ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ № 22/2143-Д-5

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» октября 2015 года

Настоящее Дополнительное соглашение в соответствии с пунктом 3.3.1 Договора присоединения вносит изменения (дополнения) в Договор присоединения, включая приложения к нему и является неотъемлемой частью Договора присоединения. Все изменения (дополнения), вносимые настоящим дополнительным соглашением в Договор вступают в силу и становятся обязательными по истечении 30 (тридцати) суток с даты размещения указанных изменений и дополнений в Договоре на сайте Исполнителя. Текст Договора присоединения изменяется и излагается в следующей редакции:

Статья 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. Исполнитель – Закрытое акционерное общество «Гринатом» (ЗАО «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://www.rosatom.ru/ca.
1.7. Информирование стороны по Договору – официальное сообщение уполномоченного лица в адрес стороны по Договору.

Статья 2. ПРЕДМЕТ ДОГОВОРА

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

Статья 3. УСЛОВИЯ ДОГОВОРА ПРИСОЕДИНЕНИЯ

3.1. Присоединение к Договору.

3.1.1. Текст Договора опубликован на сайте Исполнителя

3.1.2. Заказчик присоединяется к Договору в целом.

3.1.3. Присоединение к настоящему Договору осуществляется путем подписания и предоставления Заказчиком Исполнителю двух экземпляров Заявления о присоединении. Исполнитель, получивший Заявление о присоединении, акцептует Заявление о присоединении Заказчика, либо направляет отказ от акцепта (молчание Исполнителя не является акцептом).

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

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

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

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

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

3.2. Расторжение Договора.

3.2.1. Действие настоящего Договора может быть досрочно прекращено по инициативе одной из Сторон в следующих случаях:
- по собственному желанию одной из Сторон;
- нарушения одной из Сторон условий настоящего Договора.

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

3.2.3. Прекращение действия Договора не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Договора, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

3.2.4. 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.

3.2.5. 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 к Договору.

4.3. Услуги оказываются в соответствии с Регламентами услуг (Приложения № 2,3) по заявлениям уполномоченных лиц Заказчика, направляемым в адрес Исполнителя. Формы заявлений приведены в приложениях к Регламентам 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. 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. Заказчик обязуется в установленные Договором сроки принимать и оплачивать оказанные Услуги в соответствии с порядком и сроками, установленными Договором.

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

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

Статья 6. ПОРЯДОК ПОДТВЕРЖДЕНИЯ ВЫПОЛНЕНИЯ ОБЯЗАТЕЛЬСТВ

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

6.2. Отчётным периодом оказания Услуг является календарный квартал.

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

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

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

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

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

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

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

Статья 7. СТОИМОСТЬ И ОПЛАТА УСЛУГ

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

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

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

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

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

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

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

7.8. Восстановление (возобновление) оказания Услуг производится Исполнителем в течение суток с даты поступления денежных средств на

расчётный счёт Исполнителя при условии предоставления документов, подтверждающих оплату Услуг в полном объёме.

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

Статья 8. КОНФИДЕНЦИАЛЬНОСТЬ

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

Статья 9. ОТВЕТСТВЕННОСТЬ СТОРОН

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

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

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

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

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

9.6. По обязательствам в отношении конфиденциальной информации обе Стороны несут полную ответственность в соответствии с Соглашением о

конфиденциальности и действующим законодательством Российской Федерации.

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

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

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

Статья 10. РАЗРЕШЕНИЕ СПОРОВ

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

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

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

10.4. Все споры, разногласия или требования, возникающие из настоящего Договора или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или недействительности, которые не удалось разрешить путем переговоров, подлежат разрешению в Третейском суде для разрешения экономических споров при Частном учреждении «Центр третейского регулирования и правовой экспертизы» в соответствии с его регламентом. Решение Третейского суда является окончательным.

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

Статья 14. ЮРИДИЧЕСКИЙ АДРЕС И БАНКОВСКИЕ РЕКВИЗИТЫ ИСПОЛНИТЕЛЯ

Полное наименование: Закрытое 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:

Генеральный директор

ЗАО «Гринатом» М.Ю. Ермолаев

Гринатом М.П.

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

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

_____

_____

(наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании_____

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

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 ЗАО «Гринатом»

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

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

ЗАО «Гринатом» _____ _____

(должность, ФИО, основание) М.П

От Исполнителя:

Генеральный директор
ЗАО «Гринатом» М.П. _____М.Ю. Ермолаев

Приложение №2

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

Регламент процесса

«Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

Редакция № 2.4

г. Москва

01.10.2015

Содержание

1. Назначение и область применения

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

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

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

Руководитель предприятия/организации;

Пользователь КУЦ;

Доверенное лицо;

Оператор КУЦ;

Администратор КУЦ;

Комиссия КУЦ;

Руководитель КУЦ.

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

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

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

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)			
Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»	Действует	Федеральный закон	Данилов С.Н
Приказ ФАПСИ № 152 от 13 июня 2001г. «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»	Действует	Приказ	Данилов С.Н
Приказ ФСБ РФ от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки	Действует	Приказ	Данилов С.Н

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

и является основой при регламентации следующих подпроцессов и процедур:

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

2. Термины, определения и сокращения

Термин	Определение
Аккредитация удостоверяющего центра	признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"
Квалифицированный сертификат ключа проверки электронной подписи	сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи
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
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 или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим действующим законодательством Российской Федерации
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	Пользователь КУЦ	Корпорация

	на бумажном носителе		
9.	OCSP запрос	Пользователь КУЦ	Корпорация
10.	TSP запрос	Пользователь КУЦ	Корпорация
11.	Внешнее официальное обращение в КУЦ в части применения электронной подписи	ВСЕ	Корпорация

3.3 Основные выходы процесса

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

3.5 Описание подпроцессов

3.5.1 Подпроцесс «Предоставление информации в КУЦ»

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

Пользователь КУЦ предоставляет информацию в КУЦ в виде:

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

Пользователь КУЦ предоставляет информацию в КУЦ посредством выполнения процедур:

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

3.5.1.1 Процедура «Предоставление информации доверенным лицом»

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

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

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

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

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

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

3.5.1.2 Процедура «Предоставление информации почтовым сообщением»

Пользователь КУЦ подготавливает и отправляет в адрес КУЦ информацию для:

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

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

Для создания сертификата Пользователь КУЦ подготавливает и отправляет в адрес КУЦ комплект документов, подтверждающих

достоверность информации, предоставленной для включения в сертификат, либо их надлежащим образом заверенные копии:

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

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

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

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

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

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

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

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

3.5.1.3 Процедура «Предоставление информации при личной явке»

Пользователь КУЦ прибывает в КУЦ для:

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

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

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

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

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

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

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

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

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

3.5.1.4 Процедура «Предоставление информации по e-mail»

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

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

Официальный E-mail КУЦ: ca@rosatom.ru

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

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

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

3.5.1.5 Процедура «Предоставление информации по телефону»

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

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

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

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

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

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

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

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

3.5.1.6 Процедура «Предоставление OCSP запроса»

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

Электронный адрес обращения к Службе актуальных статусов сертификатов КУЦ:

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

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

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

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

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

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

3.5.1.7 Процедура «Предоставление TSP запроса»

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

Электронный адрес обращения к Службе штампов времени КУЦ:

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

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

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

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

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

3.5.1.8 Процедура «Предоставление официальной информации для принятия решения КУЦ»

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

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

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

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

3.5.2 Подпроцесс «Создание сертификата»

Подпроцесс «Создание сертификата» регламентирует создание сертификатов КУЦ.

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

На основании информации из заявлений на создание сертификата ключа проверки электронной подписи 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».

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 ключ ЭП и сертификат на ключевом носителе, соответствующий формату, определённому в Приложении №13.

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 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;
- при компрометации ключа ЭП Уполномоченного лица КУЦ. Временем аннулирования сертификата Пользователя КУЦ признается время компрометации ключа Уполномоченного лица КУЦ, фиксирующееся в реестре КУЦ.

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

3.5.4 Подпроцесс «Приостановление действия сертификата»

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

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

КУЦ приостанавливает действие сертификата Пользователя КУЦ в следующих случаях:

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

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

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

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

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

3.5.5 Подпроцесс «Возобновление действия сертификата».

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

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

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

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

3.5.6 Подпроцесс «Подтверждение получения сертификата»

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

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

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

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

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

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

3.5.7 Подпроцесс «Подтверждение подлинности ЭП в ЭД»

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

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

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

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

Заявление должно содержать следующую информацию:

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

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

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

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

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

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

Заключение содержит:

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

Отчет по выполненной проверке содержит:

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

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

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

3.5.8 Подпроцесс «Предоставление сервиса OCSP».

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

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

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

3.5.9 Подпроцесс «Предоставление сервиса TSP».

Данный подпроцесс регламентирует порядок предоставления штампов времени по протоколу TSP.

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

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

3.5.10 Подпроцесс «Получение информации из КУЦ»

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

Пользователь КУЦ получает информацию из КУЦ в виде:

- сертификата в бумажном виде;
- ключа ЭП и сертификата на ключевом носителе;

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

Пользователь КУЦ получает информацию из КУЦ посредством выполнения процедур:

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

3.5.10.1 Процедура «Получение информации при личной явке»

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

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

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

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

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

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

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

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

3.5.10.2 Процедура «Получение информации почтовым сообщением»

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

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

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

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

3.5.10.3 Процедура «Получение информации доверенным лицом»

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

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

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

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

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

Доверенное лицо передаёт Пользователю КУЦ комплект документов.

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

3.5.10.4 Процедура «Получение информации через службу Спецсвязи России»

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

Входящая информация поступает из подпроцесса «Создание сертификата».

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

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

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

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

3.5.10.5 Процедура «Получение информации из списков отозванных сертификатов»

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

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

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

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

Период публикации СОС составляет 1 (один) день.

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

3.5.10.6 Процедура «Получение ответа OCSP сервиса»

Входящая информация поступает из подпроцесса «Предоставление сервиса OCSP».

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

OCSP-ответ признается действительным при одновременном выполнении следующих условий:

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

3.5.10.7 Процедура «Получение ответа TSP сервиса»

Входящая информация поступает из подпроцесса «Предоставление сервиса TSP».

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

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

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

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

3.5.10.8 Процедура «Получение информации из реестра КУЦ.

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

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

Ответственным за предоставление информации из реестра сертификатов является Администратор КУЦ.

4. Нормативные ссылки

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

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

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

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

5. Порядок внесения изменений

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

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

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

6. Контроль и ответственность

6.1 Контроль выполнения требований Регламента

Пользователь КУЦ несёт ответственность за:

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

Доверенное лицо несёт ответственность за:

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

Оператор КУЦ несёт ответственность за:

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

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

Администратор КУЦ несёт ответственность за:

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

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

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

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

6.2 Ответственность работников за несоблюдение требований Регламента

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

7. Перечень приложений

Приложение №1 Матрица ответственности.

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

Приложение №3 Дополнительные выходы и дополнительные входы.

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

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

Приложение №6 Форма доверенности пользователя Удостоверяющего центра

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

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

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

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

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

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

Приложение №13 Формат сертификата ключа проверки электронной подписи.

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

Приложение №15 Ограничения использования сертификатов ключа проверки электронной подписи.

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

От Исполнителя:

Генеральный директор
ЗАО «Гринатом»

М.П.

_____М.Ю. Ермолаев

Приложение №1

Матрица ответственности

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

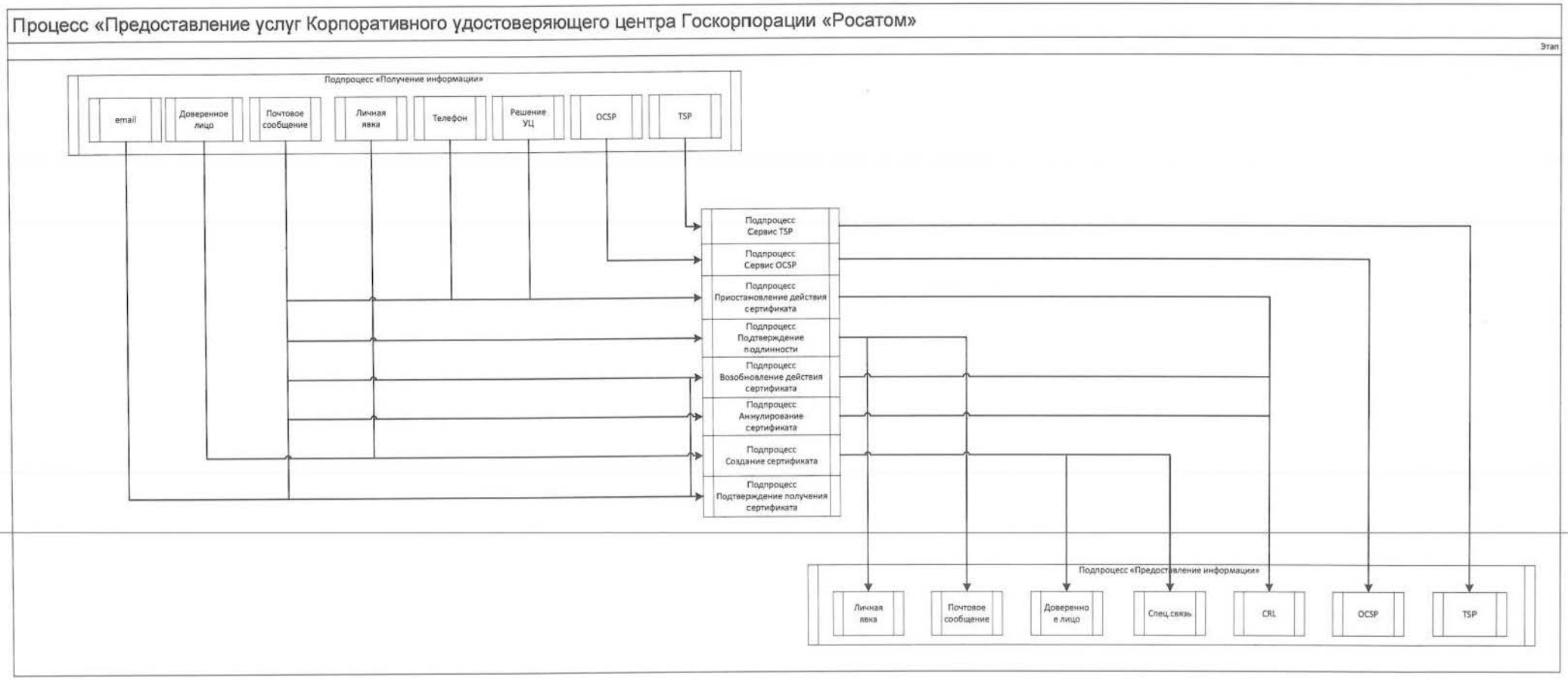
«Получение информации доверенным лицом»						
2.4. Процедура «Получение информации Спецсвязью России»		Инф		О	К	
2.5. Процедура «Получение информации CRL»		Инф			О	К
2.6. Процедура «Получение информации OCSP»		Инф			О	К
2.7. Процедура «Получение информации TSP»		Инф			О	К
3. Подпроцесс «Подтверждение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

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

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

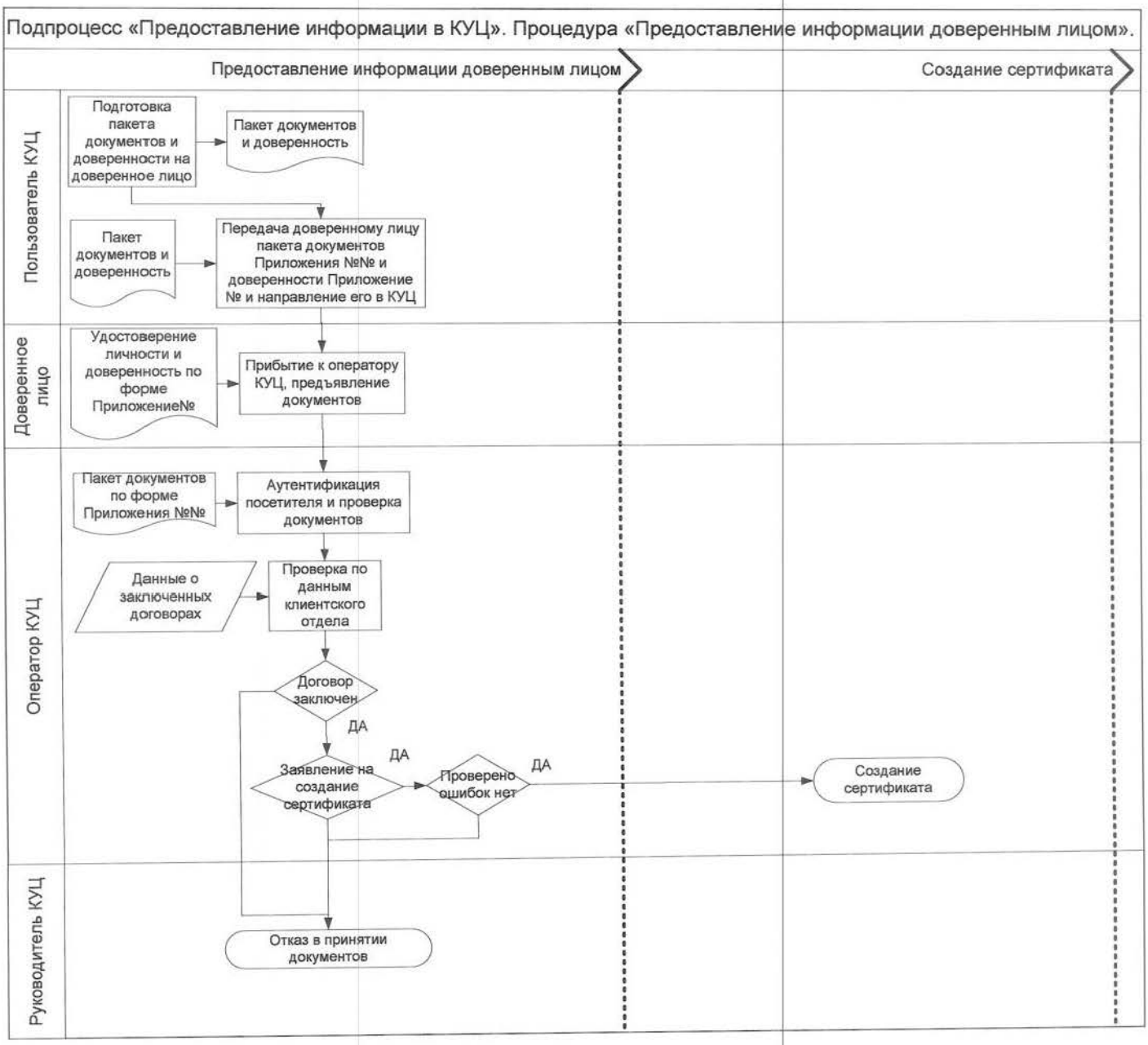
Приложение №2

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

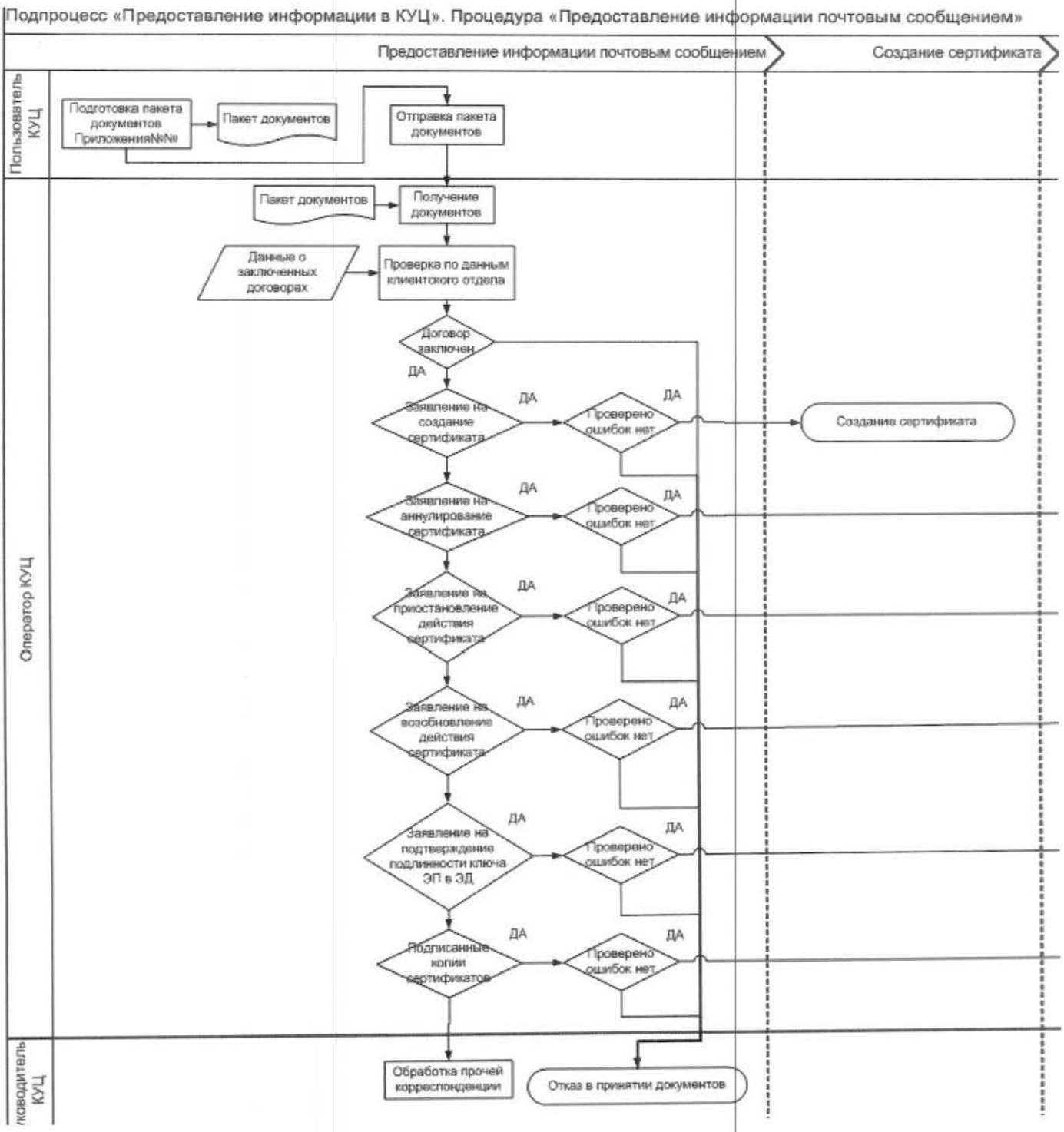


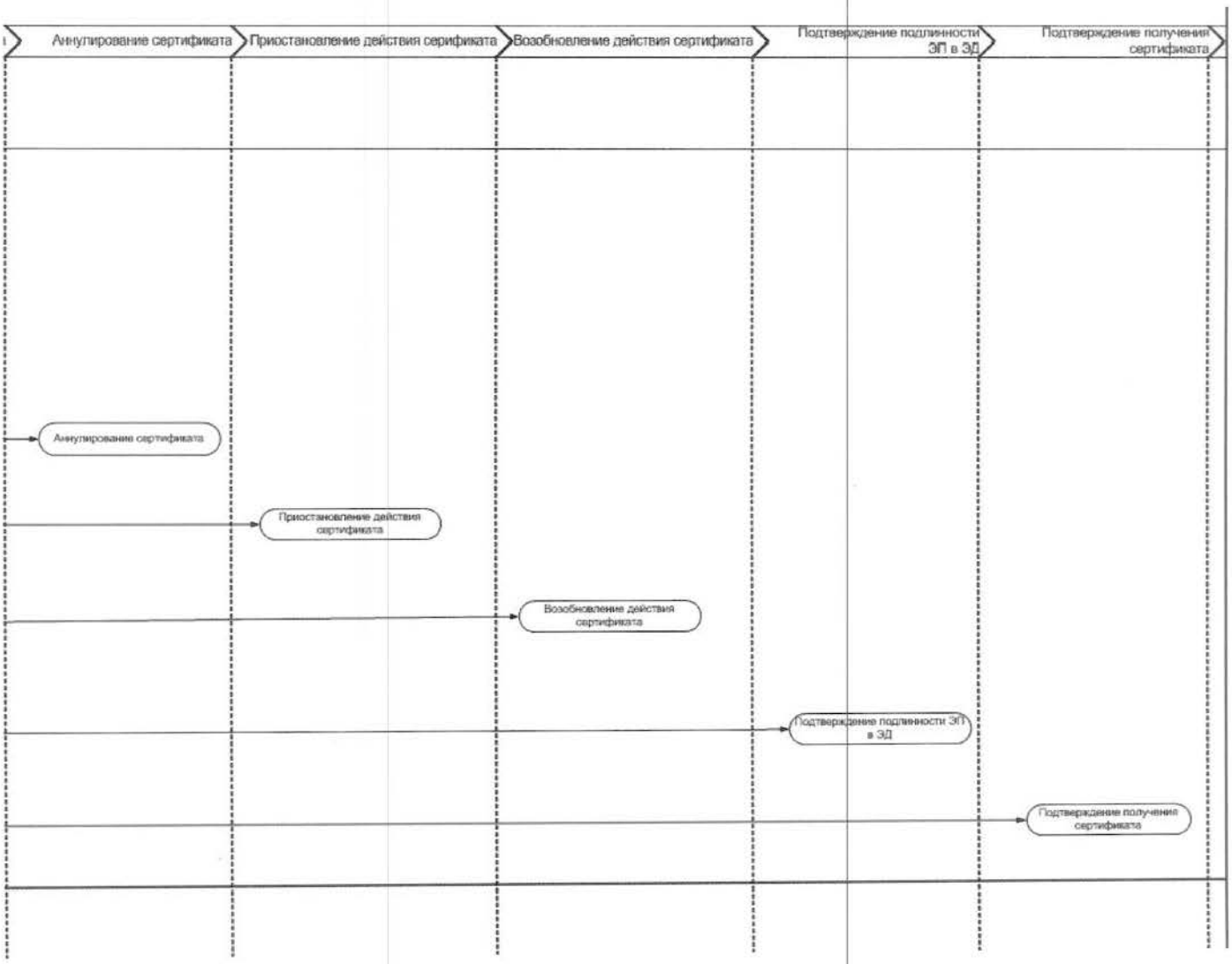
1. Подпроцесс «Предоставление информации в КУЦ»:

