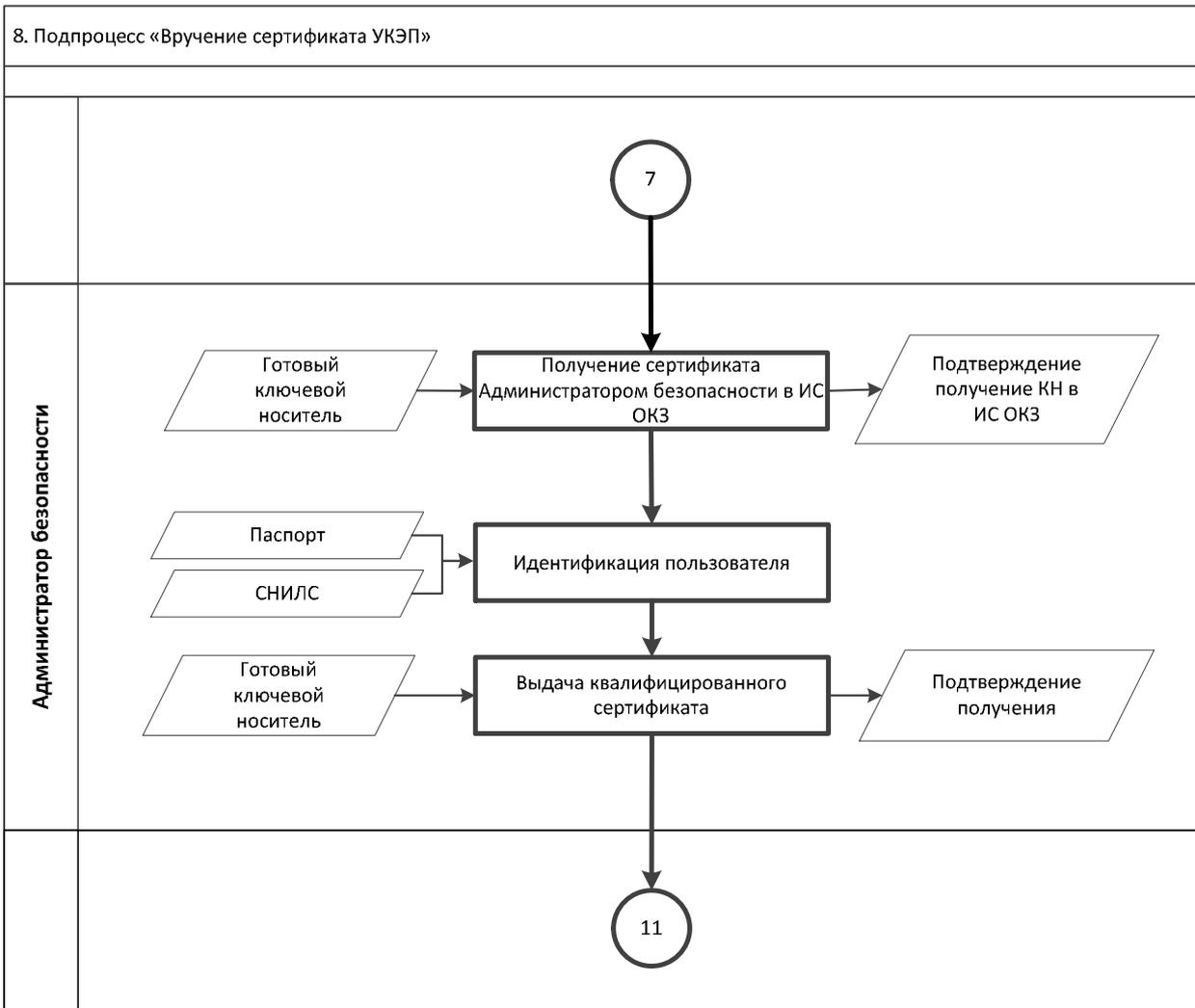


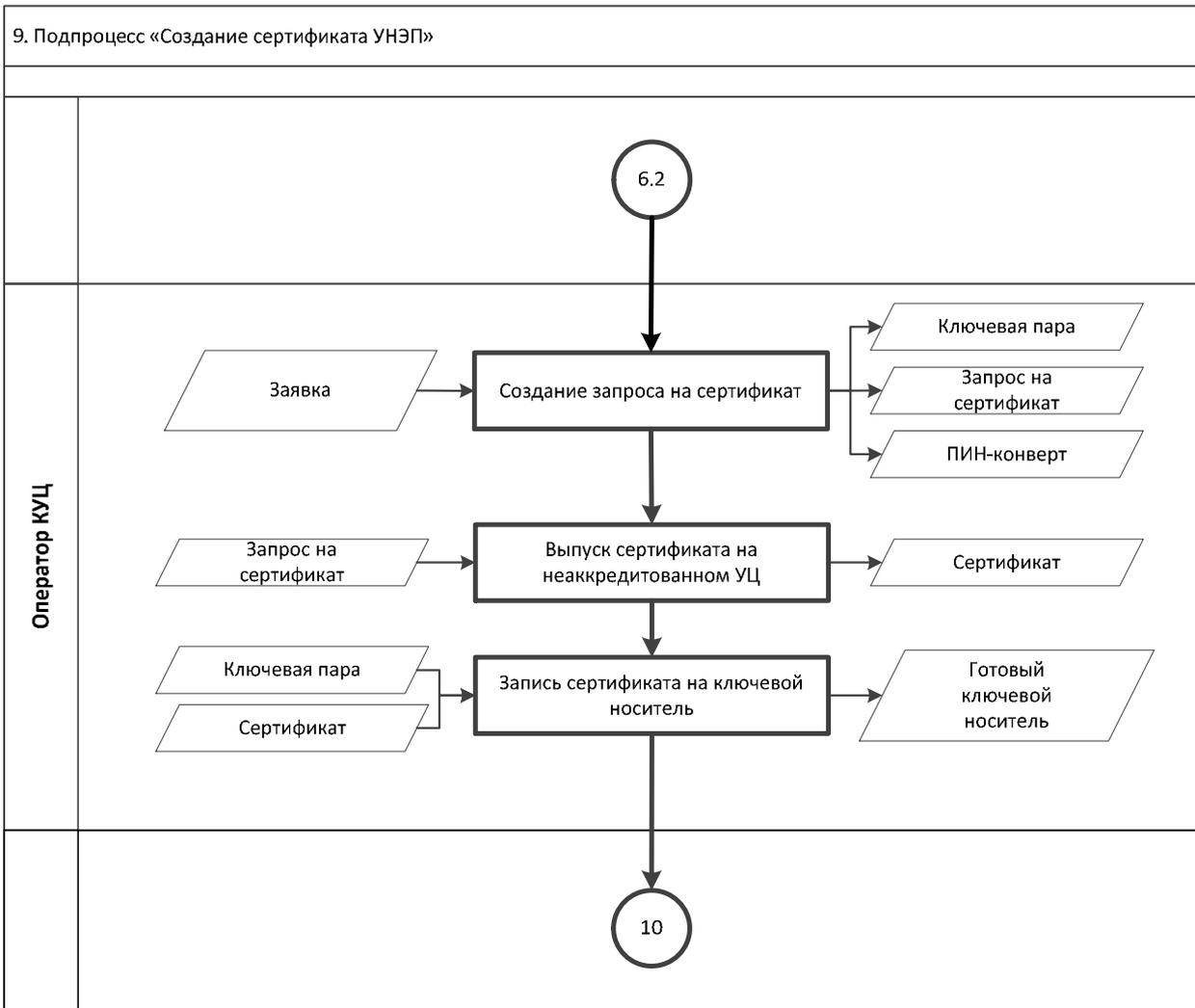


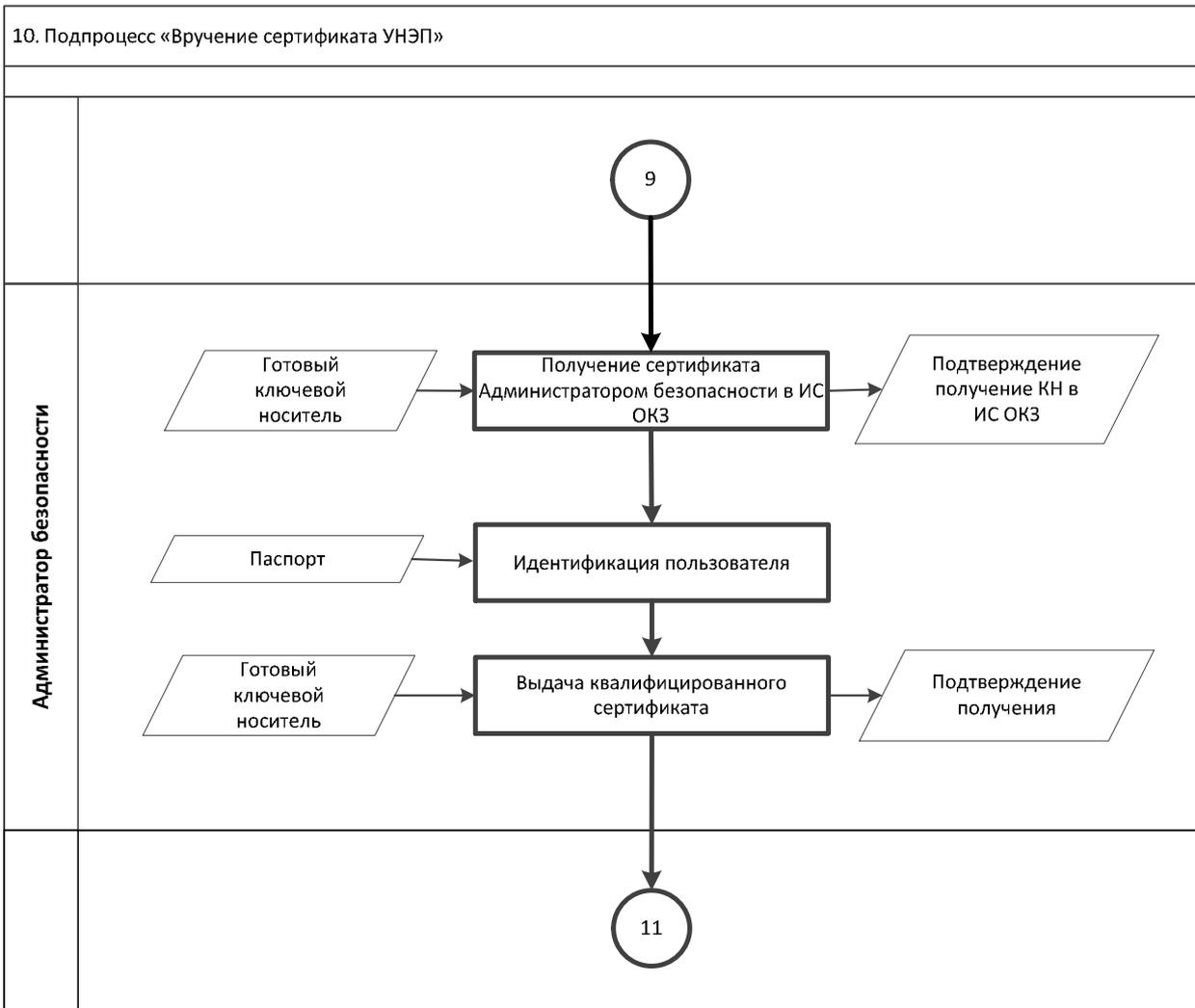


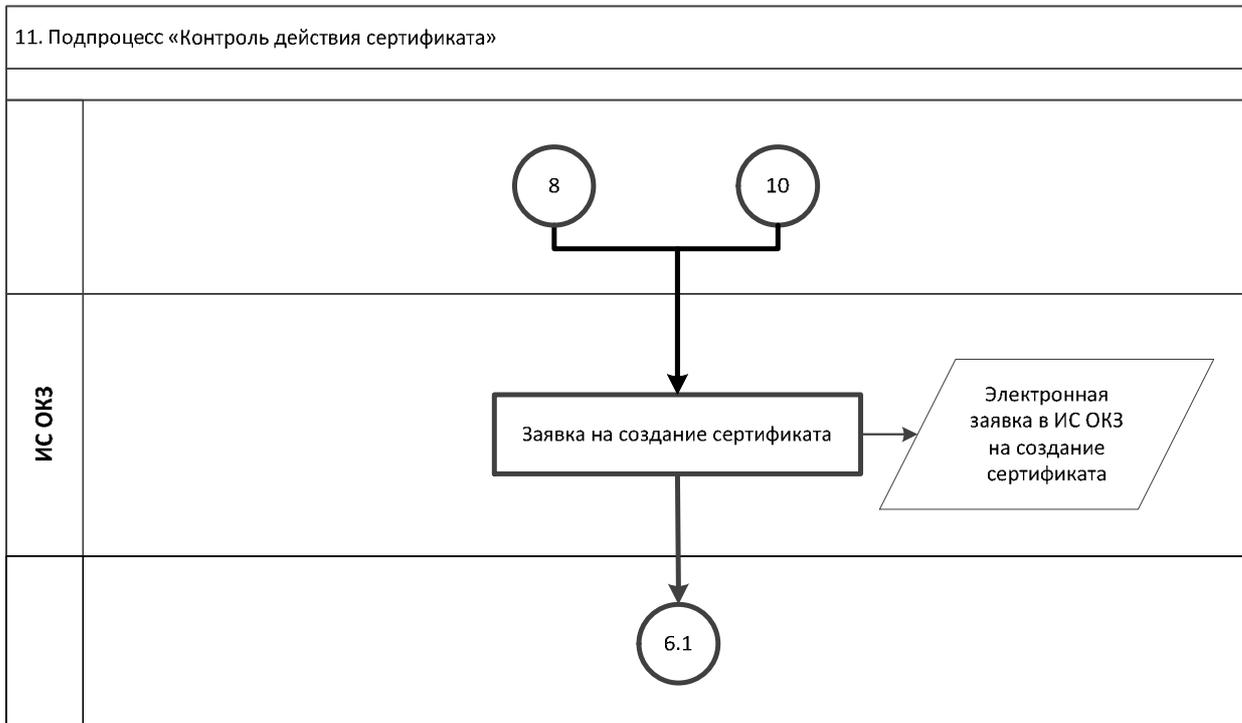












Приложение № 2

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) UnstructuredName (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	Улучшенный ключ	Могут быть внесены дополнительные области использования
Subject Key Identifier	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	Улучшенный ключ	Могут быть внесены дополнительные области использования
Subject Key Identifier	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

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

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, NTTP, 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, NTTP, 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, NTTP, 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, NTTP, 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 06 июля 2012 г.

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



С.Н. Данилов
(по дов. № 22/309/2018-ДОВ от 28.12.18)

М.П.

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 с использованием информационной системы Органа криптографической защиты»

Редакция №1

Москва 2019 г.

Оглавление

1. Назначение и область применения.....	3
2. Термины, определения и сокращения.....	5
3. Описание процесса	6
3.1. Цель процесса.....	6
3.2. Задачи процесса.....	7
3.3. Участники группы процессов и их роли.....	7
3.6. Описание подпроцессов	8
4. Нормативные ссылки.....	14
5. Порядок внесения изменений	15
6. Контроль и ответственность	15
7. Перечень приложений	16