а) Схема процедуры «Предоставление информации доверенным лицом»:

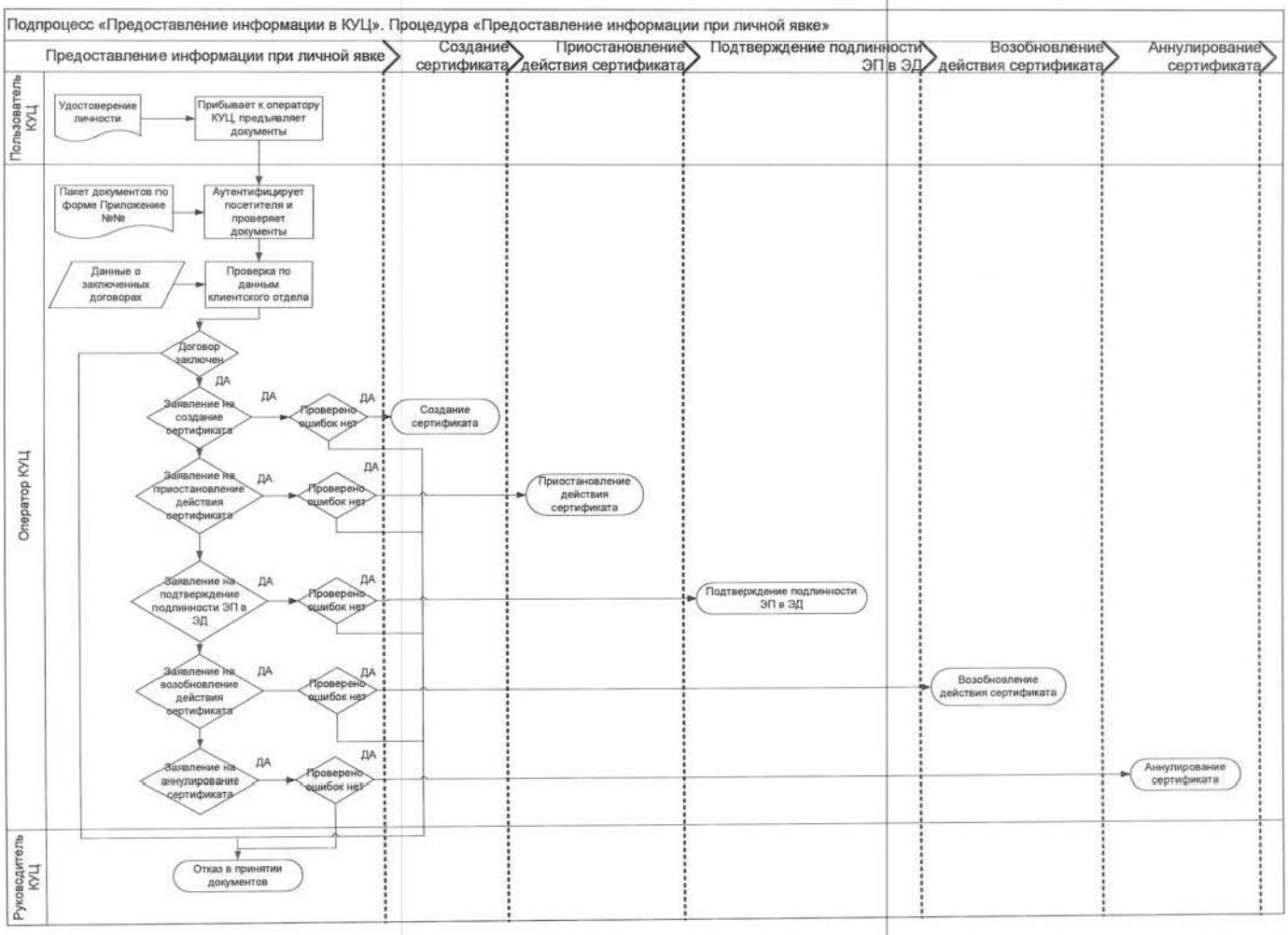


b) Схема процедуры «Предоставление информации почтовым сообщением»:

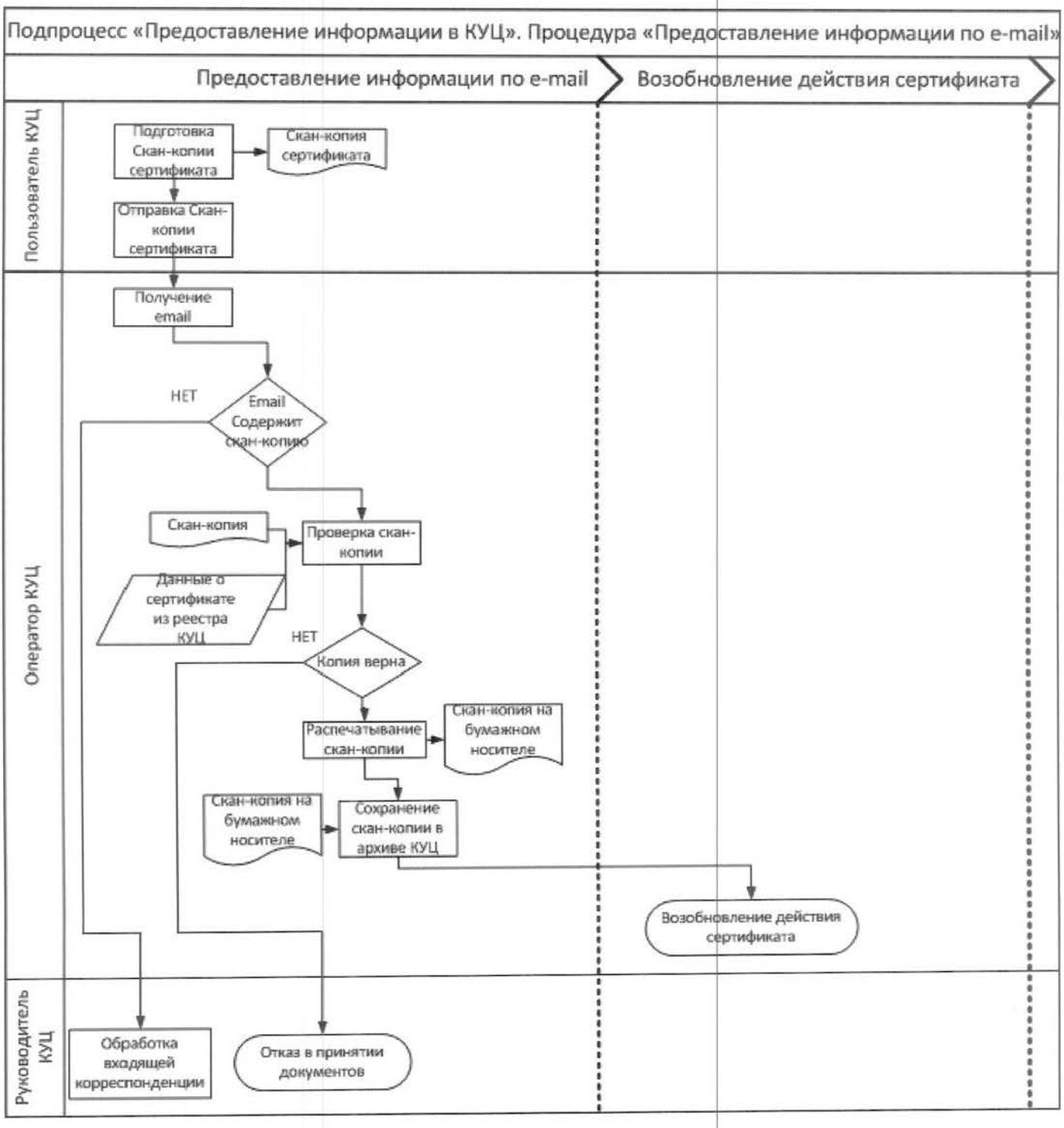



Аннулирование сертификата
Приостановление действия серификата
Возобновление действия сертификата
Подтверждение подлинности ЭП в ЭД
Подтверждение получения сертификата
Аннулирование сертификата
Приостановление действия сертификата
Возобновление действия сертификата
Подтверждение подлинности ЭП в ЭД
Подтверждение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

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



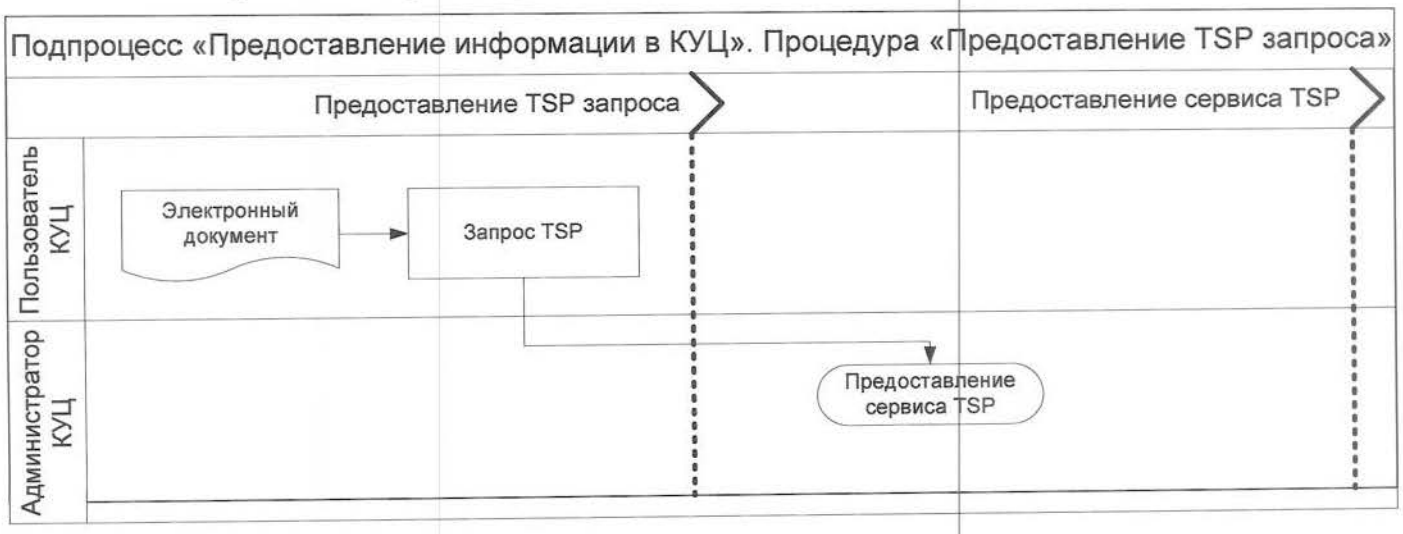
d) Схема процедуры « Предоставление информации по e-mail»:



е) Схема процедуры «Предоставление информации по телефону»:

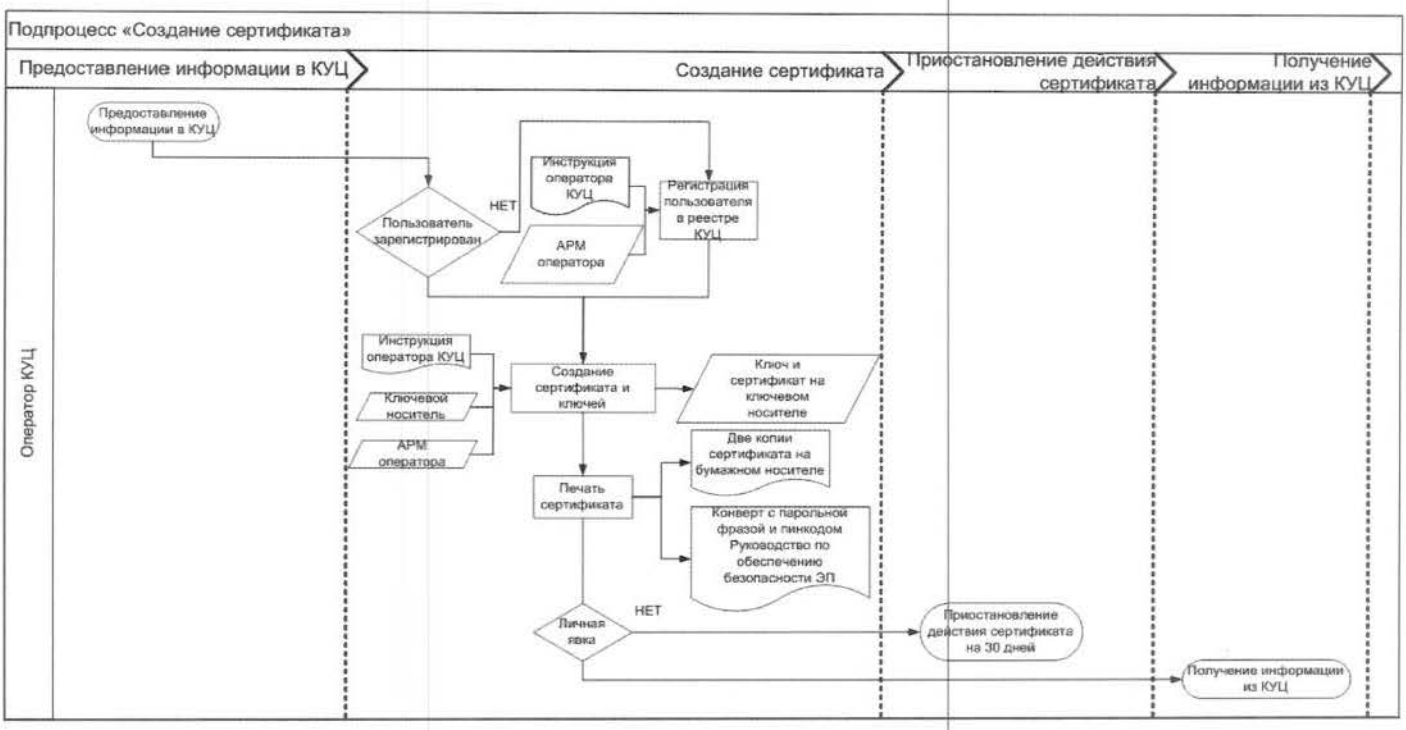
f) Схема процедуры «Предоставление OCSP запроса»:

g) Схема процедуры «Предоставление TSP запроса»:

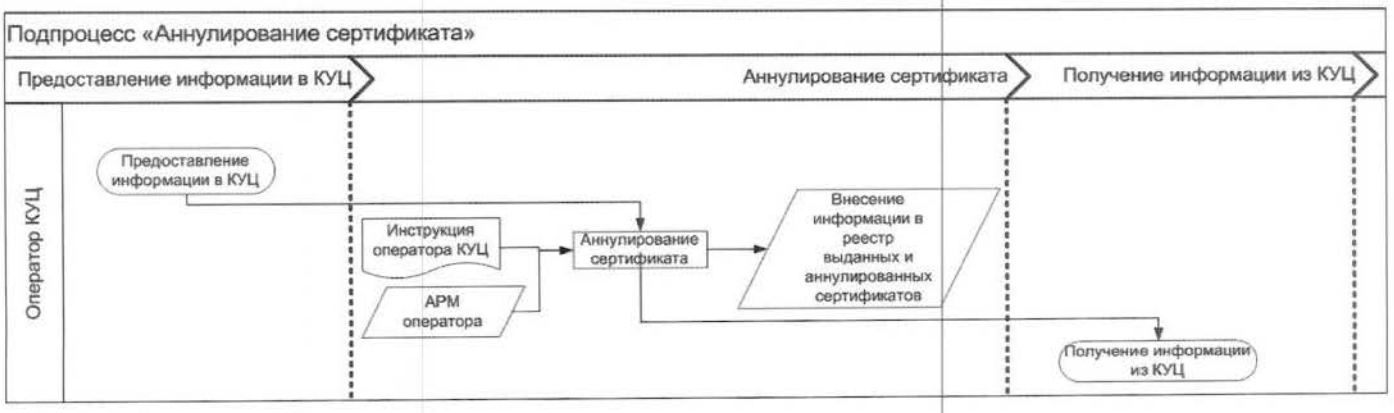


h) Схема процедуры «Предоставление официальной информации для принятия решения КУЦ»:

2. Схема подпроцесса «Создание сертификата»:



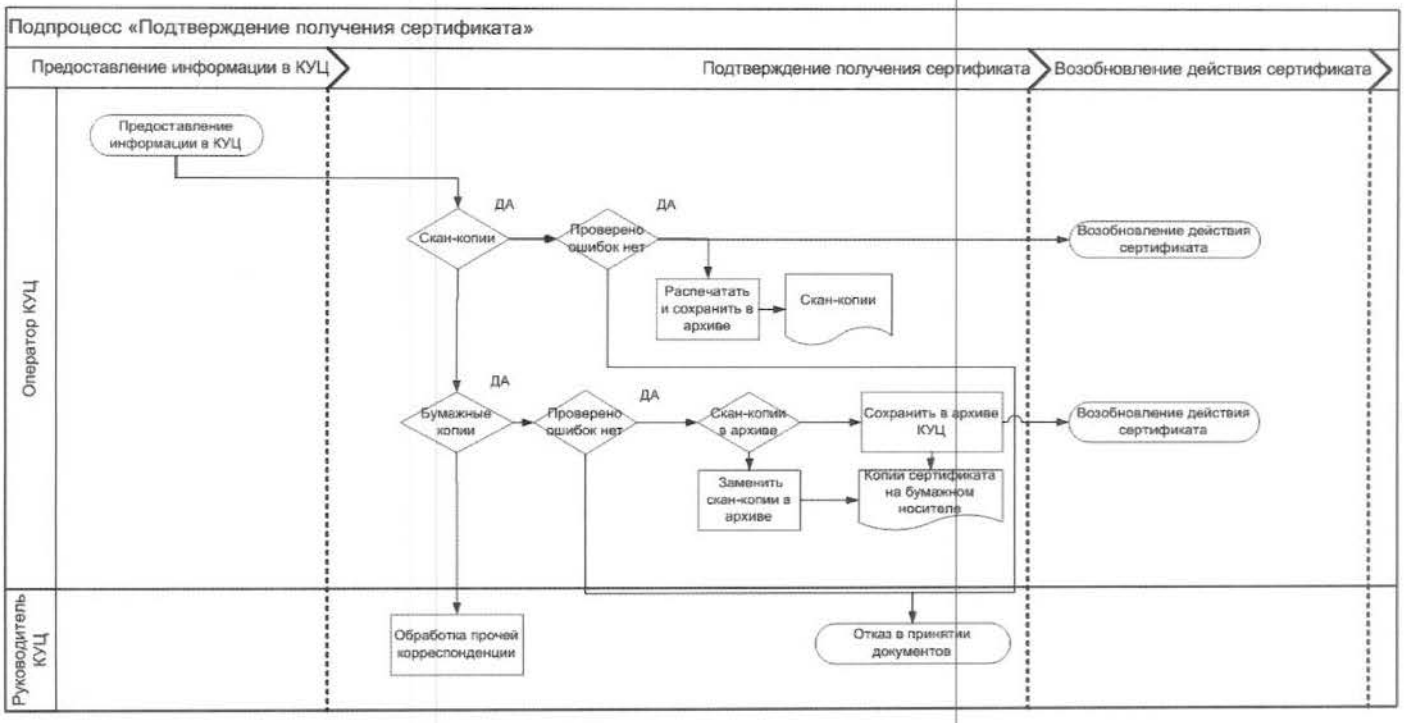
3. Схема подпроцесса «Аннулирование сертификата»:



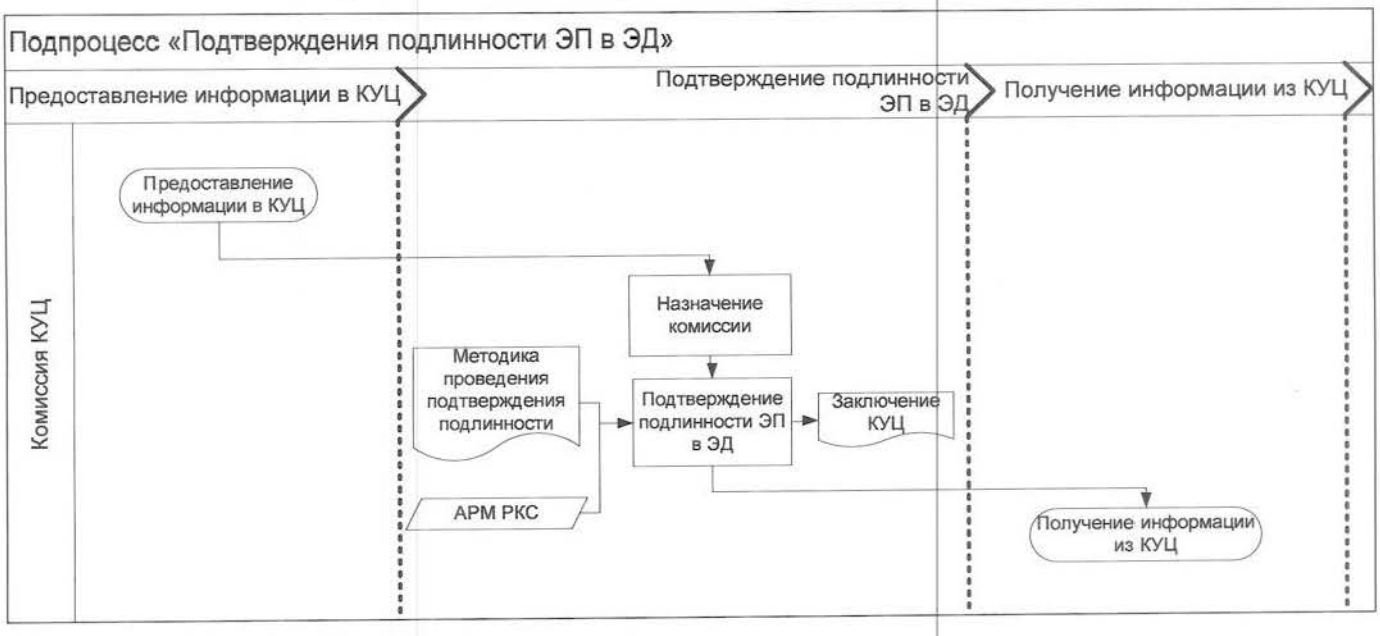
4. Схема подпроцесса «Приостановление действия сертификата»:

5. Схема подпроцесса «Возобновление действия сертификата»:

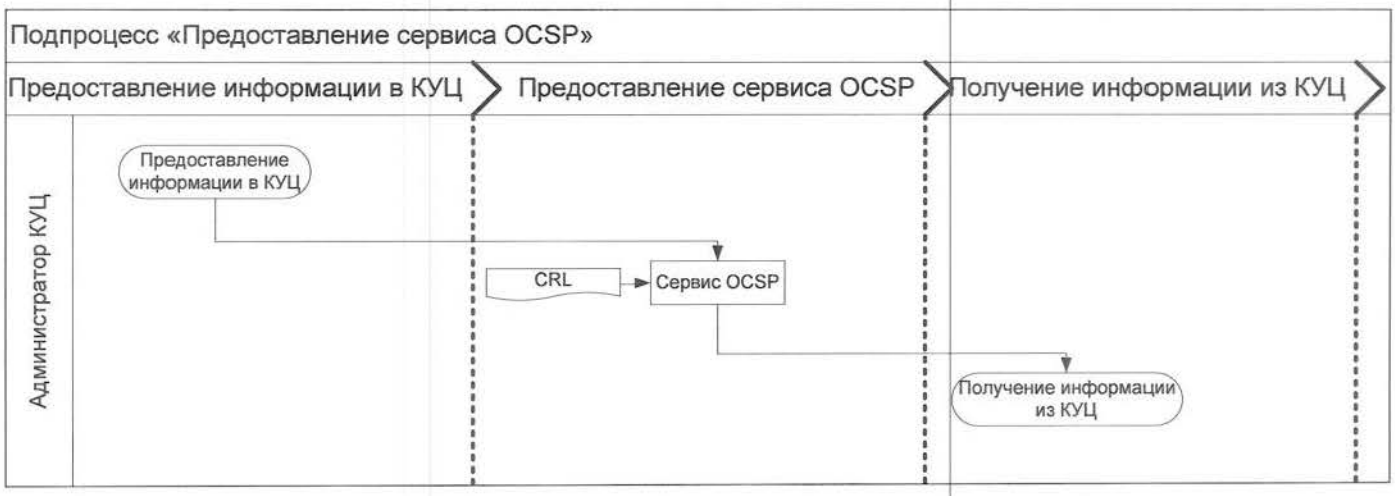
6. Схема подпроцесса «Подтверждение получения сертификата»:



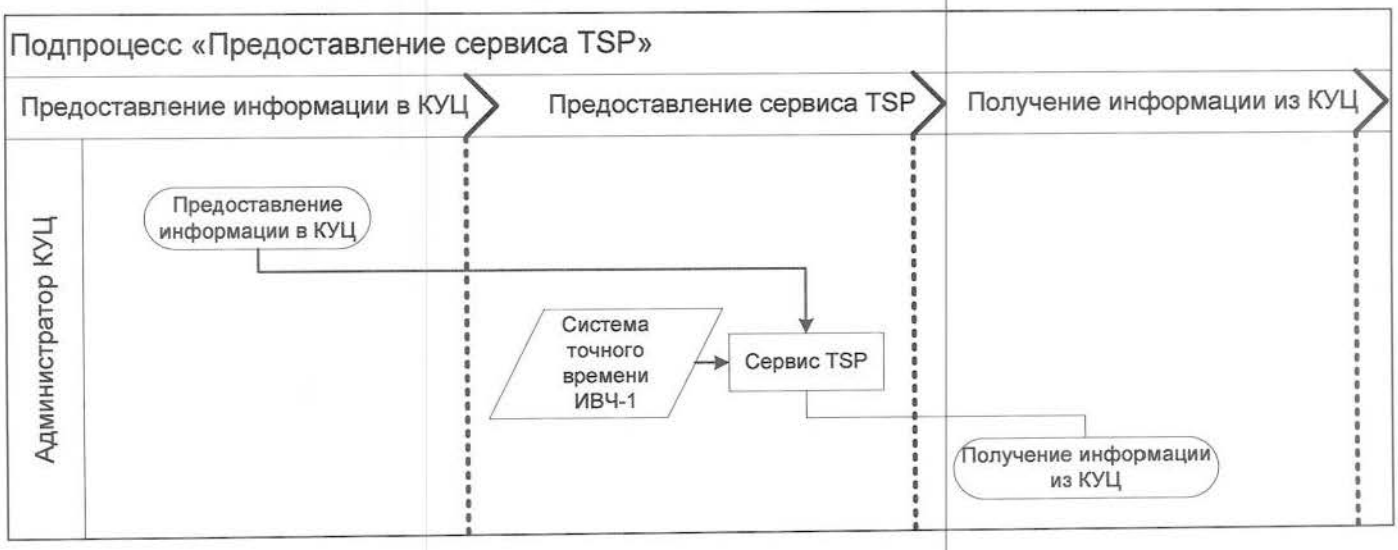
7. Схема подпроцесса «Подтверждение подлинности ЭП в ЭД»:



8. Схема подпроцесса «Предоставление сервиса OCSP»:

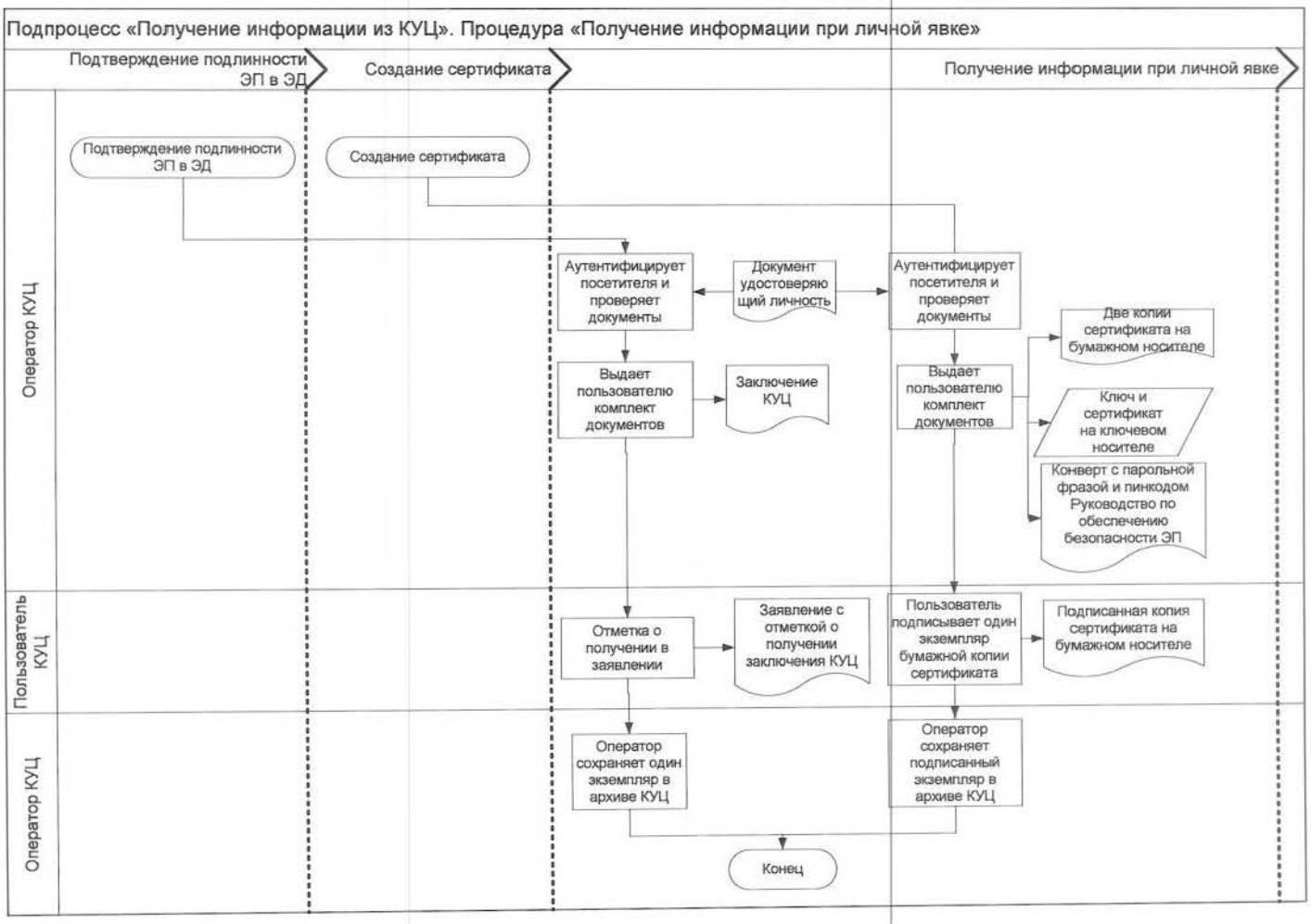


9. Схема подпроцесса «Предоставление сервиса TSP»:

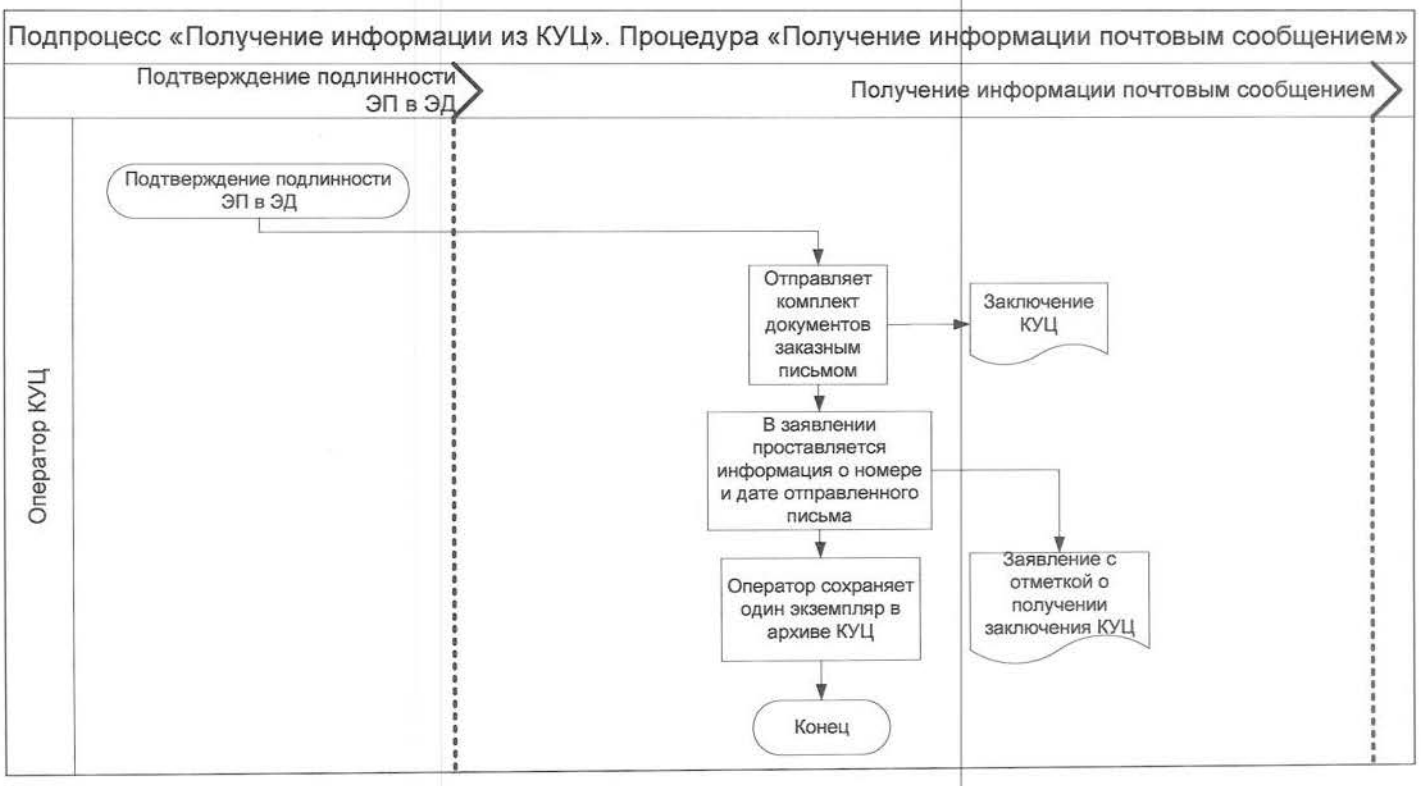


10.Подпроцесс «Получение информации из КУЦ»:

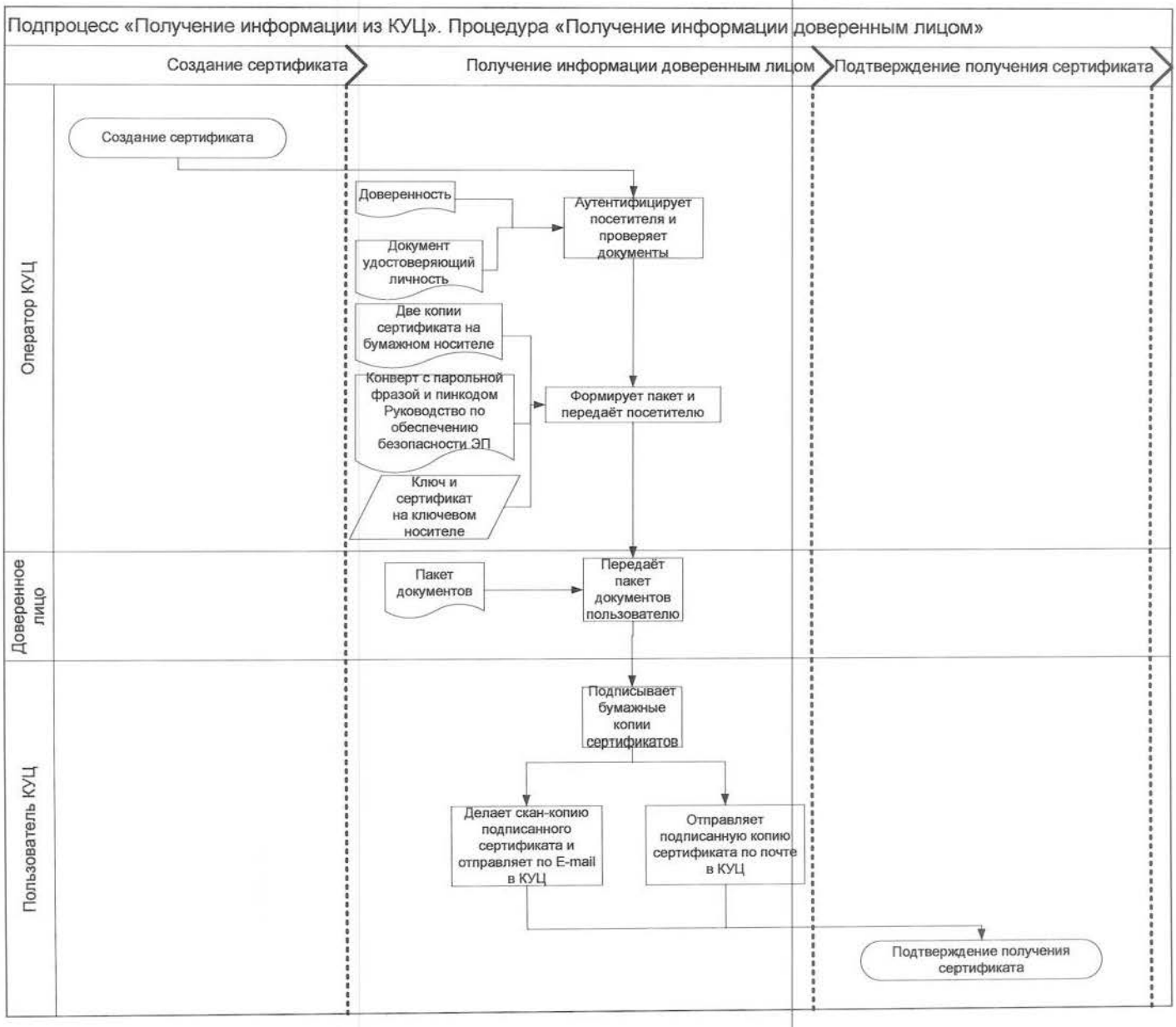
а) Схема процедуры «Получение информации при личной явке»:



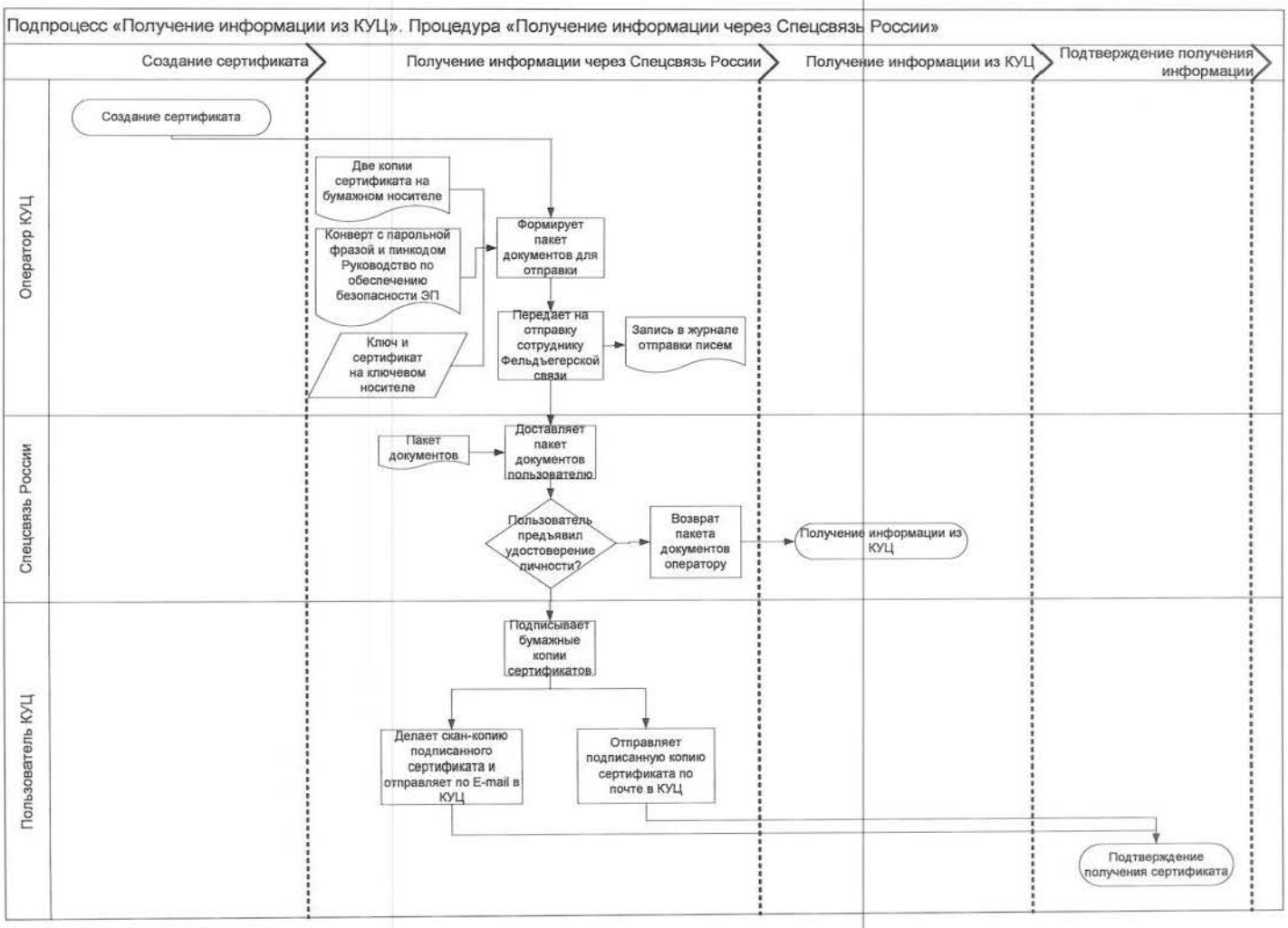
b) Схема процедуры «Получение информации почтовым сообщением»:



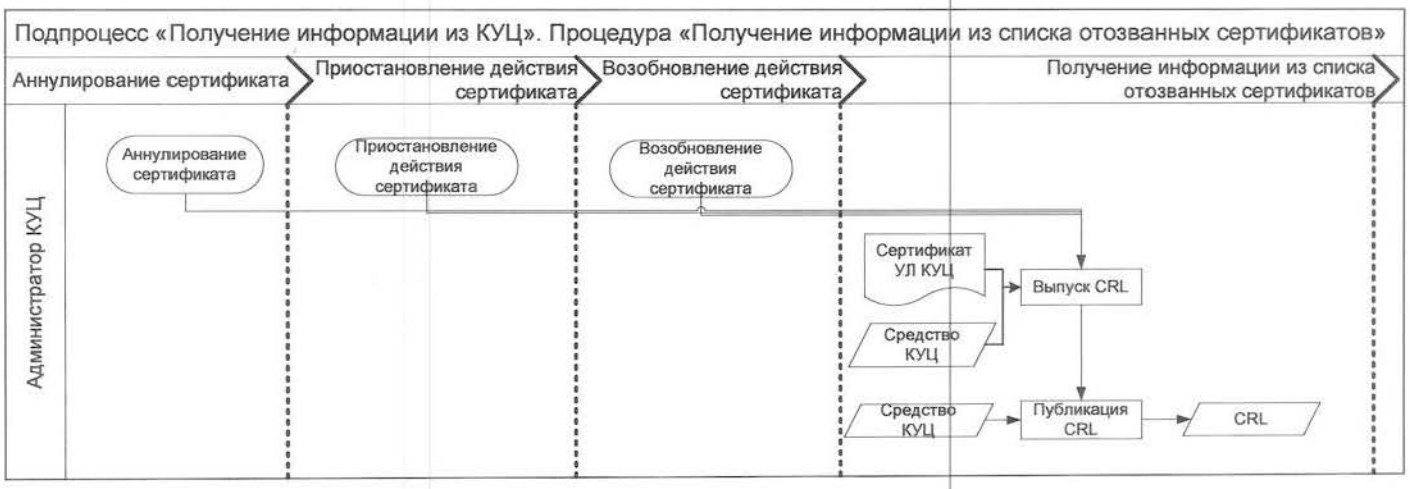
c) Схема процедуры «Получение информации доверенным лицом»:



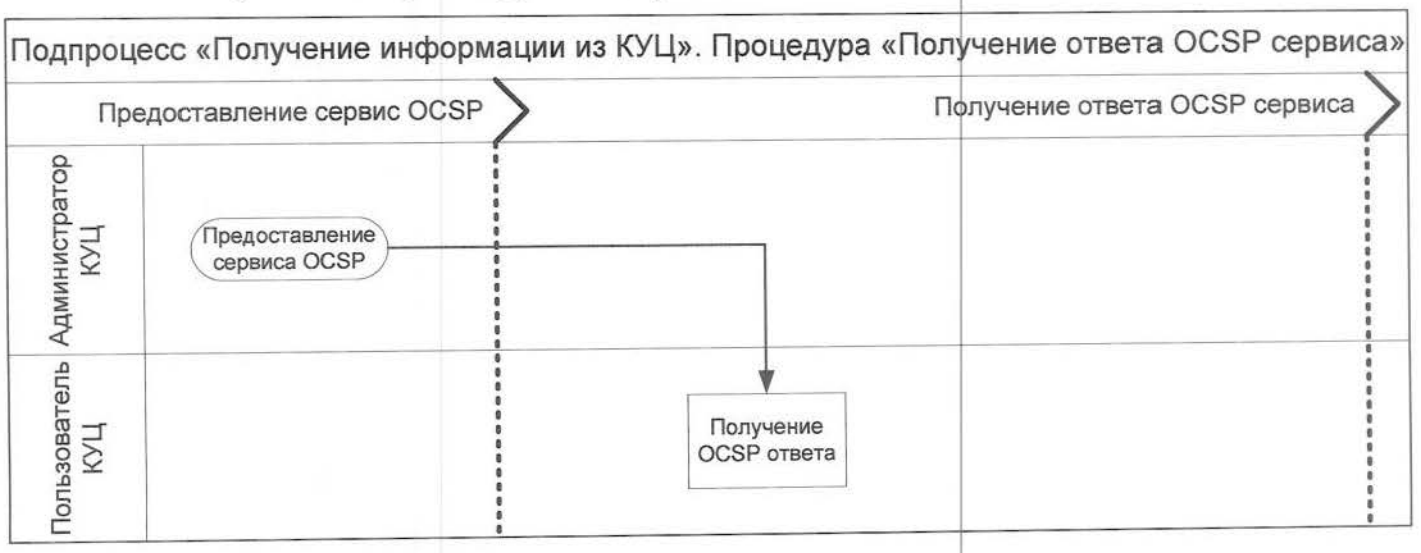
d) Схема процедуры «Получение информации через Спецсвязь России»:



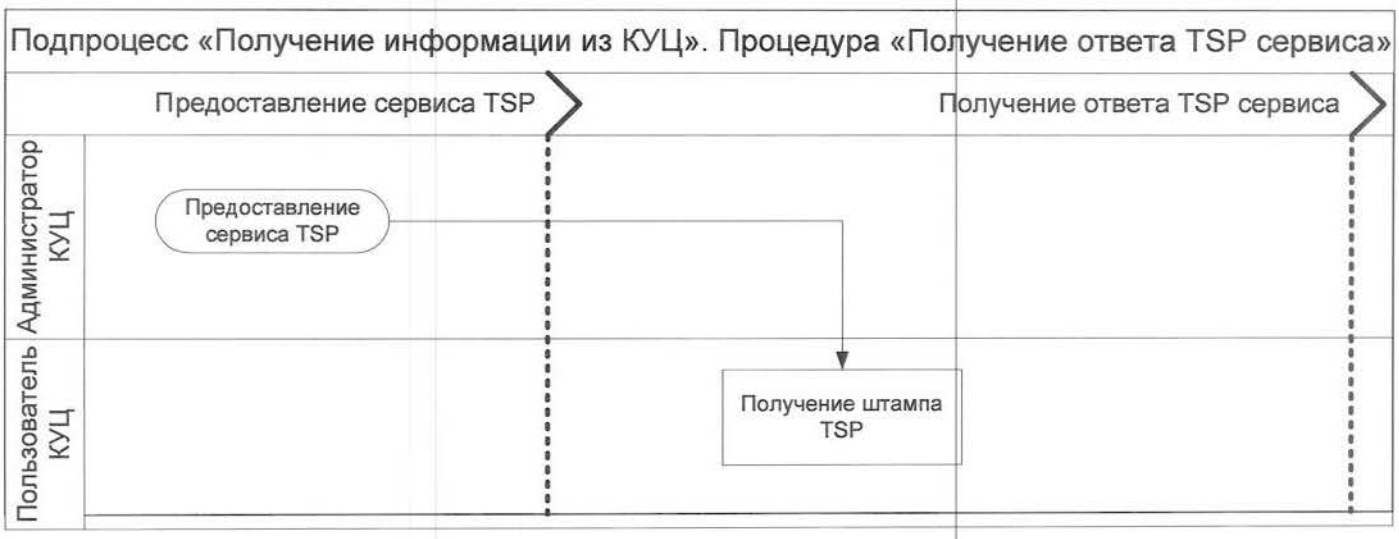
e) Схема процедуры «Получение информации из списков отозванных сертификатов»:



f) Схема процедуры «Получение ответа OCSP сервиса»:



g) Схема процедуры «Получение ответа TSP сервиса»:



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

Приложение №3

Дополнительные выходы и дополнительные входы

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

№ п/п	Наименование дополнительного входа процесса	Поставщик дополнительного входа процесса (группа процессов/ внешний контрагент)
1	Информация о заключенных договорах	ЗАО «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 ЗАО «Гринатом» и признает, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, относятся к общедоступным персональным данным.

Владелец сертификата ключа проверки электронной подписи _____/_____/

(подпись) (ФИО)

Уполномоченное должностное лицо

_____ _____/_____/

(Должность) (подпись) (ФИО)

М.П.

Приложение № 5

Правила заполнения заявлений на создание сертификатов ключей проверки электронной подписи

Правила заполнения заявлений на создание квалифицированного сертификатов ключа проверки электронной подписи

1. Общие положения

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

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

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

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

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

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

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

2. Правила заполнения полей заявления на создание сертификата

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

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

2.1. Формат поля Общее имя

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

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

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

– Длина текста – не более 64 символов.

2.2. Формат названия организации владельца сертификата.

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

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

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

2.3. Формат адреса организации владельца сертификата.

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

– Длина текста – не более 30 символов.

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

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

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

2.4. Формат названия населённого пункта.

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

– Длина текста – не более 128 символов.

– Вид населённого пункта указывается в начале текста без сокращения.

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

2.5. Формат названия региона (области).

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

– Длина текста – не более 128 символов.

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

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

2.6. Формат ИНН.

– Идентификационный номер налогоплательщика - юридического лица.

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

– Атрибут является обязательным.