Приложение №1. Матрица ответственности.....	17
Приложение №2. Схема процесса	19

1. Назначение и область применения

Настоящий 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 с использованием информационной системы Органа криптографической защиты» (далее – Регламент), разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты (далее – ОКЗ).

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

Требования настоящего Регламента распространяются на организации-обладатели конфиденциальной информации (далее - ООКИ), использующие 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 Регламент использует ссылки на следующие документы, необходимые для управления процессом «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»:

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)	Действует	Лицензия	Волков С.П.

<p>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)</p>			
<p>Федеральный закон Российской Федерации от 06.04.11 г. № 63-ФЗ "Об электронной подписи"</p>	<p>Действует</p>	<p>Федеральный закон</p>	<p>Волков С.П.</p>
<p>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»</p>	<p>Действует</p>	<p>Приказ</p>	<p>Волков С.П.</p>
<p>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)»</p>	<p>Действует</p>	<p>Приказ</p>	<p>Волков С.П.</p>
<p>Приказ ГК «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»</p>	<p>Действует</p>	<p>Требование</p>	<p>Волков С.П.</p>

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 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	<ul style="list-style-type: none"> • Согласовывает и подписывает электронные заявки в ИС ОКЗ на создание и сокращение подписок предприятия.
2	Аналитик ОКЗ АО «Гринатом» (далее – Аналитик)	<ul style="list-style-type: none"> • 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»	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Проходит обучение в ИС ОКЗ и сдает тестирование.

3.6. Описание подпроцессов

3.6.1. 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».

3.6.2. 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 информационно-системы Органа криптографической защиты» завершается.

3.6.3 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».

3.6.4 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».

3.6.5 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».

3.6.6 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.

3.6.7 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».

3.6.8 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.

3.6.9 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 ГК «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»;
- 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, защищённых 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 Регламент, а также в приложения к нему, производится посредством утверждения новой редакции Регламента.

6. Контроль и ответственность

6.1 Регламент обязаны соблюдать все следующие участники процесса:

Уполномоченное лицо предприятия;
Аналитик ОКЗ АО «Гринатом»;
Администратор безопасности ОКЗ АО «Гринатом»;
Пользователь.

6.2. Ответственность работников за несоблюдение требований Регламента.

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

7. Перечень приложений

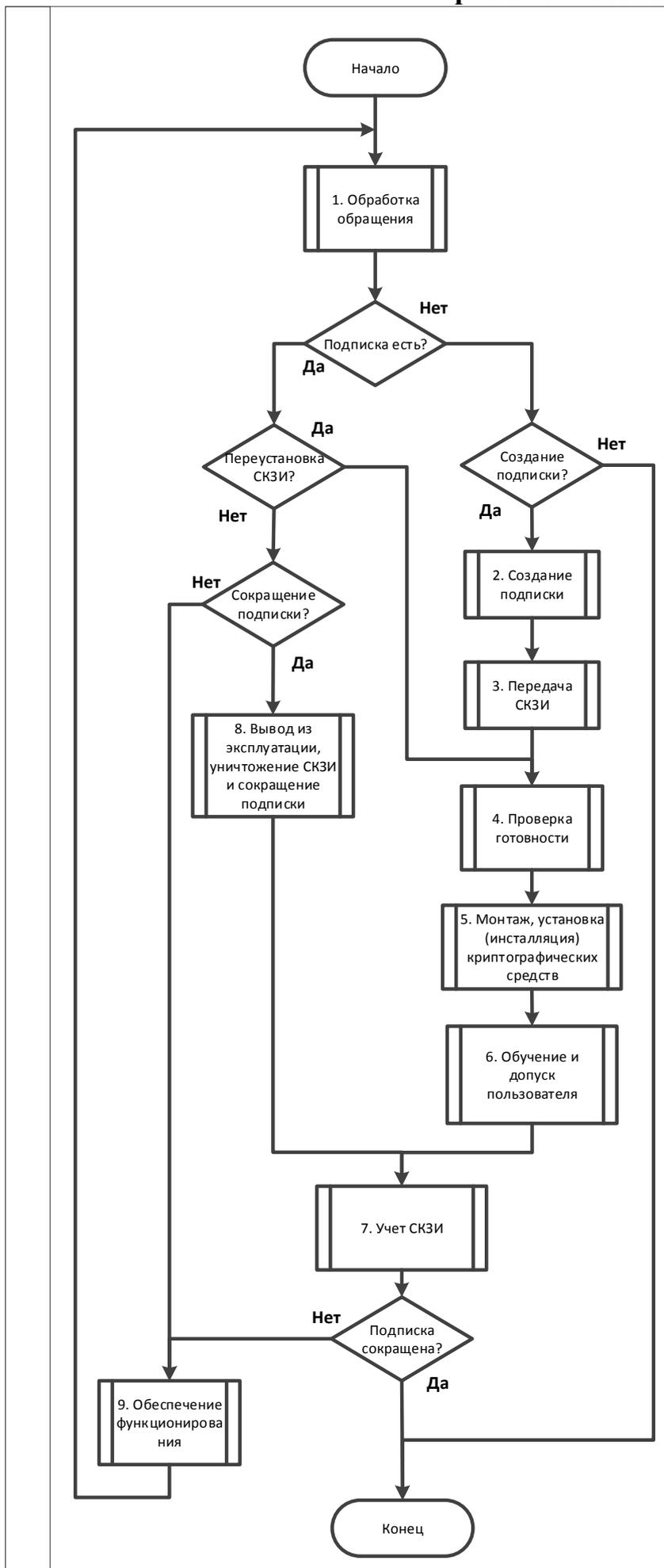
Приложение №1. Матрица ответственности.
Приложение №2. Схема процесса.