– Разрешено использовать только цифровые символы 0123456789.

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

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

– Текст длиной 13 цифр - только для юридического лица.
– Атрибут является обязательным.
– Разрешено использовать только цифровые символы 0123456789.
– Запрещено использование ОГРН, не проходящих проверку корректности на контрольные разряды.

2.8. Формат названия страны

– Название страны, где зарегистрирована организация владельца сертификата, записывается в атрибут С субъекта сертификата, атрибут является обязательным.
– Длина текста – не более 2 символов.
– В поле название страны для организации, зарегистрированных на территории Российской Федерации указывается значение «RU»

3. Правила заполнения полей владельца сертификата.

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

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

3.1. Формат фамилии владельца сертификата владельца

– Фамилия сертификата записываются в атрибут SN субъекта сертификата
– Атрибут является не обязательным.
– Длина текста – не более 40 символов.
– При выпуске сертификата для тестовых целей в поле SN либо не заполняются, либо содержит информацию о тестовых целях сертификата. (например – «Для тестовых целей» или «Тест»)
– При выпуске сертификата аутентификации сервера поля SN не заполняется

3.2. Формат Имя и отчества владельца сертификата владельца

– Имя и отчество владельца сертификата записываются в атрибут GN субъекта сертификата к, атрибут является не обязательным.
– Длина текста – не более 64 символов.
– При выпуске сертификата для тестовых целей в поле GN либо не заполняются, либо содержит информацию о тестовых целях сертификата. (например – «Для тестовых целей» или «Тест»)
– При выпуске сертификата аутентификации сервера поле GN не заполняется.

3.3. Формат должности владельца сертификата.

– Должность владельца сертификата записывается в атрибут «Т» субъекта сертификата, атрибут не является обязательным.
– Длина текста – не более 64 символов.
– Кавычки, точки и прочие знаки пунктуации разрешается использовать только в том случае, если они встречаются внутри официального названия должности.

3.4. Формат подразделения организации владельца сертификата.

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

– Длина текста – не более 64 символов.

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

3.5. Формат адреса электронной почты владельца сертификата.

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

– Длина текста – не более 128 символов.

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

– Разрешается указывать только реальный адрес электронной почты.

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

– Текст длиной 14 символов - только для физического лица

– Атрибут является обязательным.

– Разрешено использовать только цифровые символы 0123456789.

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

3.7. Формат учётной записи в домене GK

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

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

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

4. Правила заполнения области ограничения использования квалифицированного сертификата.

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

5. Правила заполнения способа доставки ключевого носителя и сертификата.

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

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

6. Дополнительные положения.

6.1. Таблица 1 - Сокращения адреса

Сокращение	Название		Сокращение	Название
ул.	улица		ш.	шоссе

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

д.	дом
корп.	корпус
стр.	строение
кв.	квартира
п.	помещение

6.2. Таблица 2 - Справочник регионов

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

			округ
40	Калужская область	91	Республика Крым
41	Камчатский край	92	г. Севастополь
42	Кемеровская область	99	Иные территории, включая, г. Байконур
43	Кировская область		

6.3. Набор разрешённых символов в запросе на сертификат.

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

Таблица 3 - Разрешённые символы

№	Символ	Название			
1		пробел	74	w	латинская строчная буква w
2	"	универсальная кавычка	75	x	латинская строчная буква x
3	%	процент	76	y	латинская строчная буква y
4	&	амперсанд	77	z	латинская строчная буква z
5	'	апостроф	78	Ё	кириллическая заглавная буква Ё
6	(	левая скобка	79	«	двойная левая угловая кавычка
7	)	правая скобка	80	ё	кириллическая строчная буква ё
8	+	знак плюс	81	№	знак номер
9	,	запятая	82	»	двойная правая угловая кавычка
10	-	дефис	83	А	кириллическая заглавная буква А
11	,	точка	84	Б	кириллическая заглавная буква Б
12	0	цифра ноль	85	В	кириллическая заглавная буква В
13	1	цифра один	86	Г	кириллическая заглавная буква Г
14	2	цифра два	87	Д	кириллическая заглавная буква Д
15	3	цифра три	88	Е	кириллическая заглавная буква Е
16	4	цифра четыре	90	Ж	кириллическая заглавная буква Ж
17	5	цифра пять	91	З	кириллическая заглавная буква З
18	6	цифра шесть	92	И	кириллическая заглавная буква И
19	7	цифра семь	93	Й	кириллическая заглавная буква Й
20	8	цифра восемь	94	К	кириллическая заглавная буква К
21	9	цифра девять	95	Л	кириллическая заглавная буква Л
22	:	двоеточие	96	М	кириллическая заглавная буква М
23	;	точка с запятой	97	Н	кириллическая заглавная буква Н
24	@	коммерческое ат «собачка»	98	О	кириллическая заглавная буква О
25	A	латинская заглавная буква A	99	П	кириллическая заглавная буква П
26	B	латинская заглавная буква B	100	Р	кириллическая заглавная буква Р
27	C	латинская заглавная буква C	101	С	кириллическая заглавная буква С
28	D	латинская заглавная буква D	102	Т	кириллическая заглавная буква Т
29	E	латинская заглавная буква E	103	У	кириллическая заглавная буква У
30	F	латинская заглавная буква F	104	Ф	кириллическая заглавная буква Ф
31	G	латинская заглавная буква G	105	Х	кириллическая заглавная буква Х
32	H	латинская заглавная буква H	106	Ц	кириллическая заглавная буква Ц
33	I	латинская заглавная буква I	107	Ч	кириллическая заглавная буква Ч
34	J	латинская заглавная буква J	108	Ш	кириллическая заглавная буква Ш
35	K	латинская заглавная буква K	109	Щ	кириллическая заглавная буква Щ

36	L	латинская заглавная буква L	110	Ъ	кириллическая заглавная буква Ъ
37	M	латинская заглавная буква M	111	Ы	кириллическая заглавная буква Ы
38	N	латинская заглавная буква N	112	Ь	кириллическая заглавная буква Ь
39	O	латинская заглавная буква O	113	Э	кириллическая заглавная буква Э
40	P	латинская заглавная буква P	114	Ю	кириллическая заглавная буква Ю
41	Q	латинская заглавная буква Q	115	Я	кириллическая заглавная буква Я
42	R	латинская заглавная буква R	116	а	кириллическая строчная буква а
43	S	латинская заглавная буква S	117	б	кириллическая строчная буква б
44	T	латинская заглавная буква T	118	в	кириллическая строчная буква в
45	U	латинская заглавная буква U	119	г	кириллическая строчная буква г
46	V	латинская заглавная буква V	120	д	кириллическая строчная буква д
47	W	латинская заглавная буква W	121	е	кириллическая строчная буква е
48	X	латинская заглавная буква X	122	ж	кириллическая строчная буква ж
49	Y	латинская заглавная буква Y	123	з	кириллическая строчная буква з
50	Z	латинская заглавная буква Z	124	и	кириллическая строчная буква и
51	_	подчеркивание	125	й	кириллическая строчная буква й
52	a	латинская строчная буква a	126	к	кириллическая строчная буква к
53	b	латинская строчная буква b	127	л	кириллическая строчная буква л
54	c	латинская строчная буква c	128	м	кириллическая строчная буква м
55	d	латинская строчная буква d	129	н	кириллическая строчная буква н
56	e	латинская строчная буква e	130	о	кириллическая строчная буква о
57	f	латинская строчная буква f	131	п	кириллическая строчная буква п
58	g	латинская строчная буква g	132	р	кириллическая строчная буква р
59	h	латинская строчная буква h	133	с	кириллическая строчная буква с
60	i	латинская строчная буква i	134	т	кириллическая строчная буква т
61	j	латинская строчная буква j	135	у	кириллическая строчная буква у
62	k	латинская строчная буква k	136	ф	кириллическая строчная буква ф
63	l	латинская строчная буква l	137	х	кириллическая строчная буква х
64	m	латинская строчная буква m	138	ц	кириллическая строчная буква ц
65	n	латинская строчная буква n	139	ч	кириллическая строчная буква ч
66	o	латинская строчная буква o	140	ш	кириллическая строчная буква ш
67	p	латинская строчная буква p	141	щ	кириллическая строчная буква щ
68	q	латинская строчная буква q	142	ъ	кириллическая строчная буква ъ
69	r	латинская строчная буква r	143	ы	кириллическая строчная буква ы
70	s	латинская строчная буква s	144	ь	кириллическая строчная буква ь
71	t	латинская строчная буква t	145	э	кириллическая строчная буква э
72	u	латинская строчная буква u	146	ю	кириллическая строчная буква ю
73	v	латинская строчная буква v	147	я	кириллическая строчная буква я

Приложение № 6

Форма доверенности пользователя удостоверяющего центра

Доверенность

_____ «_____» _____ 20___ г.

_____

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____

(должность)

_____

(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и когда выдан)

1. Получить сертификат ключа проверки электронной подписи в Корпоративном удостоверяющем центре Госкорпорации «Росатом».

2. При использовании электронной подписи электронных документов, выступать в роли Пользователя Удостоверяющего центра и осуществлять действия в рамках Регламента Удостоверяющего центра по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи, установленные для Пользователя Удостоверяющего центра.

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

Подпись пользователя Удостоверяющего центра_____ _____,

фамилия, имя, отчество подпись

подтверждаю.

Уполномоченное должностное лицо

_____ _____ / _____ /

подпись Ф.И.О.

М.П.

_____

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

Приложение № 7

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

Доверенность

_____ «_____» _____ 20___ г.

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____

(должность)

_____

(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и когда выдан)

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

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

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

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

Полномочия по настоящей доверенности не могут быть переданы другим лицам.

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

Подпись доверенного лица _____ _____,

фамилия, имя, отчество подпись

подтверждаю.

Уполномоченное должностное лицо

_____ _____ / _____ /

подпись Ф.И.О.

Приложение № 8

Заявление на аннулирование сертификата ключа проверки электронной подписи

«_____» _____ 201__ г.

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____,

должность

_____,

фамилия, имя, отчество

действующего на основании _____

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

Серийный номер сертификата	
Причина аннулирования сертификата	

Владелец сертификата ключа проверки электронной подписи _____/_____/

(подпись) (ФИО)

Уполномоченное должностное лицо

_____ _____/_____/

(подпись) (ФИО)

«___»_____201__ г. М.П.

Отметки удостоверяющего центра

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

_____/_____/

«___»_____201__ г.

Приложение № 9

Заявление на приостановление действия сертификата ключа проверки электронной подписи

«_____» _____ 201__ г.

_____

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____,

должность

_____,

фамилия, имя, отчество

действующего на основании _____

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

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

Владелец сертификата ключа проверки электронной подписи _____/_____/

(подпись) (ФИО)

Уполномоченное должностное лицо

_____ _____/_____/

(подпись) (ФИО)

«___»_____201__ г. М.П.

Отметки удостоверяющего центра

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

_____/_____/

«___»_____201__ г.

Приложение № 10

Заявление на возобновление действия сертификата ключа проверки электронной подписи

«_____» _____ 201__ г.

_____

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____,

должность

_____,

фамилия, имя, отчество

действующего на основании _____

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

Серийный номер сертификата	

Владелец сертификата ключа проверки электронной подписи _____/_____/

(подпись) (ФИО)

Уполномоченное должностное лицо

_____ _____/_____/

(подпись) (ФИО)

«___»_____201__ г. М.П.

Отметки удостоверяющего центра

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

_____/_____/

«___»_____201__ г.

Приложение № 11

Заявление на подтверждение подлинности электронной подписи в электронном документе

«_____» _____ 201__ г.

_____

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____,

должность

_____,

фамилия, имя, отчество

действующего на основании _____

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

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

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

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

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

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

Владелец сертификата ключа проверки электронной подписи _____/_____/

(подпись) (ФИО)

Уполномоченное должностное лицо

_____ _____/_____/

(подпись) (ФИО)

«___»_____201__ г. М.П.

Отметки удостоверяющего центра

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

«___»_____201__ г.

Заключение о подтверждении подлинности ЭП получено пользователем _____/_____/

_____ «___»_____201__ г.

Приложение № 12

Форма копии сертификата на бумажном носителе

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

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

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

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

Приложение № 13

Формат сертификата ключа проверки электронной подписи

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

Приложение № 14

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

Пользователь КУЦ обязан:

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

Пользователю КУЦ запрещается:

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

Пользователь КУЦ несёт ответственность за:

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

Приложение № 15

Ограничения использования сертификатов ключей проверки электронной подписи

1. Квалифицированный сертификат Госкорпорации «Росатом»

Данные сертификаты ключа проверки электронной подписи предназначены для:

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

В сертификате указываются следующие ограничения:

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

В поле улучшенный ключ:

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

Срок действия сертификата - 1 год и 3 месяца.

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

2. Квалифицированная подпись в ЕОСДО

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

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В сертификате указываются следующие ограничения:

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

Срок действия сертификата - 1 год и 3 месяца.

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

3. Аутентификация сервера

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

- Аутентификация сервера.

В сертификате указываются следующие дополнительные поля:

В поле улучшенный ключ:

- Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

Срок действия сертификата - 1 год и 3 месяца.

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

4. Клиент S-Terra (КСПД)

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

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

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В сертификате указываются следующие дополнительные поля:

В поле улучшенный ключ:

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

Срок действия сертификата - 1 год и 3 месяца.

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

5. Шлюз КСПД

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

– Узел Корпоративной системы передачи данных;

В сертификате указываются следующие дополнительные поля:

В поле улучшенный ключ:

– Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

Срок действия сертификата - 1 год и 3 месяца.

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

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

6. СЦУД

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

В сертификате указываются следующие ограничения:

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В поле улучшенный ключ:

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

Срок действия сертификата - 1 год и 3 месяца.

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

7. Тестовый сертификат

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

В сертификате указываются следующие дополнительные поля:

– Временный доступ к центру регистрации (1.2.643.2.2.34.2)

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

Срок действия сертификата - 2 месяца.

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

- 1.2.643.100.113.1 - класс средства ЭП КС 1

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 06 июля 2012 г.

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 №2

Москва 2015 г.

Оглавление

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 (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 ЗАО «Гринатом»;
3. Администратор безопасности ОКЗ ЗАО «Гринатом»;
4. Руководитель ЗАО «Гринатом»;
5. Начальник Управления информационной безопасности ЗАО «Гринатом»;
6. Руководитель Органа криптографической защиты ЗАО «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 №0011890 Рег.№14464 Н от 23.07.2015 на	Действует	Лицензия	Данилов С.Н.

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)			
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)	Действует	Приказ	Данилов С.Н.

средств защиты информации (Положение ПКЗ-2005)»			
Положение о системе Регламентирующих документов Госкорпорации «Росатом», утв. Приказом от 21.12.2012 № 1/1247-П	Действует	Приказ	Первый заместитель генерального директора ГК «Росатом» Соломон Н.И.
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, эксплуатационной и технической документации
Конфиденциальная информация	Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну
Обладатели конфиденциальной информации	Государственные органы, государственные организации и другие организации независимо от их организационно-правовой формы и формы собственности, индивидуальные предприниматели и физические лица
Орган криптографической защиты	Действующая на постоянной основе рабочая группа из числа сотрудников Управления информационной безопасности
Пользователи СКЗИ	Физические лица, непосредственно допущенные к работе с СКЗИ
Средства криптографической защиты информации (СКЗИ)	Средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче; средства имитозащиты - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности

	и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации; средства электронной подписи; средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций; средства изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств; ключевые документы - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах; аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие

	возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин; программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств; программно-аппаратные шифровальные (криптографические) средства - устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.
Электронная подпись	информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с

	такой информацией и которая используется для определения лица, подписывающего информацию

Сокращение	Расшифровка
АБ	Администратор безопасности ОКЗ ЗАО «Гринатом»
ООКИ	Организация-обладатель конфиденциальной информации
КУЦ	Корпоративный Удостоверяющий центр Госкорпорации «Росатом»
ОКЗ	Орган криптографической защиты ЗАО «Гринатом»
Руководитель ООКИ	Руководитель организации-обладателя конфиденциальной информации
СКЗИ	Средства 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	• 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; • Согласовывает 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».

2	Аналитик ОКЗ ЗАО «Гринатом» (далее – Аналитик)	• Разрабатывает и поддерживает в актуальном состоянии схему криптографической защиты информации; • Определять требования к защищенности различных информационных систем в соответствии с действующей нормативно-методической документацией; • Составляет заключение о возможности эксплуатации СКЗИ; • Формирует комплект поставки СКЗИ; • Учитывает СКЗИ в ОКЗ; • Отправляет СКЗИ в ООКИ; • Обрабатывает заключения по результатам контроля безопасности рабочих мест с установленными СКЗИ.
3	Администратор безопасности ОКЗ ЗАО «Гринатом» (далее – АБ)	• 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; • Проводит расследования по фактам нарушений использования СКЗИ; • Уничтожает выведенные из действия СКЗИ.
4	Руководитель ЗАО «Гринатом»	• Согласовывает Приказ о проведении проверки требований Регламента.

5	Начальник Управления информационной безопасности ЗАО «Гринатом»	• Согласовывает документы, необходимые для предоставления услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.
6	Руководитель Органа криптографической защиты ЗАО «Гринатом»	• Согласовывает документы, необходимые для предоставления услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.
7	Проверяющий	• Подготавливает документы для проведения проверок выполнения требований Регламента; • Осуществляет проверки выполнения требований Регламента; • Отчитывается по результатам проведения проверок выполнения требований Регламента.

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, ЗАО «Гринатом»	Организация
2	Перечень лиц,	Предприятие, ЗАО «Гринатом»	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)		
		Группа процессов/ внешний контрагент		Уровень управления (Корпорация,/ Дивизион/ Организация)
	допускаемых к самостоятельной работе с СКЗИ			
3	Приказ о назначении прав подписей Пользователей СКЗИ	Предприятие, ЗАО «Гринатом»		Организация
4	Схема организации криптографической защиты информации	ЗАО «Гринатом»		Организация
5	СКЗИ	Предприятие		Организация
6	Книга лицевых счетов	ЗАО «Гринатом»		Организация
7	Доверенность на получение АБ СКЗИ из банка	Предприятие		Организация
8	Акт приема-передачи банковского ПО и СКЗИ	Предприятие		Организация
9	Акт повреждения упаковки	ЗАО «Гринатом»		Организация
10	Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)	Предприятие, ЗАО «Гринатом»		Организация
11	Аппаратный журнал	Предприятие, ЗАО «Гринатом»		Организация
12	Акт готовности к работе СКЗИ	Предприятие, ЗАО «Гринатом»		Организация
13	Учтенные ключевые носители	Предприятие		Организация
14	Ключевой носитель с ключевой информацией	Предприятие		Организация
15	Сертификаты	Предприятие		Организация
16	Зарегистрированные	Предприятие		Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)		
		Группа процессов/ внешний контрагент		Уровень управления (Корпорация,/ Дивизион/ Организация)
	сертификаты			
17	Ведомость сдачи зачетов	Предприятие, ЗАО «Гринатом»		Организация
18	Заключение о возможности эксплуатации СКЗИ	Предприятие, ЗАО «Гринатом»		Организация
19	Журнал учета выполнения регламентных работ	Предприятие, ЗАО «Гринатом»		Организация
20	Заключение по результатам контроля безопасности АРМ с установленным СКЗИ	Предприятие, ЗАО «Гринатом»		Организация
21	Отчет по результатам ежегодного контроля (если проверку проводит АБ)	Предприятие, ЗАО «Гринатом»		Организация
22	Заключение по факту нарушения условий использования СКЗИ	Предприятие, ЗАО «Гринатом»		Организация
23	Решение Руководителя ООКИ о выводе СКЗИ из эксплуатации	Предприятие, ЗАО «Гринатом»		Организация
24	Акт об уничтожении СКЗИ	Предприятие, ЗАО «Гринатом»		Организация
25	Приказ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом,	Предприятие, ЗАО «Гринатом»		Организация

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

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)		
		Группа процессов/ внешний контрагент		Уровень управления (Корпорация,/ Дивизион/ Организация)
30	Отчет о проверке 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	ЗАО «Гринатом»		Организация

3.5. Основные входы процесса

№ п/п	Наименование основного входа процесса	Поставщик основного входа		
		Группа процессов/ внешний контрагент		Уровень управления (Корпорация/ Дивизион/ Организация).
1	Отраслевые требования по информационной безопасности ГК «Росатом» №1/910-П-дсп от 23.09.2014	ГК «Росатом»		Корпорация
2	Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам	Предприятие		Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа		
		Группа процессов/ внешний контрагент		Уровень управления (Корпорация/ Дивизион/ Организация).
	связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (с передачей СКЗИ на предприятие)			
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	Приказ о назначении администраторов безопасности и лиц их замещающих	Предприятие		Организация
5	Перечень лиц, допускаемых к самостоятельной работе с СКЗИ	Предприятие		Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа		
		Группа процессов/ внешний контрагент		Уровень управления (Корпорация/ Дивизион/ Организация).
6	Приказ о назначении прав подписей Пользователей СКЗИ	Предприятие		Организация
7	Решение Руководителя ООКИ о выводе СКЗИ из эксплуатации	Предприятие		Организация
8	Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)	Предприятие		Организация
9	Схема организации криптографической защиты конфиденциальной информации	ЗАО «Гринатом»		Организация
10	Акт повреждения упаковки	Предприятие		Организация
11	СКЗИ	ЗАО «Гринатом»		Организация
12	Сопроводительное письмо к СКЗИ	ЗАО «Гринатом»		Организация
13	Инструкция по установке СКЗИ	ЗАО «Гринатом»		Организация
14	Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ	ЗАО «Гринатом»		Организация
15	Учтенные ключевые носители	Предприятие		Организация
16	Сертификаты	Банк		Организация
17	Учебные материалы	ЗАО «Гринатом»		Организация
18	Аппаратный журнал	Предприятие		Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа		
		Группа процессов/ внешний контрагент		Уровень управления (Корпорация/ Дивизион/ Организация).
19	Ведомость сдачи зачетов	Предприятие		Организация
20	Акт готовности СКЗИ к эксплуатации	Предприятие		Организация
21	Эксплуатационная и техническая документация к СКЗИ	ЗАО «Гринатом»		Организация
22	Заключение по результатам контроля безопасности АРМ	Предприятие		Организация
23	Отчет по результатам ежегодного контроля (если проверку проводит АБ)	ЗАО «Гринатом»		Организация
24	Журнал учета выполнения регламентных работ	Предприятие		Организация
25	Договор об оказании Банком услуг ДБО с использованием СКЗИ	Предприятие, Банк		Организация
26	Заключение по факту нарушения условий использования СКЗИ	Предприятие		Организация
27	Решение Руководителя ООКИ о выводе СКЗИ из эксплуатации	Предприятие		Организация
28	Акт об уничтожении СКЗИ	Предприятие		Организация
29	Приказ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом,	ЗАО «Гринатом»		Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа		
		Группа процессов/ внешний контрагент		Уровень управления (Корпорация/ Дивизион/ Организация).
	не содержащей сведений, составляющих государственную тайну в ООКИ			
30	План-график проведения проверок на год	ЗАО «Гринатом»		Организация
31	Письмо о проведении проверки работ по договору присоединения на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств	ЗАО «Гринатом»		Организация
32	Сводная таблица по объекту проверки	ЗАО «Гринатом»		Организация
33	Программа проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ	ЗАО «Гринатом»		Организация
34	Контрольный список проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств	ЗАО «Гринатом»		Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа		
		Группа процессов/ внешний контрагент		Уровень управления (Корпорация/ Дивизион/ Организация).
	криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ			
35	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	ЗАО «Гринатом»		Организация
36	Отчет о проверке 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	ЗАО «Гринатом»		Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа		
		Группа процессов/ внешний контрагент		Уровень управления (Корпорация/ Дивизион/ Организация).
37	План реализации рекомендаций по результатам проверки лицензиата ФСБ России ЗАО «Гринатом» в ООКИ	Предприятие		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»

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 ЗАО «Гринатом» (Приложение №5). В рамках услуги GEN.23 ЗАО «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 АС (Приложение №7) (в случае если такие права предоставляются);
- Направляет в адрес ОКЗ ЗАО «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 ЗАО «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 ЗАО «Гринатом» не передает СКЗИ на предприятие;
  - Скан-копию Приказа о назначении АБ и лиц их замещающих;
  - Скан-копию Перечня лиц, допускаемых к самостоятельной работе с СКЗИ;
  - Скан-копию Приказа о предоставлении прав подписей пользователей СКЗИ.

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 (оформляется в виде распоряжения или иного документа.

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 в ООКИ» или из подпроцесса «Вывод из эксплуатации и уничтожение СКЗИ». Исходящая информация поступает в подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ», или в подпроцесс «Проверка выполнения требований Регламента» или в конец процесса..

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), Приказа о назначении АБ и лиц их замещающих, Перечня

лиц, допускаемых к самостоятельной работе с СКЗИ, Приказа о предоставлении прав подписей Пользователей СКЗИ, Решения Руководителя ООКИ о выводе СКЗИ из эксплуатации, Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации), Акта об уничтожении СКЗИ, Акта повреждения упаковки.

Начальник управления информационной безопасности ЗАО «Гринатом»:

- Утверждает Схему.

Если Аналитику пришла информация о выводе из действия и уничтожении СКЗИ, то процесс взаимодействия ОКЗ и ООКИ завершается.

Руководитель ЗАО «Гринатом»:

- Принимает решение о проведении проверки выполнения требований Регламента;
- Согласовывает 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 (Приложение №25) и План-график проведения проверок на год (Приложение №26).

Если настало время проведения проверки выполнения требований Регламента, то исходящая информация поступает в подпроцесс «Проверка выполнения требований Регламента».

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

Аналитик:

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

3.6.4. Подпроцесс «Отправка и получение СКЗИ»

Входящая информация поступает из подпроцесса «Формирование комплекта поставки СКЗИ и учет СКЗИ». Исходящая информация поступает в подпроцесс «Учет СКЗИ в ООКИ».