Приложение №1. Матрица ответственности

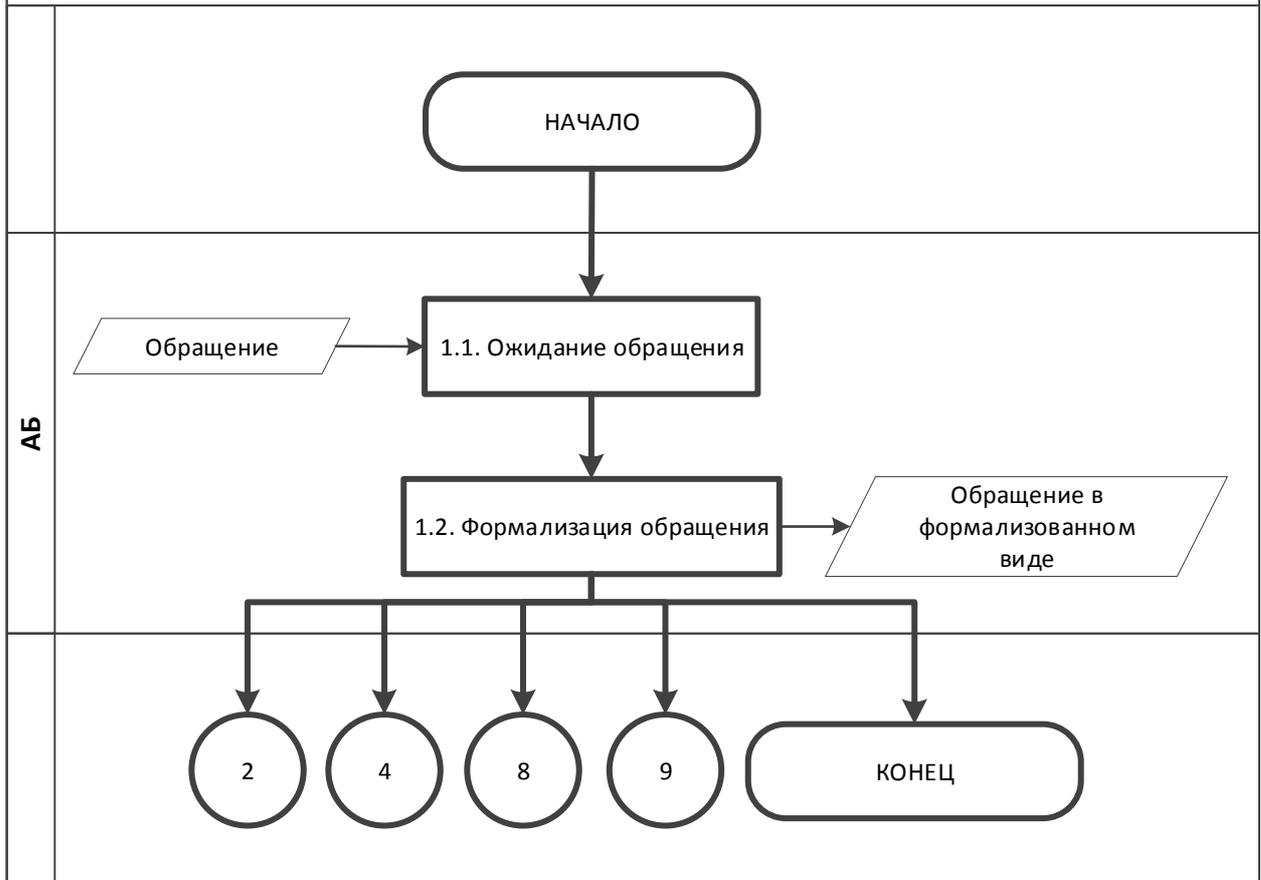
Подпроцессы в составе процесса	Участники процесса			
	Уполномоченное лицо предприятия	Аналитик	АБ	Пользователь
Подпроцесс «Обработка обращения»			О	
Подпроцесс «Создание подписки»	С	С	О	
Подпроцесс «Передача СКЗИ»	Инф.	О		Инф.
Подпроцесс «Проверка готовности»		Инф.	О	
Подпроцесс «Монтаж, установка (инсталляция) 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

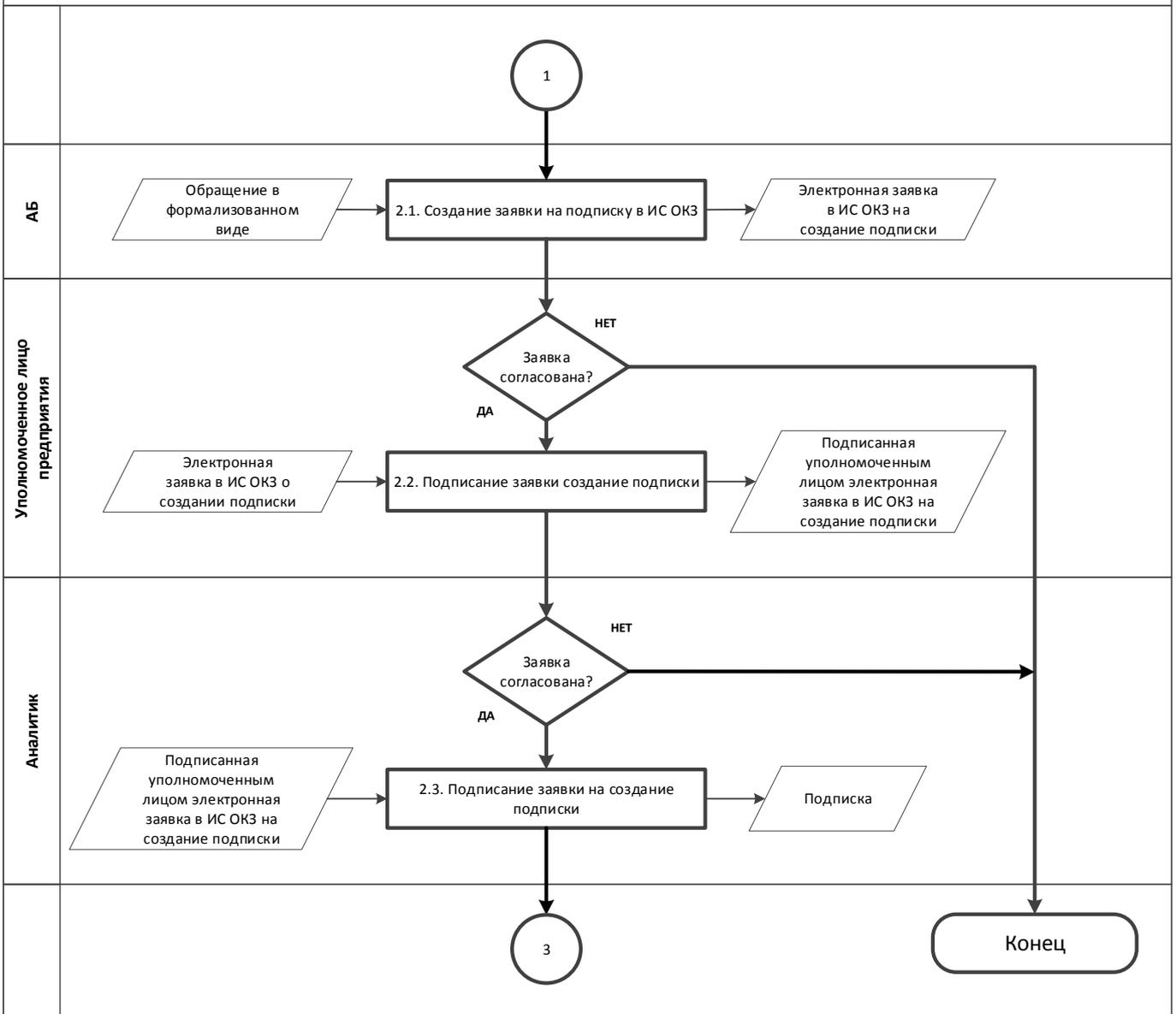
О	Ответственный	Несет ответственность за достижение результата по подпроцессу/процедуре в своей предметной области	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
Утв	Утверждающий	Утверждает - принимает окончательное решение по результату подпроцессу/процедуре	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

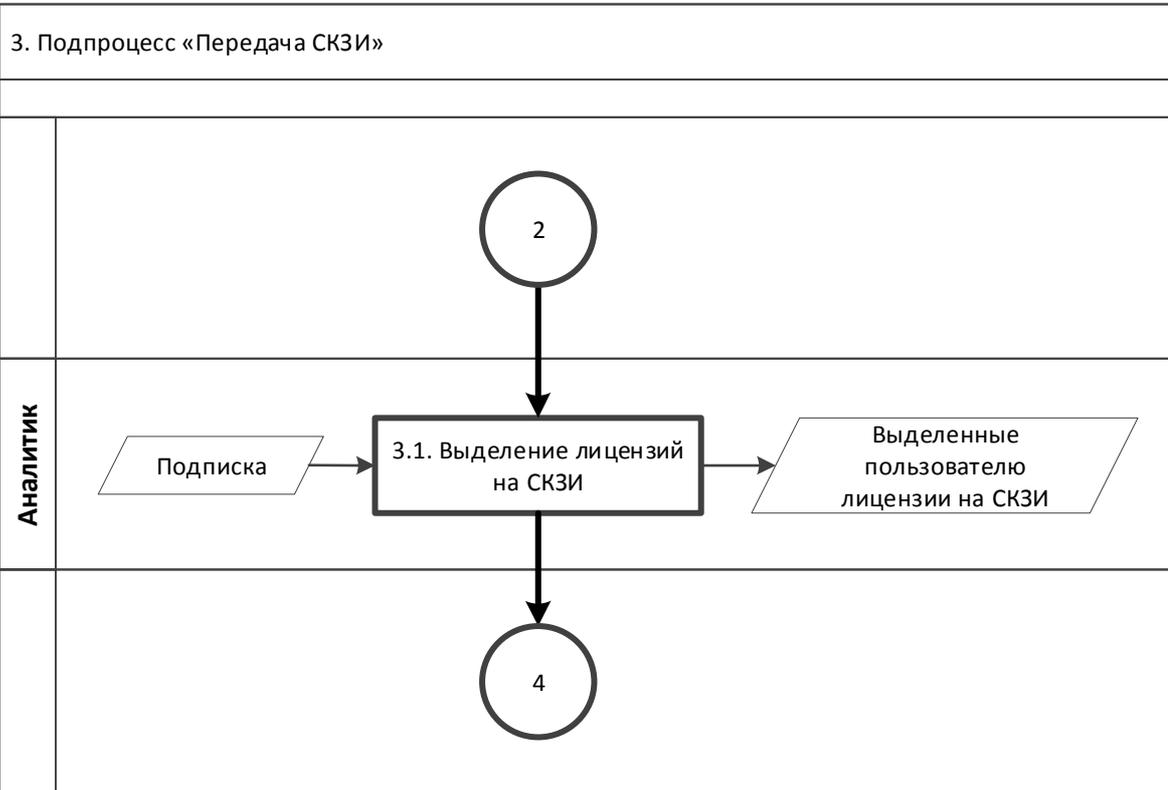


1. Подпроцесс «Обработка обращения»