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 или Пользователя СКЗИ, для которых эти упаковки предназначены. На упаковках для Пользователя СКЗИ Аналитик делает пометку «Лично». Упаковки опечатывает таким образом, чтобы исключить возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.
  Помещает во внешнюю упаковку при предъявлении фельдсвязью дополнительных требований;
- Подготавливает сопроводительное письмо (Приложение №12), в котором указывает, что посылается и в каком количестве, учетные номера изделий и/или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывает в одну из упаковок.

АБ:

- Получает упаковку с СКЗИ;
- Составляет и направляет в адрес ОКЗ ЗАО «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 ЗАО «Гринатом» о дальнейшем применении СКЗИ (*в случае составления акта повреждения упаковки*).

В случае если СКЗИ получаются из банка:

АБ:

- Оформляет доверенность на себя на получение ПО и СКЗИ из банка;
- Получает в банке ПО и СКЗИ по доверенности;
- Подписывает акт приема-передачи банковского ПО и СКЗИ по форме, установленной банком.

3.6.5. Подпроцесс «Учет СКЗИ в ООКИ»

Входящая информация поступает из подпроцесса «Отправка и получение СКЗИ». Исходящая информация поступает в подпроцесс «Установка и настройка 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 ЗАО «Гринатом» в соответствии с порядком, указанным в сопроводительном письме

Все полученные АБ экземпляры СКЗИ, эксплуатационная и техническая документация к ним должны быть выданы под расписку в Журнале учета (для обладателя конфиденциальной информации) Пользователям СКЗИ, несущим персональную ответственность за их сохранность.

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

3.6.6. Подпроцесс «Установка и настройка СКЗИ»

Входящая информация поступает из подпроцесса «Учет СКЗИ в ООКИ». Исходящая информация поступает в подпроцесс «Генерация ключевой информации».

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 Аппаратном журнале (Приложение №16).
  Аппаратный журнал ведется в случае ввода ключевой информации на весь срок эксплуатации.
- Составляет Акт готовности СКЗИ к эксплуатации (Приложение №17);

3.6.7. Подпроцесс «Генерация ключевой информации»

Входящая информация поступает из подпроцесса «Установка и настройка СКЗИ». Исходящая информация поступает в подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ».

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

АБ (в случае если СКЗИ получаются из банка):

- Ставит на учет носители информации в качестве ключевых;

Производит генерацию ключевой информации Пользователей и учитывает факт генерации и передачи Пользователям в Журнал 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.

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

Входящая информация поступает из подпроцесса «Генерация ключевой информации». Исходящая информация поступает в подпроцесс «Принятие решения о возможности эксплуатации СКЗИ».

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 (Приложение №19) и заполняет Ведомость сдачи зачетов (Приложение №20);
- Направляет в адрес ОКЗ ЗАО «Гринатом» следующий комплект документов:
  - скан-копию Журнала учета (для обладателя конфиденциальной информации);
  - скан-копию Аппаратного журнала (*в случае если он ведется*);
  - скан-копию Ведомости сдачи зачетов;
  - скан-копию Акта готовности СКЗИ к эксплуатации.

3.6.9. Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»

Входящая информация поступает из подпроцесса «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ». Исходящая информация поступает в подпроцесс «Обеспечение функционирования и безопасности и контроля за применением 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);
  - Копии Приказа о назначении администраторов безопасности и лиц их замещающих;
  - Копии Приказа о назначении лиц, допускаемых к самостоятельной работе с СКЗИ;
  - 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 Аппаратного журнала (если он ведется);
  - Скан-копии Ведомости сдачи зачетов;
  - Скан-копии Акта готовности СКЗИ к эксплуатации.

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». Исходящая информация поступает в подпроцесс «Генерация ключевой информации» или в подпроцесс «Расследование фактов нарушений условий использования СКЗИ».

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 ЗАО «Гринатом», копии находятся в ООКИ с наклеенным голографическим знаком на оборудовании.

АБ:

- 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;
- Проставляет отметки о проверке порядка использования СКЗИ в Техническом (аппаратном) журнале (в случае, если он ведется);
- 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.
- Составляет Акт готовности СКЗИ к эксплуатации (Приложение №17).

- Проводит проверку выполнения требований Регламента и делает отметки об устранении недостатков в Плане устранения недостатков.

Направляет в ОКЗ ЗАО «Гринатом» вышеуказанные документы.

Аналитик:

- Обрабатывает полученные документы от АБ.

АБ (в случае если СКЗИ получаются из банка):

- Проводит проверку порядка использования СКЗИ в соответствии с эксплуатационной и технической документацией;
- Проставляет отметки о проверке порядка использования СКЗИ в Техническом (аппаратном) журнале (в случае, если он ведется);
- Оформляет Заключение по результатам контроля безопасности АРМ с установленным СКЗИ;
- Направляет в ОКЗ ЗАО «Гринатом» вышеуказанные документы.
- 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.

3.6.11. Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»

АБ:

- Проводит расследование и составляет Заключение (Приложение № 23) по всем фактам нарушений условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации, разрабатывает и принимает меры по предотвращению возможных опасных последствий подобных нарушений;
- Направляет скан-копию Заключения в адрес ОКЗ ЗАО «Гринатом».

В случае если СКЗИ получаются из банка, разбор нарушений производится с помощью специализированного банковского ПО, в соответствии с инструкциями Банка по разбору конфликтных ситуаций. Результатом разбора нарушения является Заключение по факту нарушения условий использования СКЗИ.

АБ (в случае если СКЗИ получаются из банка):

- Проводит расследование с помощью специализированного банковского ПО в соответствии с инструкциями Банка по разбору конфликтных ситуаций и принимает меры по предотвращению возможных опасных последствий подобных нарушений;
- Подписывает Заключение по факту нарушения условий использования СКЗИ;
- Направляет скан-копию Заключения в адрес ОКЗ ЗАО «Гринатом».

3.6.12. Подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ»

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.
  Уничтожение СКЗИ производится по акту (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.
  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 ЗАО «Гринатом».
  Бумажные и прочие сгораемые материалы, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью шредеров.
  СКЗИ должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации. Если срок уничтожения эксплуатационной и технической документацией не установлен, то СКЗИ должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия).
- Делает отметки в Журнале учета (для обладателя конфиденциальной информации) об изъятии и уничтожении СКЗИ;
- Направляет в адрес ОКЗ ЗАО «Гринатом» следующие документы:

- скан-копию Решения Руководителя ООКИ о выводе СКЗИ из эксплуатации;
- скан-копию Журнала учета (для обладателя конфиденциальной информации).

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

3.6.13.Подпроцесс «Проверка выполнения требований Регламента».

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:
  - информацию из Схемы организации криптографической защиты конфиденциальной информации (перечень СКЗИ, выданных ОКЗ на предприятие);
  - информацию 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 Контрольным списком 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 – Контрольный список, Приложение №30);
- 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 №31).
Ознакомляет под расписку с Актом проверки Руководителя ООКИ;

- Подготавливает Отчет о проверке 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 – отчет о проверке, Приложение №32).
  Ознакомляет Руководителя ЗАО «Гринатом» с результатами проведения проверки.

Руководитель Органа криптографической защиты ЗАО «Гринатом»:

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

Начальник Управления информационной безопасности ЗАО «Гринатом»:

- Согласовывает Программу проверки;
- Согласовывает Акт проверки.

Руководитель ООКИ:

Составляет и направляет в адрес Начальника управления информационной безопасности ЗАО «Гринатом»:

- План реализации рекомендаций по результатам проверки лицензиата ФСБ России ЗАО «Гринатом» в ООКИ (далее – План устранения недостатков, Приложение №33);
- Один экземпляр подписанного Акта проверки.

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 №0013298 Рег.№14051Н от 16.01.2015г. На распространение шифровальных (криптографических) средств;
- Положение о системе Регламентирующих документов Госкорпорации «Росатом», утв. Приказом от 21.12.2012 № 1/1247-П;
- Отраслевые требования по информационной безопасности Госкорпорации «Росатом» безопасности №1/910-П-дсп от 23.09.2014;
- Постановление №313 от 16.04.2012 г. Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

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 ЗАО «Гринатом»;
Администратор безопасности ОКЗ ЗАО «Гринатом»;
Руководитель ЗАО «Гринатом»;
Начальник Управления информационной безопасности ЗАО «Гринатом»;
Начальник Отдела криптографической защиты ЗАО «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.	Ведомость сдачи зачетов
Приложение №21.	Заключение о возможности эксплуатации СКЗИ
Приложение №22.	Журнал выполнения регламентных работ
Приложение №23.	Заключение по факту нарушения условий использования СКЗИ
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. Контрольный список
Приложение №31. Акт проверки
Приложение №32. Отчет о проверке
Приложение №33. План устранения недостатков

От Исполнителя:

Генеральный директор

ЗАО «Гринатом»

М.Ю. Ермолаев

М.П.

Приложение №1. Матрица ответственности

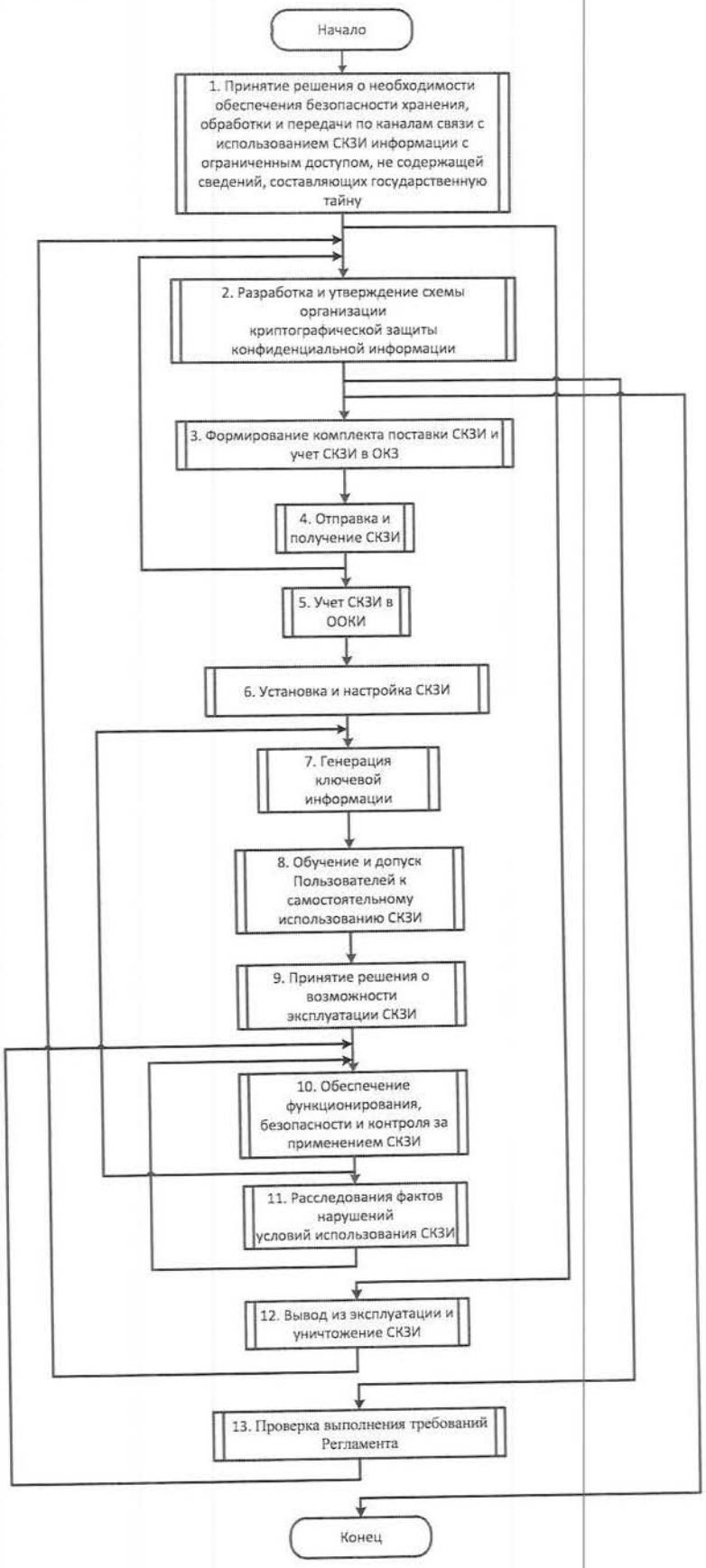
Подпроцессы в составе процесса	Участники процесса							
	Руководитель ООКИ	Аналитик ОКЗ ЗАО «Гринатом	АБ ОКЗ ЗАО «Гринатом	Начальник Управления информационной безопаснос		Руководитель Органа криптографической защиты ЗАО	Руководитель ЗАО «Гринатом	Проверяющий
Подпроцесс «Принятие решения о необходимости 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.			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.	О					
Подпроцесс «Вывод из эксплуатации и уничтожения СКЗИ»	Утв.	Инф.	О					
Подпроцесс «Проверка выполнения требований Регламента»	О		Инф.	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

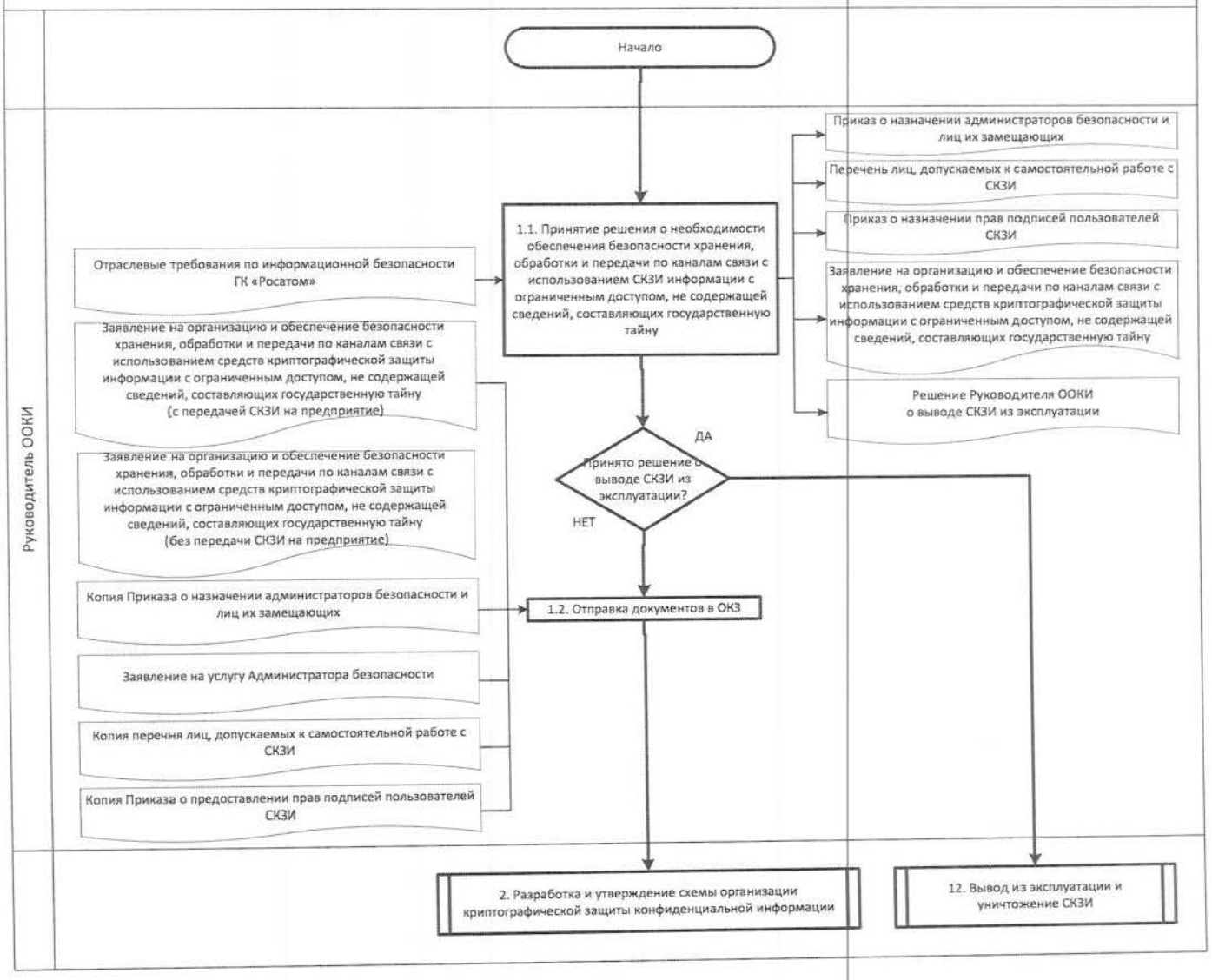
И	Интегратор	Интегрирует результаты подпроцесса/процедуры и отвечает за организацию подпроцесса/процедуры, включая взаимодействие участников	Структурное подразделение Корпорации/Дивизиона/ Организации
К	Контролер	Осуществляет контроль выполнения и достижения результатов подпроцесса/процедуры	Структурное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

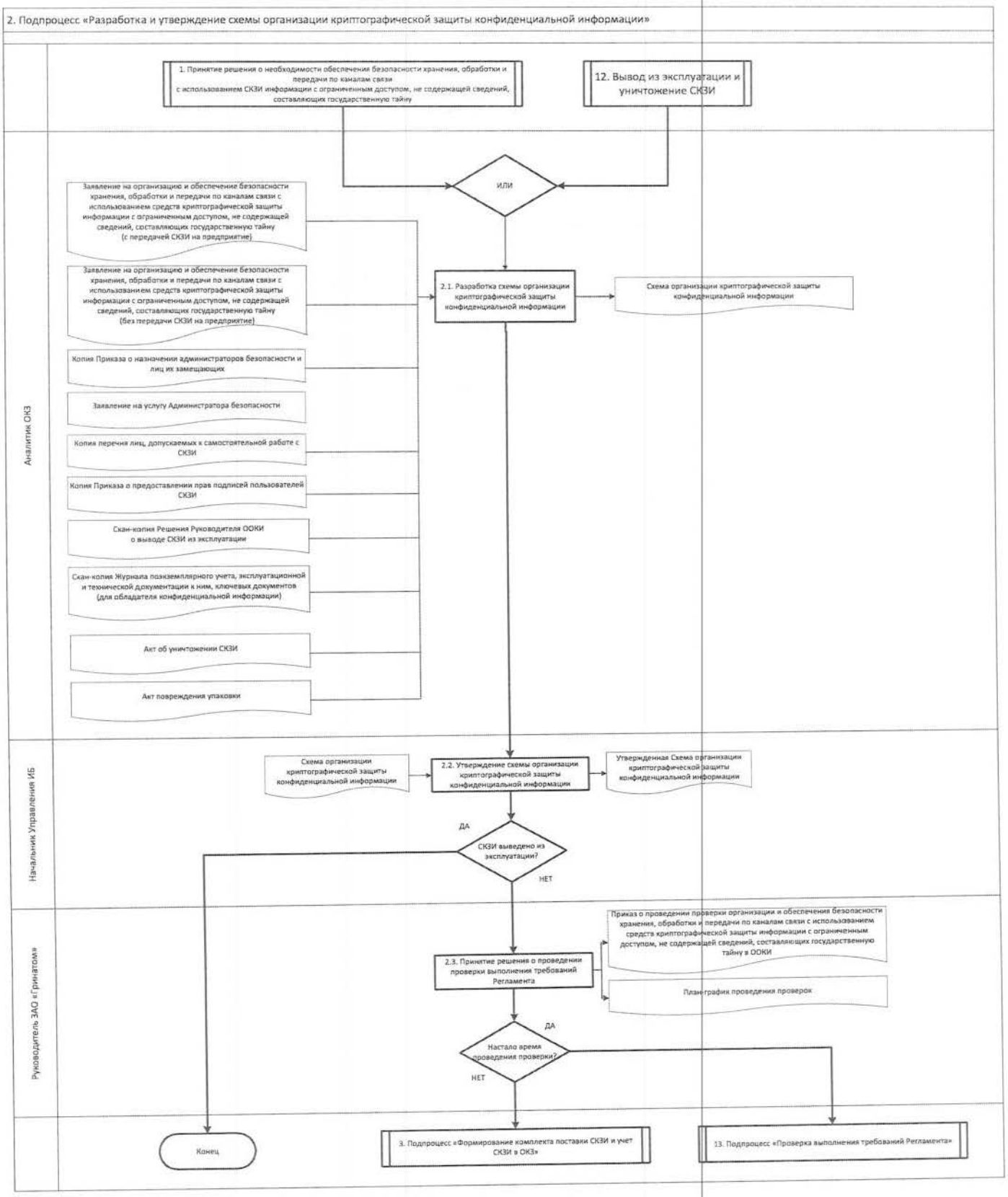
Приложение №2. Схема процесса

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»

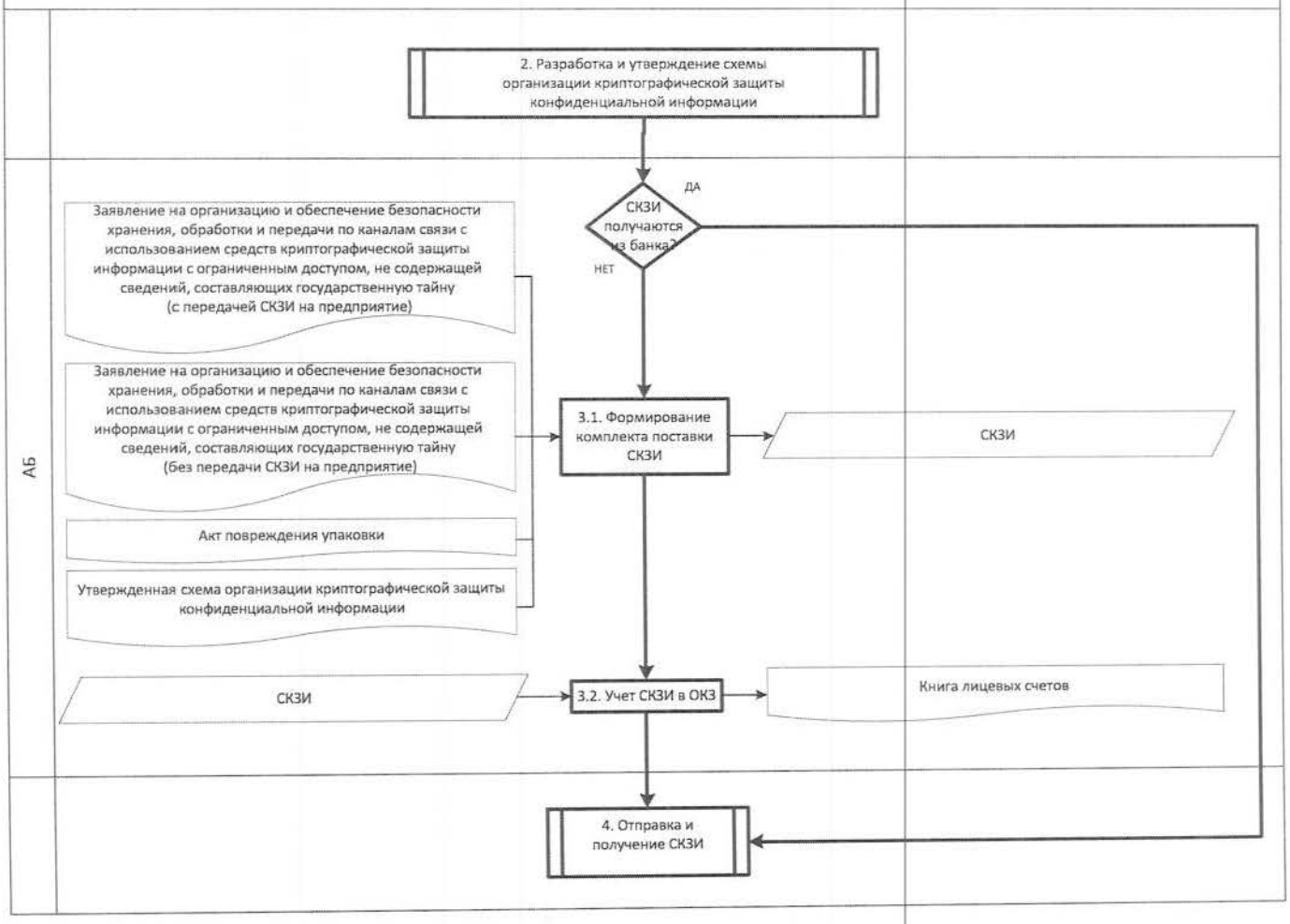


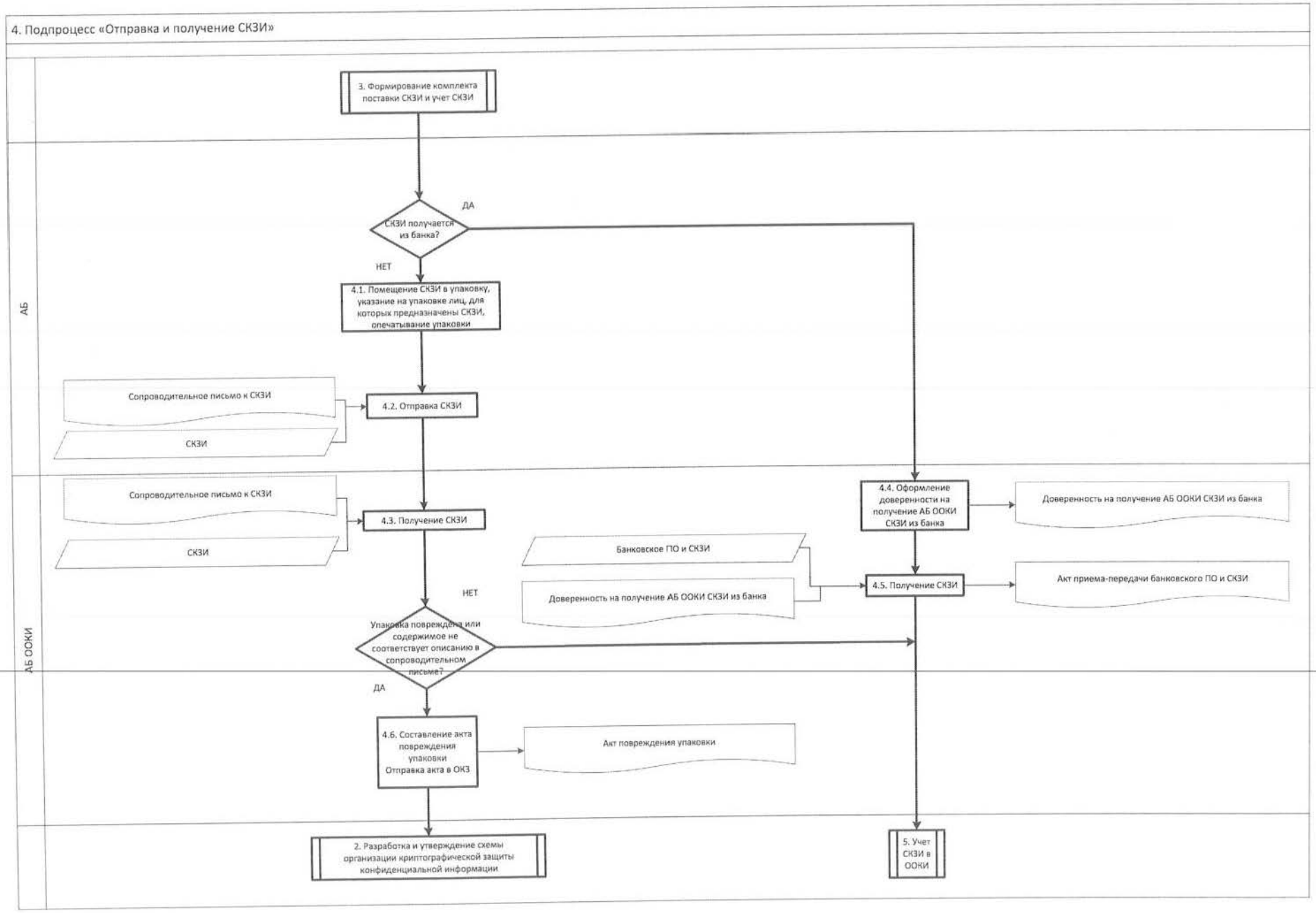
1. Подпроцесс «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»