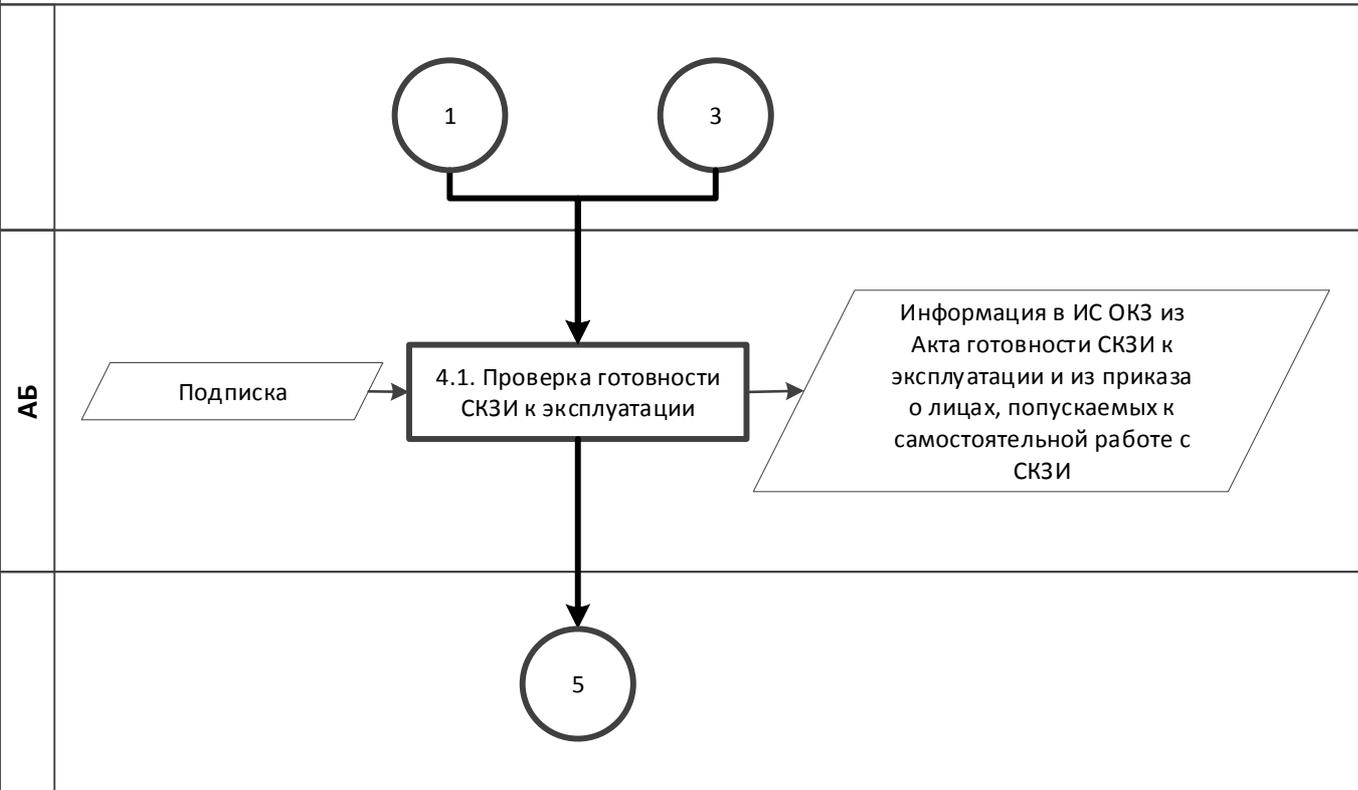


2. Подпроцесс «Создание подписки»