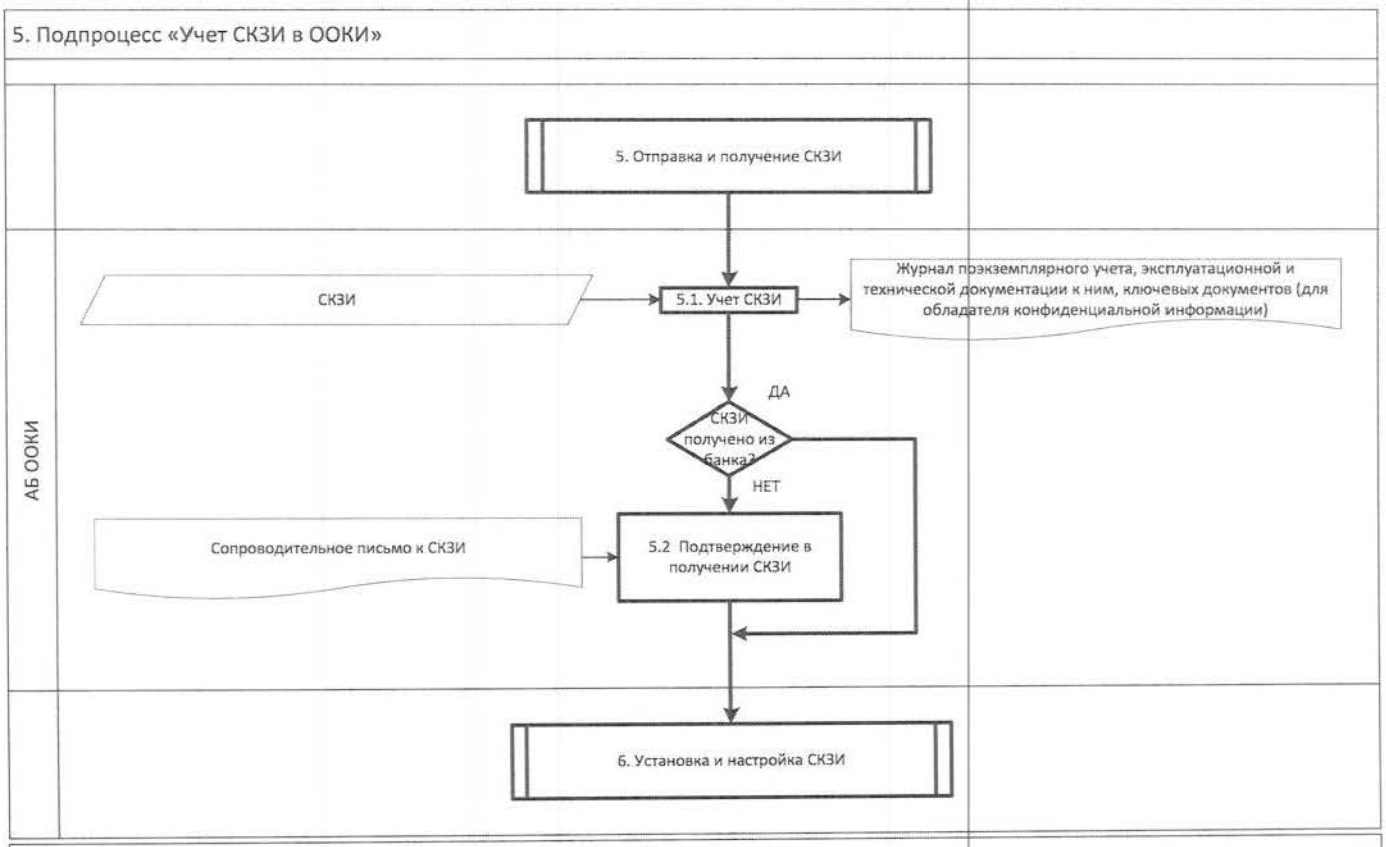

2. Подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации»
Аналитик ОКЗ
Начальник Управления ИБ
Руководитель ЗАО «Гринатом»
1. Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну
12. Вывод из эксплуатации и уничтожение СКЗИ
ИЛИ
Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (с передачей СКЗИ на предприятие)
Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (без передачи СКЗИ на предприятие)
Копия Приказа о назначении администраторов безопасности и лиц их замещающих
Заявление на услугу Администратора безопасности
Копия перечня лиц, допускаемых к самостоятельной работе с СКЗИ
Копия Приказа о предоставлении прав подписей пользователей СКЗИ
Скан-копия Решения Руководителя ООКИ о выводе СКЗИ из эксплуатации
Скан-копия Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Акт об уничтожении СКЗИ
Акт повреждения упаковки
2.1. Разработка схемы организации криптографической защиты конфиденциальной информации
Схема организации криптографической защиты конфиденциальной информации
Схема организации криптографической защиты конфиденциальной информации
2.2. Утверждение схемы организации криптографической защиты конфиденциальной информации
Утвержденная Схема организации криптографической защиты конфиденциальной информации
ДА
СКЗИ выведено из эксплуатации?
НЕТ
2.3. Принятие решения о проведении проверки выполнения требований Регламента
Приказ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ
План-график проведения проверок
ДА
Настало время проведения проверки?
НЕТ
Конец
3. Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ в ОКЗ»
13. Подпроцесс «Проверка выполнения требований Регламента»

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

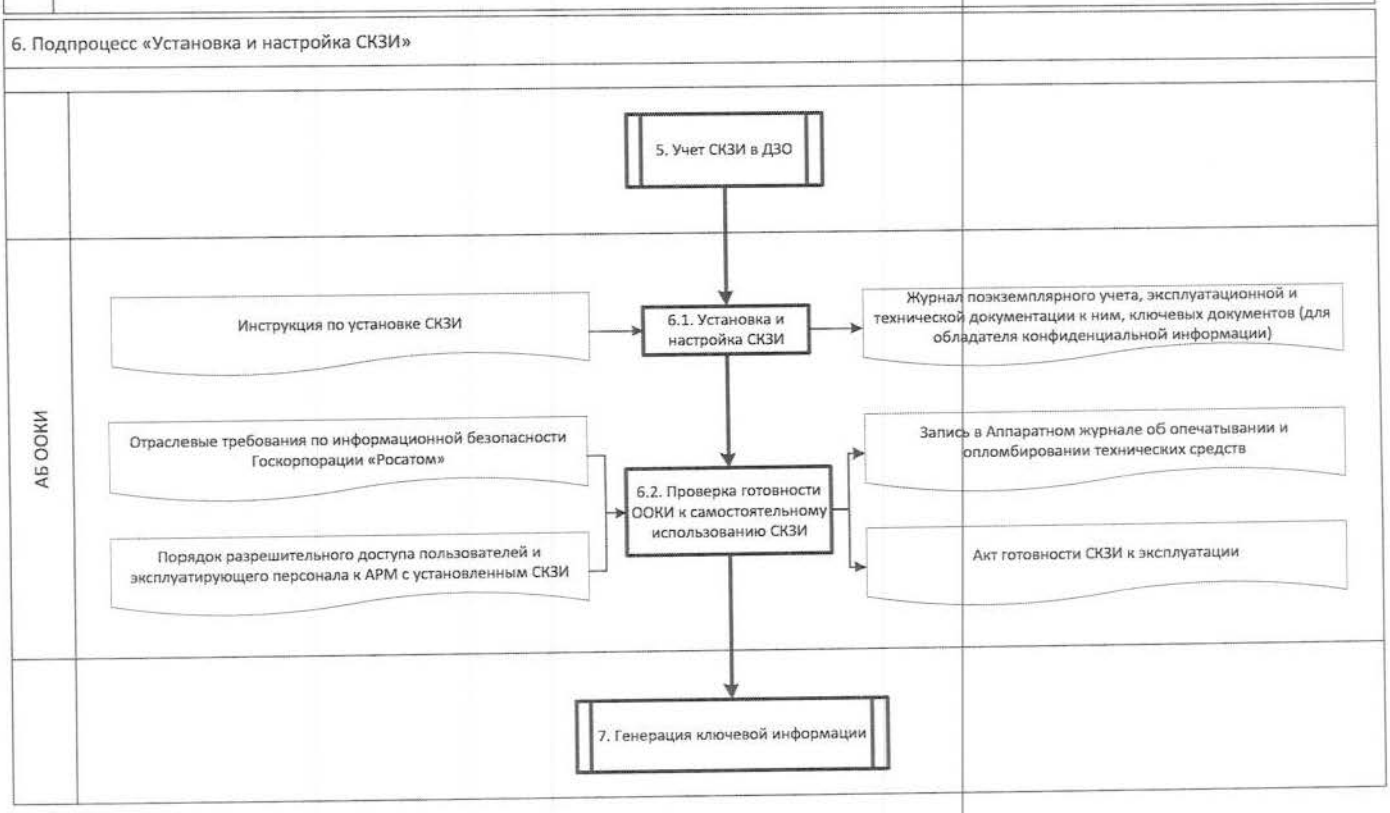



4. Подпроцесс «Отправка и получение СКЗИ»
АБ
АБ ООКИ
3. Формирование комплекта поставки СКЗИ и учет СКЗИ
СКЗИ получается из банка?
ДА
НЕТ
4.1. Помещение СКЗИ в упаковку, указание на упаковке лиц, для которых предназначены СКЗИ, опечатывание упаковки
Сопроводительное письмо к СКЗИ
СКЗИ
4.2. Отправка СКЗИ
Сопроводительное письмо к СКЗИ
СКЗИ
4.3. Получение СКЗИ
4.4. Оформление доверенности на получение АБ ООКИ СКЗИ из банка
Доверенность на получение АБ ООКИ СКЗИ из банка
Банковское ПО и СКЗИ
Доверенность на получение АБ ООКИ СКЗИ из банка
4.5. Получение СКЗИ
Акт приема-передачи банковского ПО и СКЗИ
НЕТ
Упаковка повреждена или содержимое не соответствует описанию в сопроводительном письме?
ДА
4.6. Составление акта повреждения упаковки Отправка акта в ОКЗ
Акт повреждения упаковки
2. Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации
5. Учет СКЗИ в ООКИ

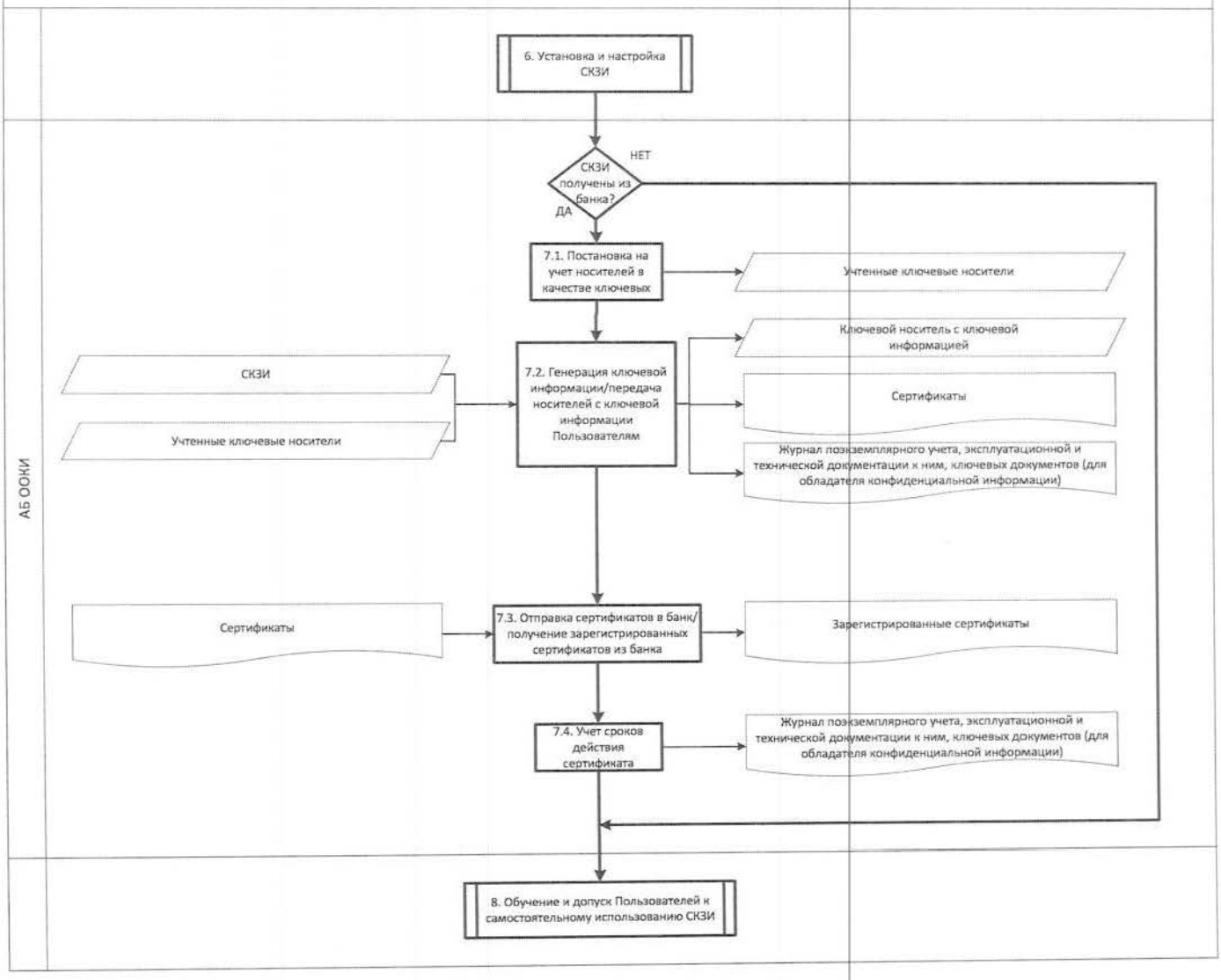
5. Подпроцесс «Учет СКЗИ в ООКИ»



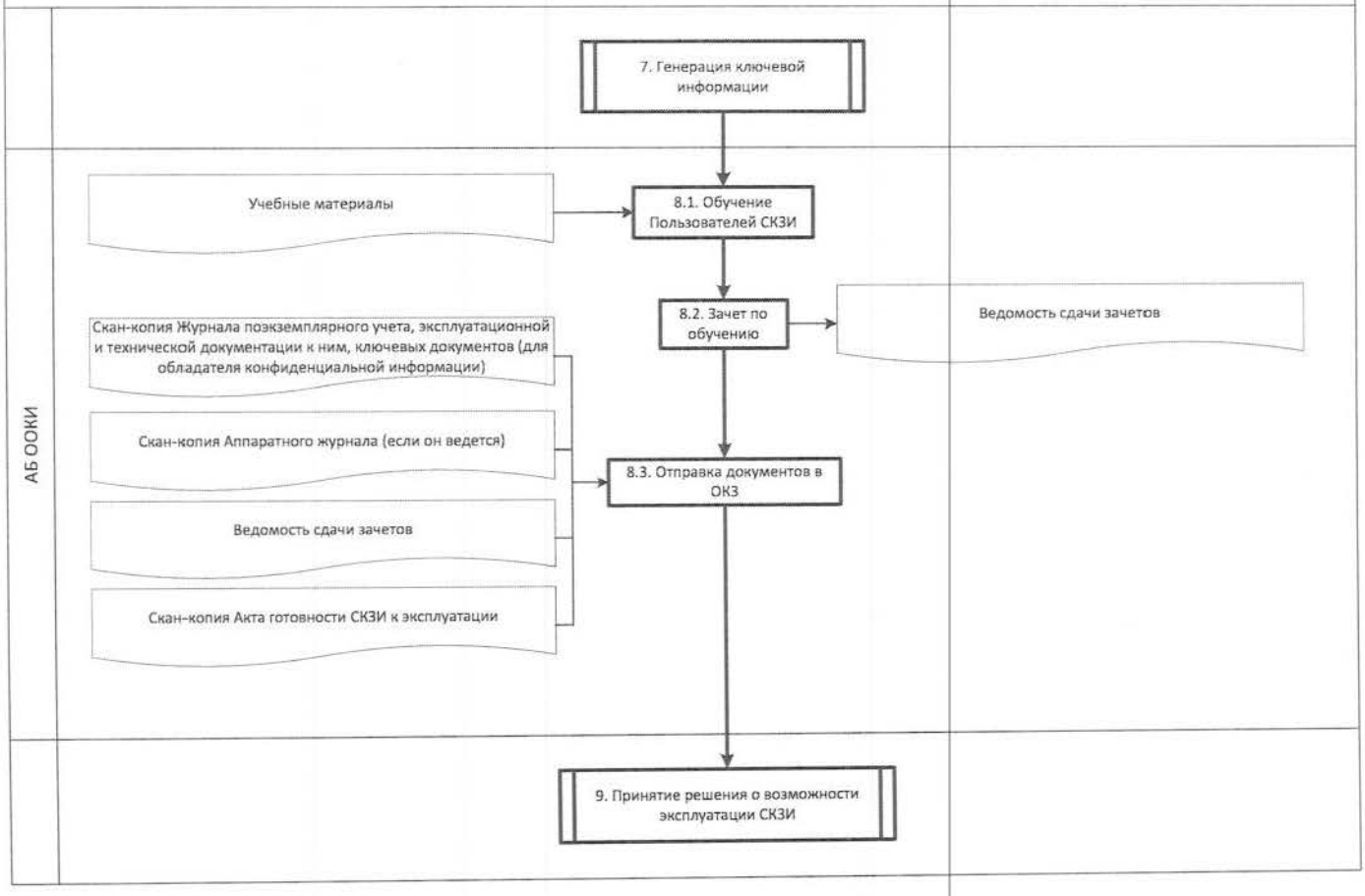
6. Подпроцесс «Установка и настройка СКЗИ»

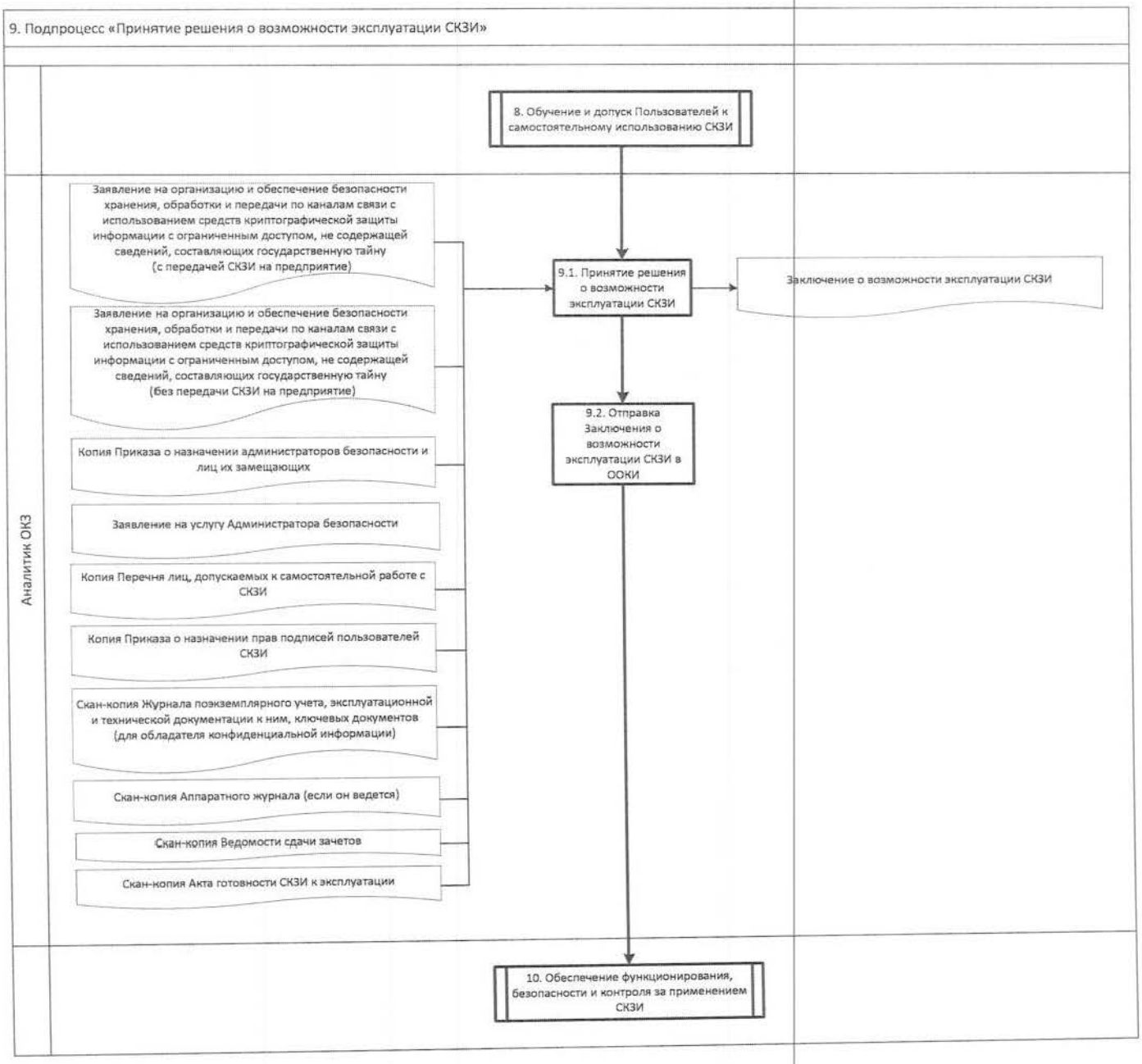


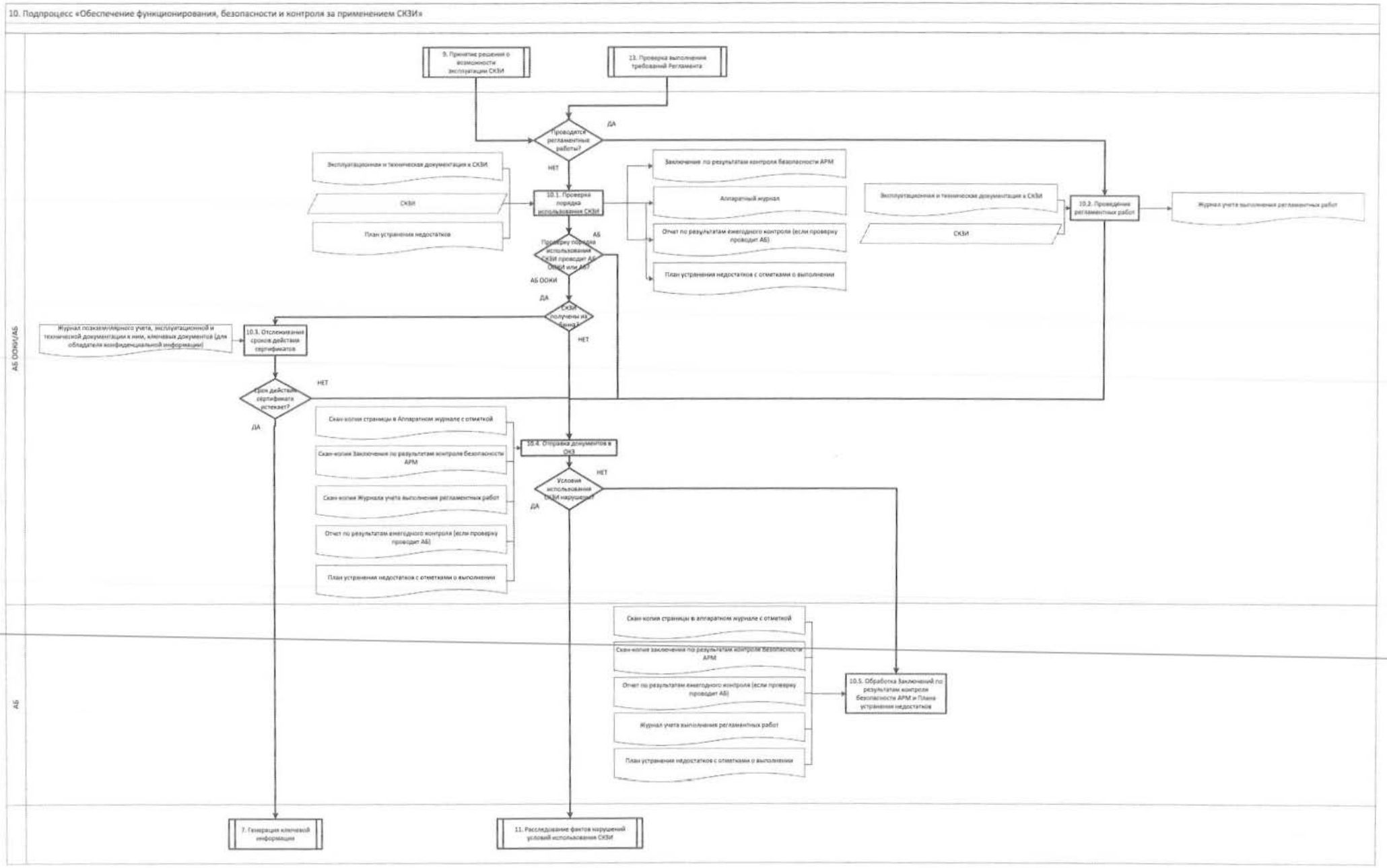
7. Подпроцесс «Генерация ключевой информации»



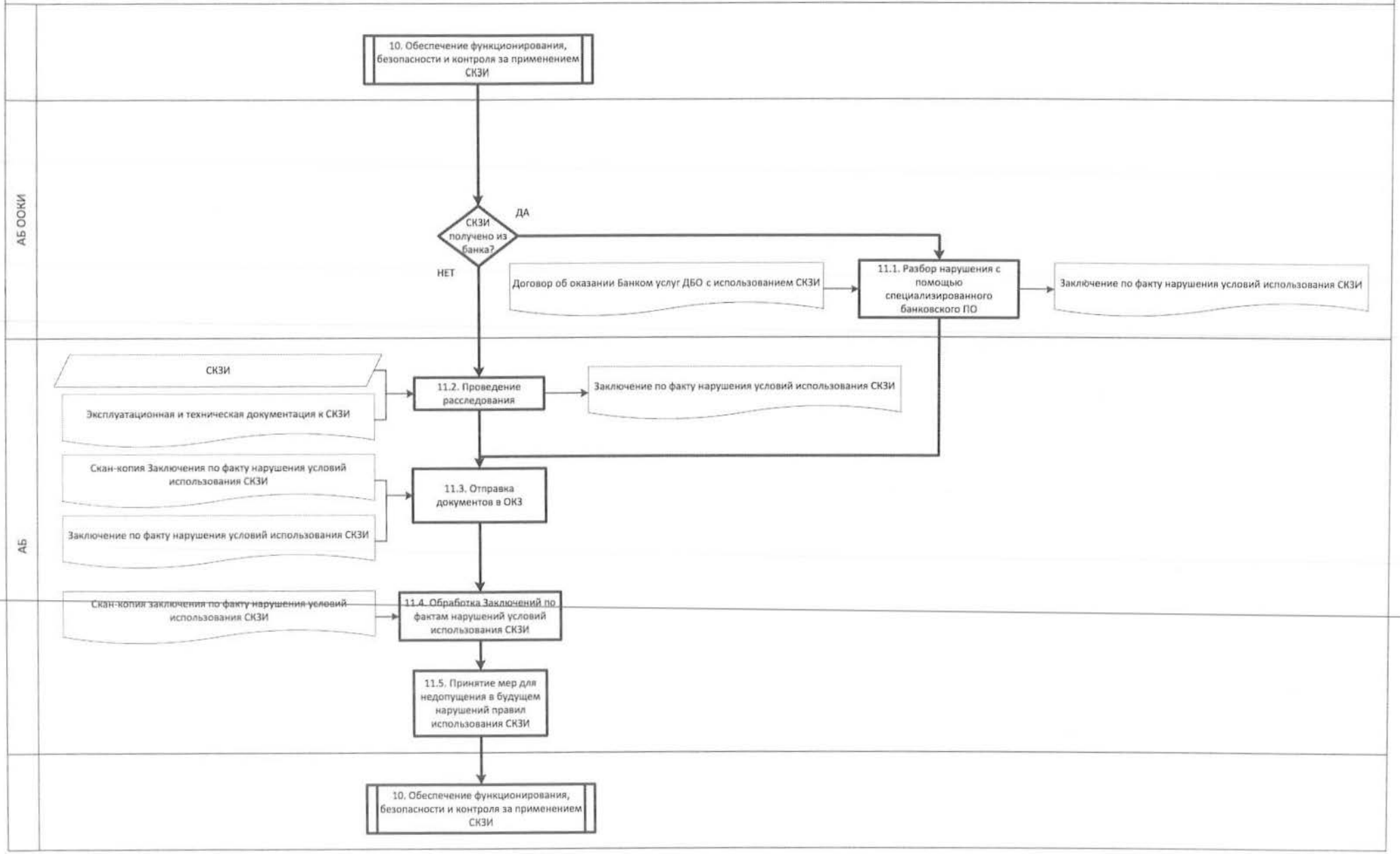
8. Подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ»

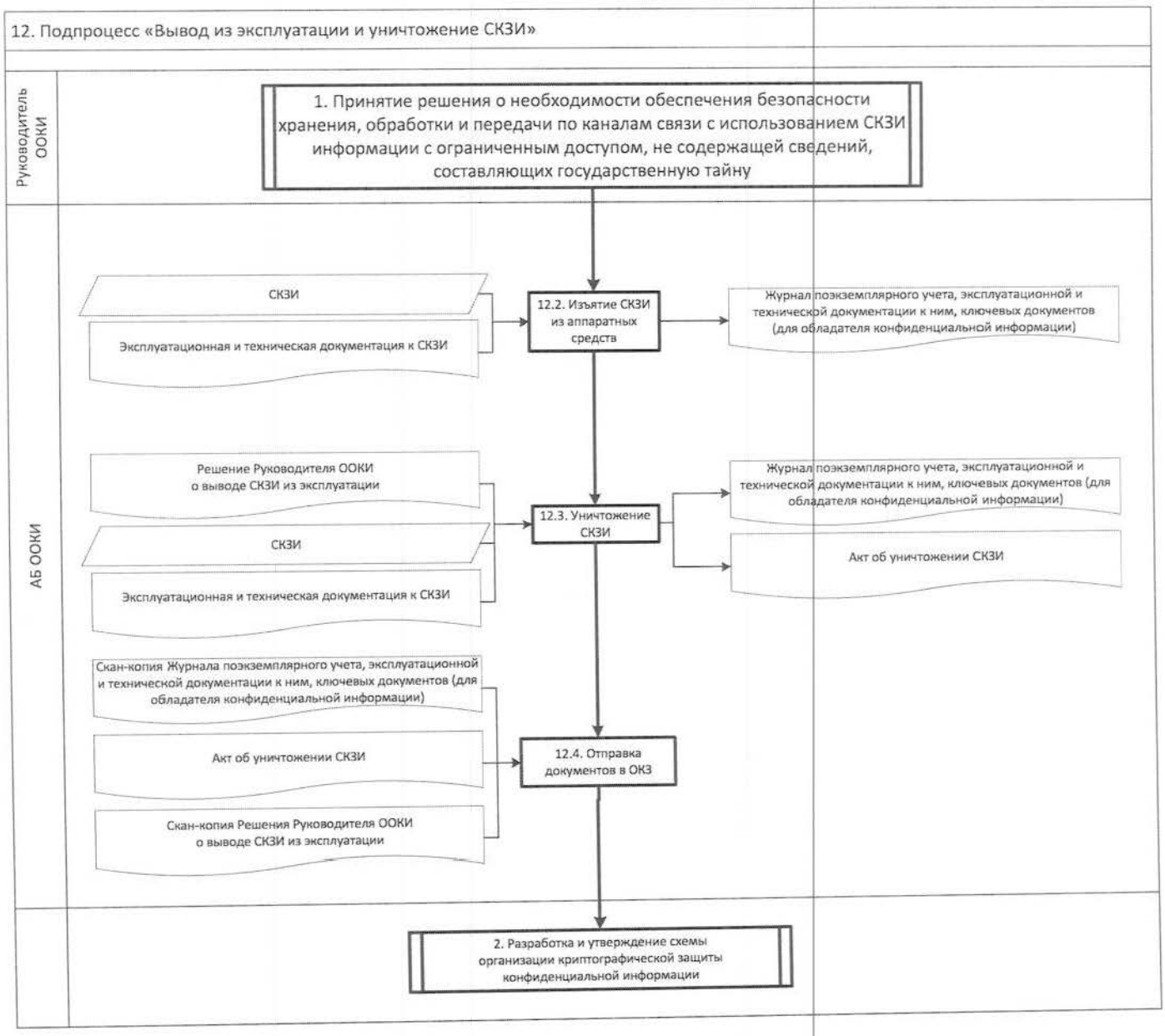



9. Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»
Аналитик ОКЗ
8. Обучение и допуск Пользователей к самостоятельному использованию СКЗИ
Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты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

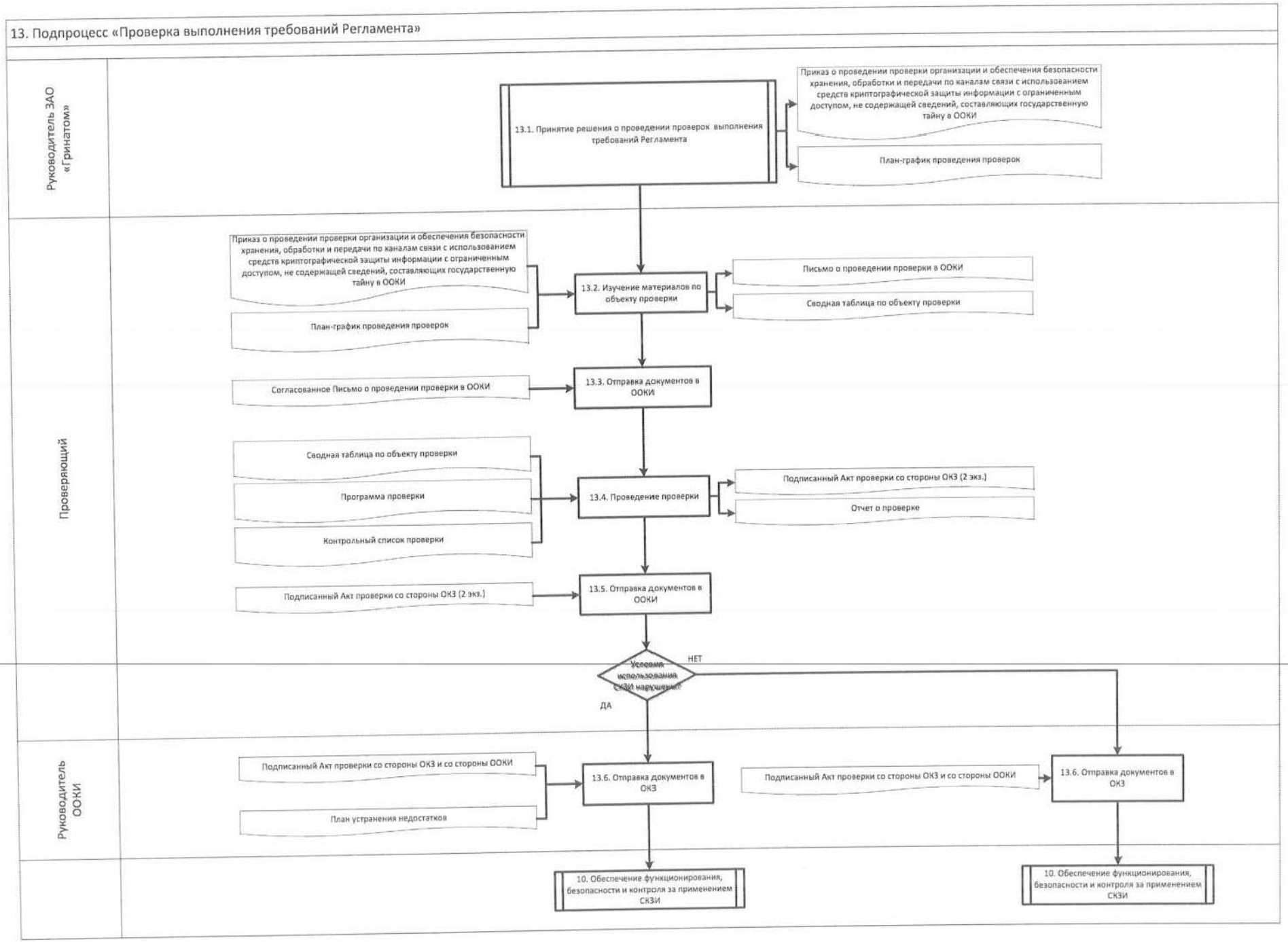

10. Подпроцесс «Обеспечение функционирования, безопасности и контроля за применением СКЗИ»
АБ ООКИ/АБ
АБ
9. Принятие решения о возможности эксплуатации СКЗИ
13. Проверка выполнения требований Регламента
Проводятся регламентные работы?
ДА
НЕТ
Эксплуатационная и техническая документация к СКЗИ
СКЗИ
План устранения недостатков
10.1. Проверка порядка использования СКЗИ
Заключение по результатам контроля безопасности АРМ
Аппаратный журнал
Отчет по результатам ежегодного контроля (если проверку проводит АБ)
План устранения недостатков с отметками о выполнении
Эксплуатационная и техническая документация к СКЗИ
СКЗИ
10.2. Проведение регламентных работ
Журнал учета выполнения регламентных работ
Проверку порядка использования СКЗИ проводит АБ ООКИ или АБ?
АБ
АБ ООКИ
ДА
СКЗИ получены из фонда?
НЕТ
Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
10.3. Отслеживание сроков действия сертификатов
Срок действия сертификата истекает?
НЕТ
ДА
Скан-копия страницы в Аппаратном журнале с отметкой
Скан-копия Заключения по результатам контроля безопасности АРМ
Скан-копия Журнала учета выполнения регламентных работ
Отчет по результатам ежегодного контроля (если проверку проводит АБ)
План устранения недостатков с отметками о выполнении
10.4. Отправка документов в ОКЗ
Условия использования СКЗИ нарушены?
НЕТ
ДА
Скан-копия страницы в аппаратном журнале с отметкой
Скан-копия заключения по результатам контроля безопасности АРМ
Отчет по результатам ежегодного контроля (если проверку проводит АБ)
Журнал учета выполнения регламентных работ
План устранения недостатков с отметками о выполнении
10.5. Обработка Заключений по результатам контроля безопасности АРМ и Плана устранения недостатков
7. Генерация ключевой информации
11. Расследование фактов нарушений условий использования СКЗИ

11. Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»




12. Подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ»
Руководитель ООКИ
АБ ООКИ
1. 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
СКЗИ
Эксплуатационная и техническая документация к СКЗИ
12.2. Изъятие СКЗИ из аппаратных средств
Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Решение Руководителя ООКИ о выводе СКЗИ из эксплуатации
СКЗИ
Эксплуатационная и техническая документация к СКЗИ
12.3. Уничтожение СКЗИ
Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Акт об уничтожении СКЗИ
Скан-копия Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Акт об уничтожении СКЗИ
Скан-копия Решения Руководителя ООКИ о выводе СКЗИ из эксплуатации
12.4. Отправка документов в ОКЗ
2. Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации

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)
1	Протокол принятия решения о необходимости обеспечения безопасности конфиденциальной информации	Предприятие
2	Технический (аппаратный) журнал	ЗАО «Гринатом»
3	Лицевой счет	ЗАО «Гринатом»

№ 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

ПРИКАЗ

_____ № ___

(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 контролю за соблюдением требований по безопасности на следующего(-их) сотрудника(-ов):

_____

(Ф.И.О., должность, подразделение, e-mail, телефон)

_____

(Ф.И.О., должность, подразделение, e-mail, телефон)

2. Администратору(-ам) безопасности провести инструктаж и обучение Пользователя(-ей) 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)

М.П.

Приложение №5. Форма Заявления на услугу Администратора безопасности

Заявление
на услугу Администратора безопасности

«_____» _____ 201__ 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

Уполномоченное должностное лицо

_____ _____ / _____ /

(Должность) (подпись) (ФИО)

М.П.

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

ПРИКАЗ

_____ № ___

(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)

М.П.

Приложение №7. Форма Приказа о предоставлении прав подписей

ПРИКАЗ

_____ № ____

(дата)

О предоставлении прав подписей в системе(ах)

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

ПРИКАЗЫВАЮ:

1. Предоставить право первой подписи в системе :

_____
(Ф.И.О., должность)

_____
(Ф.И.О., должность)

2. Предоставить право второй подписи в системе :

_____
(Ф.И.О., должность)

_____
(Ф.И.О., должность)

3. Предоставить право запроса выписки в системе :

_____
(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)

«___» _____ 201__ г.

_____

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____,

должность

_____,

фамилия, имя, отчество

действующего на основании _____

просит ОКЗ ЗАО «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)

Уполномоченное должностное лицо
_____ _____/_____/
(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)

«___» _____ 201__ г.

_____

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____,

должность

_____,

фамилия, имя, отчество

действующего на основании _____

просит ОКЗ ЗАО «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)

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

м.п.

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

Схема криптографической защиты информации <Наименование организации>																			
№ п/п	Наименование предприятия	Учетный номер "Заявления..." о присоединении	Учетный номер "Заявления..." на обеспечение СКЗИ	Ф.И.О., рабочий телефон и e-mail администратора безопасности ОКЗ, № и дата приказа о назначении	Пользователь СКЗИ (должность, Ф.И.О.)	Тип используемого СКЗИ	Лицензия №/Ключевые документы (№ сертификата ключа проверки электронной подписи)	Автоматизированная/информационная система	Учетный номер АРМ/серийный номер, на котором установлено СКЗИ	Адрес месторасположения ПЭВМ	Программное обеспечение, установленное на ПЭВМ	Вид защищаемой информации	Ведомость сдачи зачетов	Акт готовности СКЗИ к эксплуатации	Лицевой счет/Журнал поэкземплярного учета	Приказ о назначении лиц, допускаемых к самостоятельной работе с СКЗИ	Приказ о предоставлении прав подписей в платежных системах	Заключение о возможности эксплуатации СКЗИ	Отметки об уничтожении	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

ЗАО «Гринатом»

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 картотеке	Расписка лица оформившего л/с	Отметки о местонахождении

Лицевой счет _____ тел. _____

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

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

ДОВЕРЕННОСТЬ
доверенного лица, наделенного правом получения средств криптографической защиты информации

г. _____ «____» _____20__г.

_____
_____
_____
наименование организации, включая организационно-правовую форму

в лице_____,
(должность)

действующего на основании_____
уполномачивает_____
(фамилия, имя, отчество)

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

зарегистрированного по адресу: _____,

получать в Органе криптографической защиты ЗАО «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.

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

М.П.

Приложение №12. Сопроводительное письмо к СКЗИ

Общий центр обслуживания Госкорпорации «Росатом»

ГРИНАТОМ

ЗАО «Гринатом»
115114, Москва
Павелецкая наб., дом 8, стр. 1
+7 499 949 4919
info@greenatom.ru
www.greenatom.ru

___(должность сотрудника)___
___(наименование организации)___

ФИО сотрудника

_____ № _____
На № _____/_____ от _____г.
О предоставлении СКЗИ и документации

Уважаемый __(ИО)__!

Направляем Вам СКЗИ в соответствии с Договором № _____ от _____ с ЗАО «Гринатом».

Описание:
1.

___(должность сотрудника)___ ФИО

Приложение №13. Акт повреждения упаковки

АКТ №_____

г. Москва «___» _____ 201__ г.

Администратор безопасности ФИО _____ составил настоящий акт в том, что полученная упаковка повреждена (указать степень повреждения).

Вывод:

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

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

_____/_____
(подпись) (Ф.И.О)

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

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

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

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

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

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

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

Москва
2015 г.

Оглавление

1. Общие положения

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

2. Требования к размещению технических средств установленными СКЗИ

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

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленными СКЗИ, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования к программному и аппаратному обеспечению

Технические средства с установленными СКЗИ должны отвечать следующим требованиям:

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

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

4. Защита информации от НСД

При использовании СКЗИ необходимо принять следующие организационные меры:

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

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

условиях возможно полное удаление ресурса или его неиспользуемой части):

- Системный реестр;
- Файлы и каталоги;
- Временные файлы;
- Журналы системы;
- Файлы подкачки;
- Кэшируемая информация (пароли и т.п.);
- Отладочная информация.

Кроме того, необходимо организовать затирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

- Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;
- Необходимо регулярно устанавливать пакеты обновления безопасности ОС, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
- В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети;
- При использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых ОС, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты;
- Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита;
- Организовать и использовать комплекс антивирусной защиты;
- Исключить одновременную работу в ОС с работающим СКЗИ и загружаемой ключевой информацией нескольких пользователей.

Приложение №16. Технический (аппаратный) журнал

Технический (аппаратный) журнал

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

Приложение №17. Акт готовности СКЗИ к эксплуатации

Акт № _____

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

г. _____ «___» _____ 20___ г.

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

в соответствии с заявкой на установку СКЗИ «_____» версии
(наименование СКЗИ)

от «_____»_____ 20____ г. ,

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	
Установлено сертифицированное СЗИ от НСД Secret Net версии 6.5 и выше. ОС настроена в соответствии с отраслевыми требованиями по информационной безопасности №1/910-П-дсп от 23.09.2014	

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»	

СКЗИ « » версии установлено:

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

Вывод:

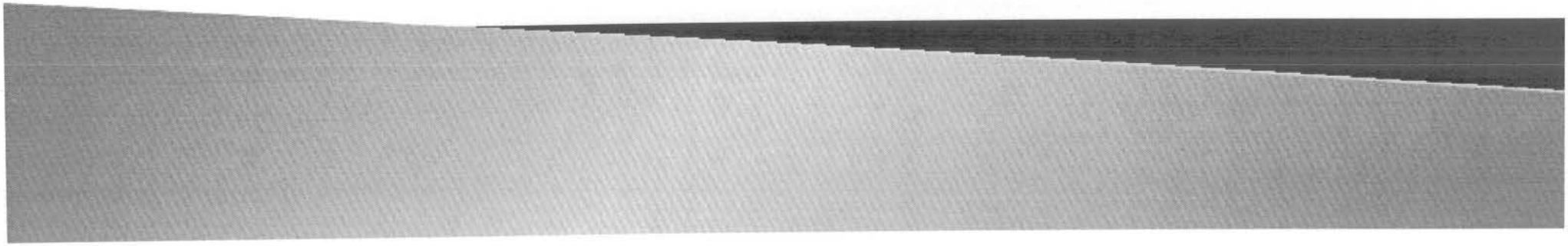
Оборудование АРМ соответствует Отраслевым требованиям по информационной безопасности №1/910-П-дсп от 23.09.2014 и требованиям «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным 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 « _____ »
(Наименование СКЗИ)
версии _____ .

_____ / _____
(подпись) (Ф.И.О.)

Управление информационной безопасности

Обучение пользователей правилам работы со средствами криптографической защиты информации

ГРИНАТОМ



Программа обучения пользователей правилами работы с СКЗИ

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

Корпоративные ценности ЗАО «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.

БЕЗОПАСНОСТЬ

это защищенность от возможного нанесения ущерба при возникновении различных возможных угроз

Ущерб может быть прямым и косвенным:

- ✓ материальный
- ✓ моральный
- ✓ физический

Субъектами нанесения ущерба, в конечном счете, всегда являются люди

Влияние осведомленности пользователей на уровень информационной безопасности

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

Типичные причины нарушений пользователей

- Использование ресурсов не по назначению

Действие:

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

Последствия:

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

Контрмеры:

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

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

Типичные причины нарушений пользователей

- Непринятие мер по предотвращению порчи или утраты оборудования

Действие:

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

Последствия:

прямой материальный ущерб. Частичный или полный отказ системы - потери из-за простоев и затраты на восстановление ресурсов и работоспособности (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, инсталляция сторонних программ, внесение изменений в настройки аппаратной части ЭВМ, программных продуктов, установленных на ЭВМ.

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)

Типичные причины нарушений пользователей

- Отключение или создание помех для работы штатных антивирусных программ

Действие:

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

Последствия:

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

Контрмеры:

повышение ответственности пользователей, внедрение более совершенных антивирусных средств

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

Типичные причины нарушений пользователей

- Использование нелицензионного программного обеспечения

Действие:

использование нелицензионного 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

- Нарушение установленного порядка обращения с конфиденциальной информацией

Типичные причины нарушений пользователей

- Самовольное создание и использование разделяемых сетевых ресурсов

Действие:

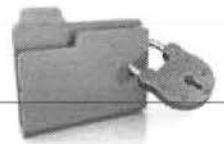
самовольное создание совместно используемых сетевых ресурсов (папок общего пользования) на своих компьютерах, несанкционированное удаление или изменение прав доступа к ним

Последствия:

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

Контрмеры:

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



ГРИНАТОМ

Типичные причины нарушений пользователей

- Личная (непроизводственная) переписка по электронной почте

Действие:

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

Последствия:

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

Контрмеры:

повышение ответственности сотрудников, подписание соглашений о контроле за перепиской

Типичные причины нарушений пользователей

- Пересылка конфиденциальных сведений ГК «Росатом» в открытом виде

Действие:

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

Последствия:

утечка конфиденциальной информации (в том числе коммерческих секретов)

Контрмеры:

повышение ответственности, применение Защищенной корпоративной почтовой системы

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

Типичные причины нарушений пользователей

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

Действие:

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

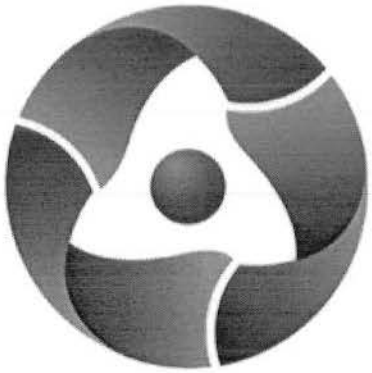
Последствия:

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

Приказ от 16.04.2014 №I/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.