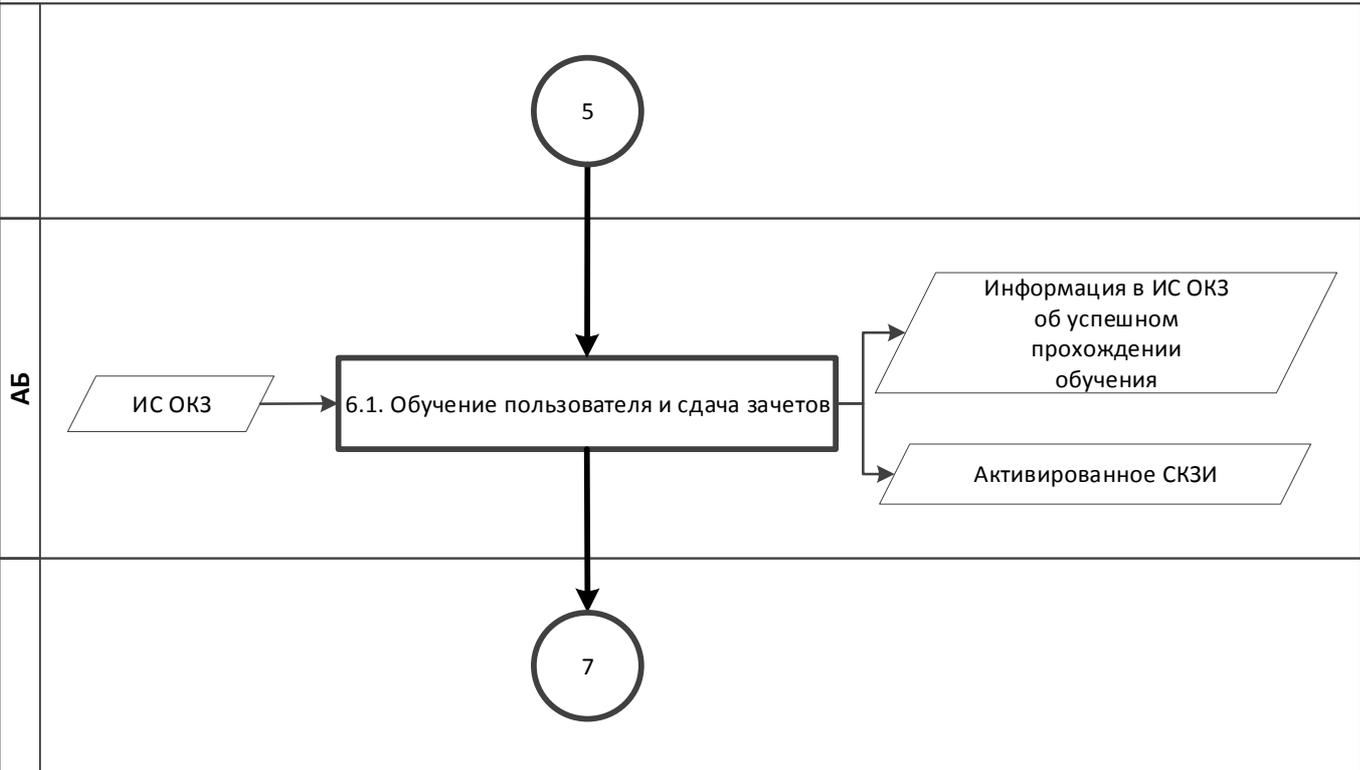




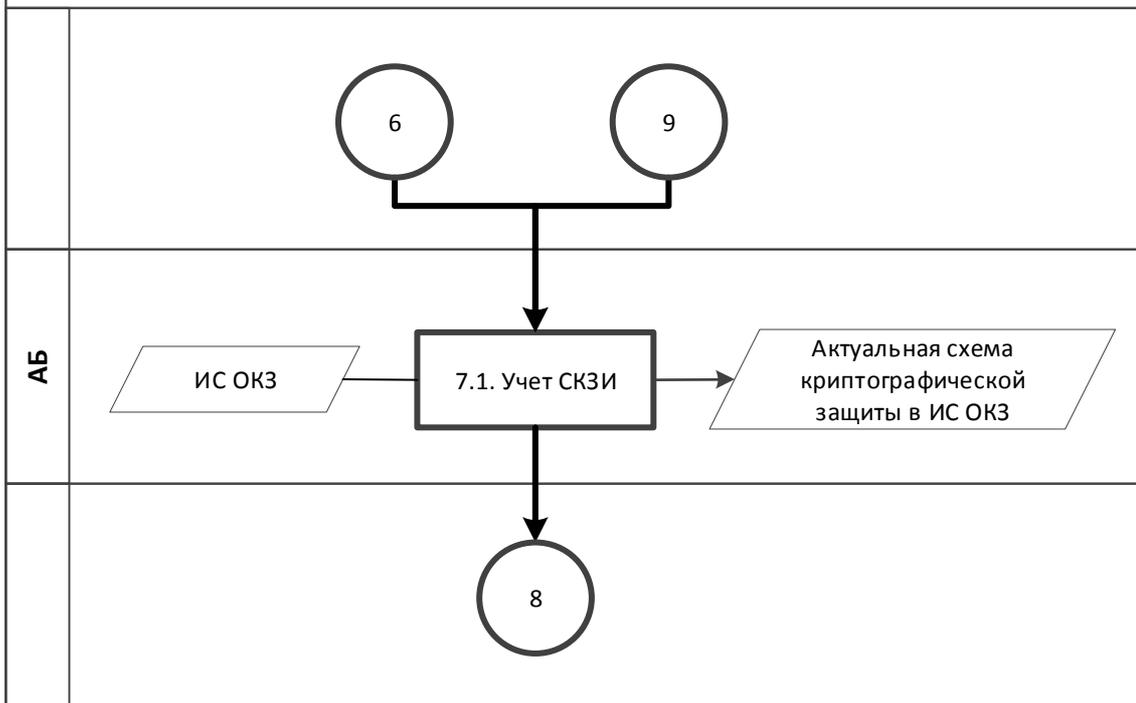
4. Подпроцесс «Проверка готовности»



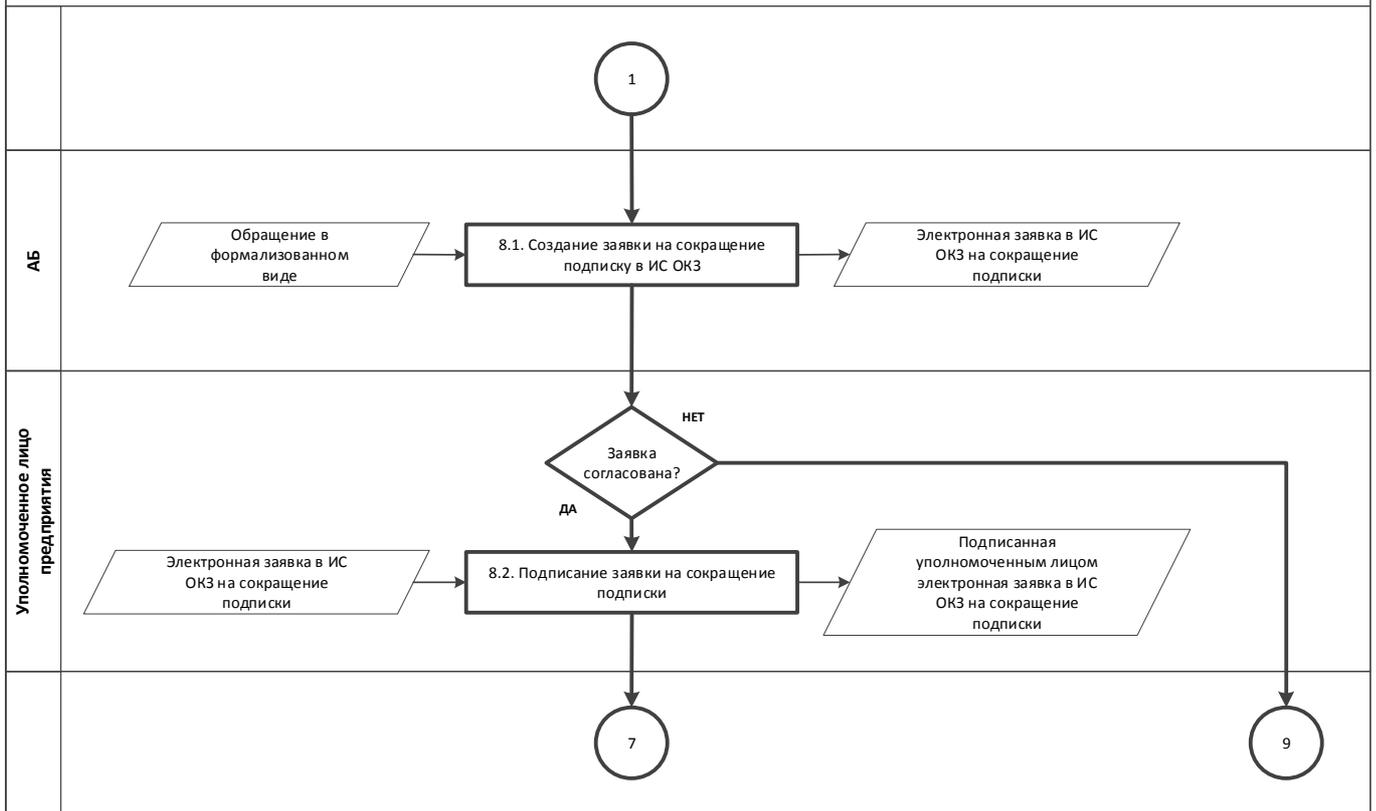
6. Подпроцесс «Обучение и допуск пользователя»