ГРИНАТОМ

Типичные причины нарушений пользователей

- Нарушение правил использования средств криптографической защиты информации

Действие:

нарушение правил применения средств криптографической защиты информации

Последствия:

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

Контрмеры:

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

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

ГРИНАТОМ

Требования к эксплуатации СКЗИ

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

Требование к размещению технических средств с установленными СКЗИ

- Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленными СКЗИ, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию
- Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

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

Требования к программному и аппаратному обеспечению

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

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 ключей

Компрометация – любая возможность (или совершившийся факт) попадание ключей посторонним (не допущенным) лицам

- утрата ключевого носителя с последующим обнаружением
- увольнение сотрудников, имевших доступ к ключевой информации
- временное оставление ключевого носителя без присмотра
- нарушение печатей на сейфе с ключевыми носителями
- нарушение печатей пеналов, в которых хранятся ключевые носители
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями

В случае утери действующего ключевого носителя с ЭП, а также обнаружения после потери – немедленно направить администратору безопасности сообщение о компрометации ключей ЭП

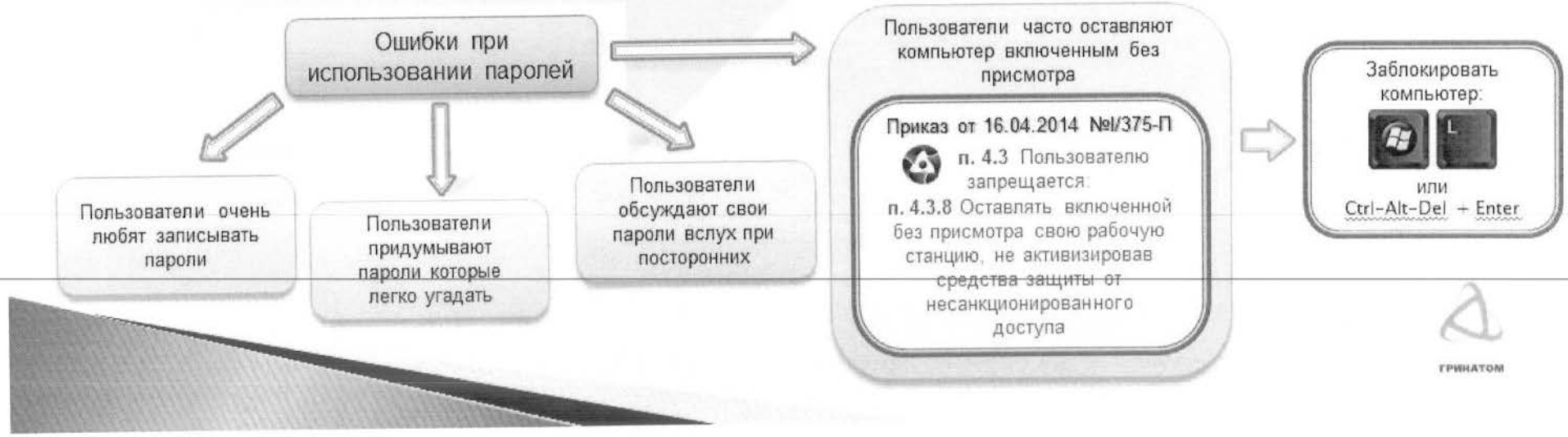
Типичные причины нарушений пользователей

- 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



Меры предосторожности при работе с паролями

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

Правила придумывания стойких и запоминающихся паролей

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

Приказ от 16.04.2014 №I/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.

ГРИМАТОМ

Ответственность

для лиц, допустивших нарушения требований по защите конфиденциальной информации

Трудовой кодекс РФ

ст. 81 Расторжение трудового договора по инициативе работодателя

Трудовой договор может быть расторгнут работодателем в случаях:

...

б) однократного грубого нарушения работником трудовых обязанностей;

...

в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника

Уголовный кодекс РФ

ст. 137 Нарушение неприкосновенности частной жизни;
ст. 138 Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений;
ст. 183 Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну;
ст. 272 Неправомерный доступ к компьютерной информации;
ст. 273 Создание, использование и распространение вредоносных программ для ЭВМ;
ст. 274 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети;
ст. 293 Халатность;
ст. 171 Незаконное предпринимательство;

Наказание до 7 лет лишения свободы
штраф до 300 000 руб.

Кодекс РФ об административных правонарушениях

ст. 13.11 Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);

ст. 13.12 Нарушение правил защиты информации;

ст. 13.14 Разглашение информации с ограниченным доступом;

Штраф до 30 000 руб. с конфискацией, приостановление деятельности на срок до 90 суток

Приложение №19. Анкета для опроса пользователей

Анкета для опроса пользователей СКЗИ

Заполняется персонально пользователем СКЗИ

ФИО _____

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 или Win + L;
   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 120 000 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 службы технической поддержки для генерации новых ключей ЭП;
    b) направить администратору безопасности сообщение о компрометации ключей ЭП.

17. В случае обнаружения после потери своего ключевого носителя, содержащего действующие ключи ЭП:
    a) сообщить сотрудникам службы технической поддержки для генерации новых ключей ЭП;
    b) продолжить использование данного ключевого носителя без генерации новых ключей ЭП;
    c) 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 службы технической поддержки;
    b) администратору безопасности;
    c) только своему коллеге по подразделению;
    d) 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 300 000 руб;
    d) уголовная: штраф 500 000 руб;
    e) административная: штраф 30 000 руб, приостановление деятельности организации на срок до 90 суток.

Подпись _____

Дата _____

Результаты проверки

Всего ответов _____(кол-во)

Правильных ответов _____(кол-во)

Зачтено/не зачтено

Проверил

ФИО, подпись_____

Приложение №20. Ведомость сдачи зачетов

Ведомость сдачи зачетов

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

Состав проверяющей комиссии:

ФИО Администратора безопасности, должность, отдел, управление	Подпись, дата

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__ №__ 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 при Президенте РФ 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.

Таблица 2

№ п.п.	ФИО Пользователя	

Эксплуатацию СКЗИ Наименование СКЗИ разрешаю до «___» _____ 20__ г[1]

Начальник отдела
криптографической защиты
ЗАО «Гринатом» _____/Н. И. Беленький

М.П.

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

ЖУРНАЛ
учета выполнения регламентных работ

(наименование организации)

Начат: «___» _____ 20__ г.

Окончен: «___» _____ 20__ г.

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

Приложение №23. Заключение по факту нарушения условий использования СКЗИ

ЗАКЛЮЧЕНИЕ
по факту нарушения условий использования СКЗИ

Специалистами ОКЗ ЗАО «Гринатом» в период с _____ по _____ было проведено расследование по факту нарушения условий использования СКЗИ. По результатам расследования было установлено _____.

Место проведения расследования: _____
Состав специалистов ОКЗ ЗАО «Гринатом»:

1. Должность, отдел, управление где работает сотрудник, организация, ФИО.
2. Должность, отдел, управление где работает сотрудник, организация, ФИО.

Состав оборудования :

- АРМ s/n _____
- ОС windows _____
- Система контроля защищенности и соответствия стандартам _____

Установленные нарушения

Нарушения	Ссылка на требования	Ответственный

ВЫВОДЫ:
(Предложения по устранению и дальнейшему предотвращению нарушений условий использования СКЗИ)

_____/_____
(подпись) (Ф.И.О)

Приложение №24. Акт уничтожения СКЗИ

АКТ № ____
уничтожения СКЗИ

г. (город) "___" _____ 20__г

Администратор безопасности _____, назначенный приказом от _____ г. № _____ в (Наименование организации) в соответствии с (наименование, реквизиты документа) уничтожил СКЗИ, указанные в табл. путем (способ уничтожения).

Наименование СКЗИ	**АРМ, уч. №**	**Серийный номер сертификата ключевой информации / номер лицензии**	**ФИО Пользователя СКЗИ**

Уничтожено СКЗИ (наименование СКЗИ) в количестве ____ (количество прописью) экземпляров.

_____/_____
(подпись) (Ф.И.О)

Приложение №25. Приказ о проведении проверки

ГРИНАТОМ

ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ГРИНАТОМ»

П Р И К А З

« » _____ 20__ г. Москва №_____

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 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. Управлению IT-активов обеспечить специалистов техническими средствами.
3. Контроль выполнения требований по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну возложить на отдел криптографической защиты управления информационной безопасности ЗАО «Гринатом».
4. Контроль исполнения настоящего приказа возложить на заместителя директора по информационным технологиям «И.О. Фамилия».

Генеральный директор И.О. Фамилия

Приложение №26. План-график проведения проверок

Приложение №1. План-график проведения проверок
к Приказу 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	Ответственное лицо от предприятия	Кол-во СКЗИ (на момент составления приказа)

Приложение №27. Информационное письмо о проведении проверки

Общий центр обслуживания Госкорпорации «Росатом»

ГРИНАТОМ

ЗАО «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. в «Наименование организации», 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 квалифицированного сертификата ключа проверки электронной подписи (услуга CLB.11) в «Наименование организации» выдано 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 ЗАО «Гринатом» и утверждён план-график проведения проверки.

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

Начальник отдела криптографической защиты «И.О. Фамилия»

Приложение №28. Сводная таблица по объекту проверки

№п/п	Наименование предприятия	Администратор безопасности	Пользователь СКЗИ (должность, Ф.И.О.)	Сертификат ключа проверки ЭП	Тип используемого СКЗИ	Серийный номер СКЗИ	Учетный номер АРМ/серийный номер, на котором установлено СКЗИ	Адрес местоположения ПЭВМ	Общесистемное программное обеспечение	Ведомость сдачи зачетов	Акт готовности СКЗИ к эксплуатации	Лицевой счет/ЖПУ	Приказ о назначении лиц, допускаемых к самостоятельной работе с СКЗИ	Заключение о возможности эксплуатации СКЗИ

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:

1. **Администратор безопасности.**

1.1. Контактные данные;
1.2. Подтверждение профессиональной подготовки;
1.3. Приказ о назначении;
1.4. Функциональные обязанности;
1.5. 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 №152 от 13 июня 2001г;
1.6. Инсталлирующие СКЗИ носители, эксплуатационная и техническая документация к СКЗИ, ключевые документы.

2. **Документы.**

2.1. Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
2.2. Акт готовности СКЗИ к эксплуатации;
2.3. Ведомость сдачи зачетов;

2.4. Заключение о возможности эксплуатации средств криптографической защиты информации;
2.5. Утвержденный перечень лиц, допускаемых к самостоятельной работе с СКЗИ;
2.6. Журнал учета хранилищ и ключей;
2.7. Журнал учета печатей (для опечатывания АРМ).

3. Помещения и хранилища.

3.1. Входные двери и замки, гарантирующие надежное закрытие помещений в нерабочее время;
3.2. Сигнализация в помещениях;
3.3. Окна помещений на первых или последних этажах зданий, окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц. Металлические решетки или ставни на таких окнах, или охранная сигнализация, или другие средства, препятствующие неконтролируемому проникновению в помещения;
3.4. Списки лиц, допускаемых в помещения;
3.5. Опечатывание помещений в нерабочее время;
3.6. Сейфы, пеналы, печати;
3.7. Расположение АРМ.

4. Проверка АРМ с установленными СКЗИ и Пользователей СКЗИ

4.1. Опечатывание АРМ;
4.2. Настройка АРМ;
4.3. Установка СЗИ НСД;
4.4. Инструментальный контроль (программная проверка настроек).

Основание для проверки: план-график проведения проверок на 201__ год.
Время проведения проверки: «__»_____ - «__»_____ 201__ года.

График проведения проверки:

№ п.п.	Вид выполняемых работ	Срок выполнения, ответственный
1	*Подготовительный этап*	

1.1	Изучение материалов по объекту проверки: • информация из выписки из Схемы организации криптографической защиты конфиденциальной информации; • информация из выписки из Центра Регистрации Удостоверяющего центра Госкорпорации «Росатом». Уточнение перечня объектов, подлежащих контролю: • перечень СКЗИ; перечень сертификатов ключей проверки электронной подписи.	
1.2.	Формирование комиссии по проверке (Приказ о командировке)	
1.3.	Согласование с уполномоченными лицами предприятия используемых технических средств проведения проверки	
2	*Проведение проверки.*	
2.1	• Прибытие на предприятие; • Встреча с руководителем, проведение установочного совещания (разъяснение цели проверки); • Проверка администратора безопасности: – Контактные данные; – Подтверждение профессиональной подготовки; – Приказ о назначении; – Функциональные 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 №152 от 13 июня 2001г; – Хранение СКЗИ, эксплуатационной и технической документации к ним. • Проверка ведения документации: – Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов; – Акт готовности СКЗИ к эксплуатации; – Ведомость сдачи зачетов; – Заключение о возможности эксплуатации средств криптографической защиты информации; – Утвержденный перечень пользователей,	

	допускаемых к самостоятельной работе с СКЗИ; – Журнал учета хранилищ и ключей; – Журнал учета печатей (для опечатывания АРМ).	
2.2	• Проверка помещений и хранилищ, где установлены СКЗИ или хранятся ключевые документы к ним на соответствие требованиям эксплуатационной и технической документации к СКЗИ и 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 №152 от 13 июня 2001г; • Проверка АРМ с установленными СКЗИ на соответствие требованиям эксплуатационной и технической документации к СКЗИ и 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 №152 от 13 июня 2001г.	
2.3	Формирование акта проверки	
2.4	Доклад результатов проверки руководству предприятия	

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

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

Приложение №30. Контрольный список

КОНТРОЛЬНЫЙ СПИСОК

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»

№	Требование	Комментарии
1. Администратор безопасности		
1.1. ☐	Контактные данные	
1.2. ☐	Подтверждение профессиональной подготовки в наличии	
1.3. ☐	Приказ о назначении в наличии	
1.4. ☐	Функциональные обязанности зафиксированы в функциональных инструкциях	
1.5. ☐	Расписка в ознакомлении 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 №152 от 13 июня 2001г	
1.6. ☐	Инсталлирующие СКЗИ носители, эксплуатационная и техническая документация к СКЗИ, ключевые документы хранятся в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение	
2. Проверка документов		
2.1.☐	Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним,	

	ключевых документов ведется		
2.2.☐	Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов сшит надлежащим образом		
2.3.☐	Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведется верно		
2.4.☐	Ключевые носители учтены в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов		
2.5.☐	Акты готовности СКЗИ к эксплуатации в наличии		
2.6.☐	Акты готовности СКЗИ к эксплуатации оформлены верно		
2.7.☐	Акты готовности СКЗИ к эксплуатации актуальны		
2.8.☐	Ведомость сдачи зачетов на всех пользователей СКЗИ в наличии		
2.9.☐	Ведомость сдачи зачетов на всех пользователей СКЗИ оформлена верно		
2.10.☐	Заключения о возможности эксплуатации средств криптографической защиты информации в наличии		
2.11.☐	Утвержденный Перечень лиц, допускаемых к самостоятельной работе с СКЗИ в наличии		
2.12.☐	Журнал учета хранилищ и ключей ведется		
2.13.☐	Журнал учета хранилищ и ключей актуален		
2.14.☐	Журнал учета печатей (для опечатывания АРМ) ведется		
2.15.☐	Журнал учета печатей (для опечатывания АРМ) актуален		
3. Проверка помещений и хранилищ			
3.1.☐	Есть список сотрудников, допущенных в помещение		

3.2. ☐	Помещения имеют прочные входные двери с замками, гарантирующие надежное закрытие помещений в нерабочее время		
3.3. ☐	Помещения оборудованы сигнализацией		
3.4. ☐	Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, оборудованы металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения		
3.5. ☐	Списки лиц, допускаемых в помещения в наличии		
3.6. ☐	Списки лиц, допускаемых в помещения актуальны		
3.7. ☐	Помещение запирается в нерабочее время		
3.8. ☐	Помещение опечатывается в нерабочее время		
3.9. ☐	Сейфы, пеналы, печати в наличии и используются		
3.10. ☐	Мониторы АРМ с установленными СКЗИ не направлены в сторону окон (в случае, если окна не защищены) или входной двери		
4. Проверка АРМ с установленными СКЗИ и Пользователей СКЗИ			
4.1. ☐	Пароль на вход в операционную систему установлен		
4.2. ☐	Пароль на вход в BIOS установлен		
4.3. ☐	У пользователя стандартные права		
4.4. ☐	Сертифицированное СЗИ НСД установлено		
4.5. ☐	Сертифицированный антивирус установлен		

4.6. ☐	Рабочее место соответствует стандарту оснащения		
4.7. ☐	Результаты инструментального контроля собраны (тип СКЗИ и номер лицензии)		
4.8. ☐	У Пользователей СКЗИ есть персональные печати		
4.9. ☐	Носители ключевой информации присутствуют у Пользователей СКЗИ		
4.10. ☐	Не выявлено оставленных без присмотра ключей ЭП		
4.11. ☐	Ключевые носители хранятся в личных опечатываемых тубусах		
4.12. ☐	Личные опечатываемые тубусы хранятся в опечатываемых хранилищах		

Приложение №31. Акт проверки

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 «Наименование организации»

« » _____ 201 г. г. _____

В соответствии с планом основных мероприятий органа криптографической защиты лицензиата[2] ФСБ России ЗАО «Гринатом» (далее – ОКЗ) « » _____ 201 года «должность проверяющего» «Фамилия И.О. проверяющего» проведена проверка 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».

В ходе проверки установлено следующее:

1. **Организация и обеспечение безопасности с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в «Наименование организации».**

Работы по защите с использованием средств криптографической защиты информации осуществляет на договорной основе (договор присоединения от 06.07.2012 № 22/2143-Д) лицензиат ФСБ России ЗАО «Гринатом».

В соответствии с заявлениями №__ от _____ и №__ от _____ «Наименование организации» оказывается услуга CLB.18 в объеме « » единиц, включающая работы, определенные в пунктах Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств постановления правительства от 16 апреля 2012 г. N 313 «Об утверждении положения О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических)

---

[2] Лицензия от 23.07.2015 ЛСЗ №0011890 Рег.№14464 на деятельность 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).

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)»:

12. Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств.
13. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем.
14. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
20. Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
21. Передача шифровальных (криптографических) средств.

В соответствии с регламентом оказания услуги CLB.18 в «Наименование организации»:

Руководителем организации должен быть реализован следующий комплекс мероприятий:

- локальным нормативным актом назначен администратор безопасности;
- локальным нормативным актом назначены лица, допускаемые к самостоятельной работе со средствами криптографической защиты информации (далее – СКЗИ).

Администратором безопасности должны быть:

- направлены в Орган криптографической защиты информации ЗАО «Гринатом» Заявления на СКЗИ, копия локального нормативного акта о назначении администратора безопасности и копия локального нормативного акта о назначении лиц, допускаемых к самостоятельной работе с СКЗИ;
- осуществлен поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним;
- проведены мероприятия по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них

сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам и требованиями лицензиата ФСБ России;
- осуществлен допуск пользователей к работе с СКЗИ на основании локального нормативного акта о назначении лиц, допускаемых к самостоятельной работе с СКЗИ после прохождения ими соответствующего обучения и сдачи зачетов;
- направлены в ОКЗ Ведомости сдачи зачетов пользователей СКЗИ, Акты готовности СКЗИ к эксплуатации и копия заполненных страниц Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- получены соответствующие заключения ОКЗ о возможности эксплуатации СКЗИ;
- осуществляется контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатами соответствия ФСБ России и требованиями органа криптографической защиты лицензиата ФСБ России.

Для оценки организации и состояния защиты информации представлены следующие документы:
- …
- …

В ходе проверки установлено:

1. Мероприятия по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов соответствия, а также в соответствии с эксплуатационной и технической документацией к этим средствам и требованиями ОКЗ **выполнены частично/полностью** на « » (количество словами) АРМ, в соответствии с поданными в ОКЗ Заявлениями на СКЗИ и полученными Заключениями о возможности эксплуатации СКЗИ.

Обнаружены следующие недостатки:
– …
– …

2. Хранение ключевой документации осуществляется:
– …
– …

3. Помещения:
– …
– …

2. Выводы

Основными причинами выявленных недостатков являются:

1. …
2. …

3. Рекомендации

1. …
2. …

Руководитель проверки

_____/_____
(подпись) (Ф.И.О)

Члены комиссии

_____/_____
(подпись) (Ф.И.О)

_____/_____
(подпись) (Ф.И.О)

Руководитель Органа криптографической защиты
ЗАО «Гринатом»

_____/_____
(подпись) (Ф.И.О)

Начальник управления информационной безопасности
ЗАО «Гринатом»

_____/_____
(подпись) (Ф.И.О)

С актом ознакомлен

«Должность уполномоченного
лица, Наименование организации» _____/_____
(подпись) (Ф.И.О)

Приложение №32. Отчет о проверке

ОТЧЕТ

о проверке 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»

« » _____ 201 г. г. _____

В соответствии с 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» (копия Приказа, Приложение №1), Планом-графиком проведения проверок на 2015 год (копия Плана-графика, Приложение №2) и 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 «Наименование организации» (Приложение №3) Органом криптографической защиты лицензиата ФСБ России ЗАО «Гринатом» (далее – ОКЗ) в лице «должность проверяющего» «Фамилия И.О. проверяющего» « » _____ 201 года проведена проверка 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».

Подробная информация о результатах проверки находится 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» (Приложение №4).

Выводы:

1. …
2. …

Приложения:

1. 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;

2. Программа проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ;
3. 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.

Руководитель проверки

_____/_____

(подпись) (Ф.И.О)

Приложение №33. План устранения недостатков

«___» _____ 20___ г

ПЛАН

реализации рекомендаций по результатам проверки лицензиата ФСБ России ЗАО «Гринатом» в «Наименование организации»

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

«Должность уполномоченного лица, Наименование организации»

_____/_____

(подпись) (Ф.И.О)

Приложение № 4

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

ФОРМА АКТА СДАЧИ-ПРИЕМКИ ОКАЗАННЫХ УСЛУГ

по Договору №_____ от «___»_____г.

г. Москва «_____» _____201__ г.

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

Закрытое акционерное общество «Гринатом» (ЗАО «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 18%_____(_____) 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.

Подписи Сторон:

Заказчик:

_____

_____

_____

М.П.

Исполнитель:

ЗАО «Гринатом»

_____

_____

М.П.

От Исполнителя:

Генеральный директор
ЗАО «Гринатом»

_____М.Ю. Ермолаев

М.П.

Приложение № 5

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

Перечень и стоимость услуг Исполнителя

г. Москва «01» октября 2015 г.

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	Предоставление услуг Удостоверяющего центра с записью сертификата и ключа электронной подписи на ключевой носитель	4491,70 единовременно за один ключевой документ	685,17
2.	CLB.18	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 ЗАО «Гринатом»	1130,61 в квартал за одно рабочее место с СКЗИ	172,47
3.	CLB.18	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.	871,68 в квартал за одно рабочее место с СКЗИ	132,97
4.	GEN.23	Услуга Администратора безопасности ЗАО «Гринатом»	3125,21 в квартал за одно рабочее место с СКЗИ	476,73

№	Код вида Услуги	Наименование вида Услуги	Стоимость Услуги с НДС, руб.	В том числе НДС, руб.
5.	GEN.23 (Электросталь)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Электросталь	1059,99 в квартал за одно рабочее место с СКЗИ	161,69
6.	GEN.23 (Ковров)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Ковров	554,79 в квартал за одно рабочее место с СКЗИ	84,63
7.	GEN.23 (Владимир)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Владимир	500,80 в квартал за одно рабочее место с СКЗИ	76,39
8.	GEN.23 (Новоуральск)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Новоуральск	1030,78 в квартал за одно рабочее место с СКЗИ	157,24
9.	GEN.23 (Ангарск)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Ангарск	1468,05 в квартал за одно рабочее место с СКЗИ	223,94
10.	GEN.23 (Подольск)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Подольск	1212,06 в квартал за одно рабочее место с СКЗИ	184,89
11.	GEN.23 (Зеленогорск)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Зеленогорск	1330,04 в квартал за одно рабочее место с СКЗИ	202,89
12.	GEN.23 (Глазов)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Глазов	857,39 в квартал за одно рабочее место с СКЗИ	130,79
13.	GEN.23 (Новосибирск)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Новосибирск	1097,14 в квартал за одно рабочее место с СКЗИ	167,36
14.	GEN.23 (Северск)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Северск	1145,04 в квартал за одно рабочее место с СКЗИ	174,67

№	Код вида Услуги	Наименование вида Услуги	Стоимость Услуги с НДС, руб.	В том числе НДС, руб.
15.	GEN.23 (Нижний Новгород)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Нижний Новгород	1416,27 в квартал за одно рабочее место с СКЗИ	216,04
16.	GEN.23 (Санкт-Петербург)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Санкт-Петербург	1232,38 в квартал за одно рабочее место с СКЗИ	187,99
17.	GEN.23 (Саров)	Услуга Администратора безопасности ЗАО «Гринатом» в городе Саров	2597,83 в квартал за одно рабочее место с СКЗИ	396,28

От Исполнителя:

Генеральный директор
ЗАО «Гринатом»

М.П.

_____М.Ю. Ермолаев