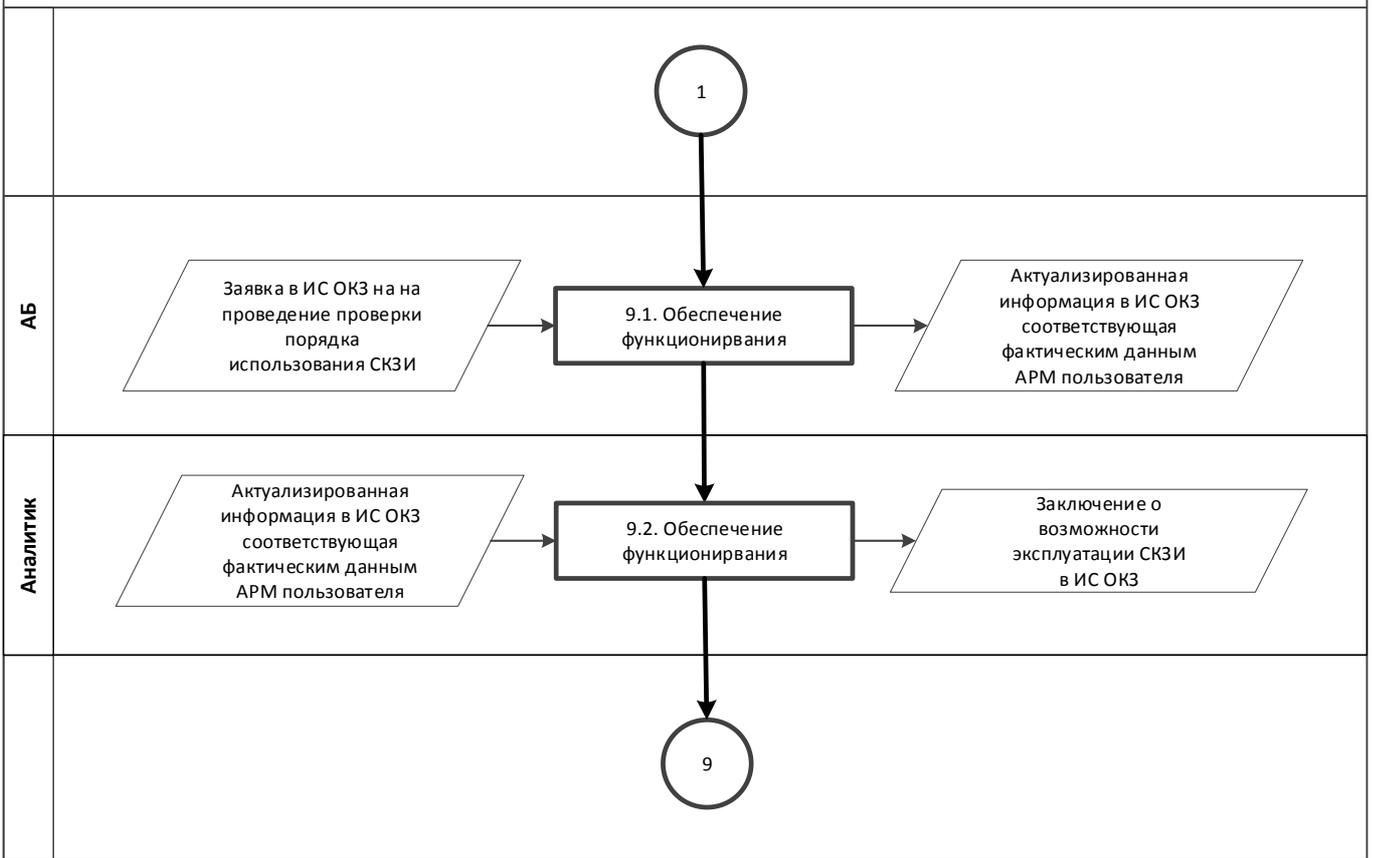
7. Подпроцесс «Учет СКЗИ»



8. Подпроцесс «Вывод из эксплуатации, уничтожение СКЗИ и сокращение подписки»



9. Подпроцесс «Обеспечение функционирования»



Приложение №10
к Договору присоединения № 22/2143-Д от 06 июля 2012 г.

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



С.Н. Данилов

(по дову № 22/309/2018-ДОВ от 28.12.18)

М.П.

Соглашение
о применении простой и усиленной неквалифицированной электронных подписей
в информационной системе органа криптографической защиты
АО «Гринатом»

Москва 2019 г.

Оглавление

1. Термины и сокращения	3
2. Предмет Соглашения	3
3. Общие положения	3
3.1. Ключи простой и неквалифицированной электронных подписей.....	4
3.2. Средства простой и усиленной неквалифицированной электронных подписей 4	4
3.3. Условия равнозначности простой и усиленной неквалифицированной электронных подписей собственноручной.....	5
4. Обязанности владельцев ключей простой и усиленной неквалифицированной электронных подписей.....	5
5. Ответственность Участников системы.....	5
6. Форс-мажор	6
7. Разрешение споров.....	6
8. Порядок заключения Соглашения.....	6
8.1. Срок действия соглашения.....	7
8.2. Изменение условий соглашения.....	7
9. Дополнительные условия.....	7
10. Юридический адрес АО «Гринатом».....	8

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.

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

Генеральный директор АО «Гринатом»

_____ / М.Ю. Ермолаев /
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,

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 Составы 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 промежутки 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 № 11
к Договору присоединения № 22/154 от 5 июля 2012 г.

утверждена
информационно-технологическим директором
АО «Гринатом» / С.И. Давыдов
от 28.06.2018 № 22/309/2018-ДО/ИТ



Предоставление/отключение доступа/изменение прав доступа пользователей к информационному ресурсу

В соответствии с Приказом ГК Росатом 1/577-П от 27.06.2017 года заявка на массовое предоставление оформляется в случае назначения 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	Бессрочно	Беленный Н.И.		Тихонов А.В.	

Фамилия Имя Отчество - администратор	Табельный номер	Должность	Организация (полное наименование)	Подразделение	Гражданство (РФ или иное)	Login	e-mail	Место расположения	Контактный телефон	Действия	Назначение роли		Техническое имя
											Пользователь		
1													
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 предоставление, возлагается на руководителей организаций 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 машинным способом, внесение изменений и исправлений не допускается

При запросе доступа к информационному ресурсу "Корпоративная почтовая система ГК Росатом" указать, требуется ли сортировать почтовый ящик из отраслевой адресной книги.