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

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

М.П.

_____ / А.Н. Киселёв /

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ПО ИТ.
НАЧ. УПРАВЛ. И. П. ТАРАСОВ
ДОВЕРЕННОСТЬ ОТ 18.06.2021
22/306/2021-ДОВ

ПОРЯДОК

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

Москва 2021 г.

Содержание

1. Назначение и область применения

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

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

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

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

Настоящий Порядок использует ссылки на следующие документы, необходимые для контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем»:

Документ	Статус	Тип документа	Ответствен-ный
Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686 Н от 19.01.2017 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования	Действует	Лицензия	Кривовяз М.А.

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	Кривовяз М.А.
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	Кривовяз М.А.
Приказ ФСБ № 66 от 09.02.2005 г. «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»	Действует	Приказ	Кривовяз М.А.
Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты	Действует	Требование	Кривовяз М.А.

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

2. Термины, определения и сокращения

Термин	Определение
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока
Конфиденциальная информация	Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну
Обладатели конфиденциальной информации	Государственные органы, государственные организации и другие организации независимо от их организационно-правовой формы и формы собственности, индивидуальные предприниматели и физические лица
Орган криптографической защиты	Действующая на постоянной основе рабочая группа из числа работников, назначенных Приказом «О возложении дополнительных функциональных обязанностей работников Органа криптографической защиты АО «Гринатом» на штатных работников»
Пользователи СКЗИ	Физические лица, непосредственно допущенные к работе с СКЗИ
Система	Информационная/телекоммуникационная система, защищенная с использованием шифровальных (криптографических) средств

Средства криптографической защиты информации (СКЗИ)	Средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче; средства имитозащиты - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации; средства электронной подписи; средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций; средства изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;

	ключевые документы - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах; аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин; программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;

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

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

3. Описание процесса

3.1. Цель процесса

Предоставление услуг ОКЗ по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с

использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

3.2. Задачи процесса

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

3.3. Участники группы процессов и их роли

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

3.4. Основные выходы процесса

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация,/ Дивизион/ Организация)
1	2	3	4
1	Письмо в Банк о предоставлении информации, необходимой для контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем	Банк	Организация
2	Письмо в Банк с запросом на приведение Системы в соответствие с ЕОМУ	Банк	Организация
3	Заключение Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе	ООКИ	Организация
4	Отчет о проведении регламентных работ	ООКИ	Организация
5	Выписка из Заключения Органа криптографической	Банк	Организация

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

3.5. Основные входы процесса

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

	(доп. соглашений) на Системы		
3	Скан-копии документов по аттестации на соответствие требованиям безопасности объекта информатизации, где обрабатывается конфиденциальная информация	ООКИ	Организация
4	Единые отраслевые методические указания по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утв. Приказом от 22.10.2015 №1/1009-П	ГК «Росатом»	Корпорация
5	Выписка из Заключения Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе	АО «Гринатом»	Организация
6	Документы из Банка	Банк	Организация
7	Отчет о проведении регламентных работ	АО «Гринатом»	Организация
8	Ответ Банка о приведении Системы в соответствие с ЕОМУ	Банк	Организация
9	Заключение Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе	АО «Гринатом»	Организация

3.6. Описание процесса

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

в ОКЗ из ООКИ поступает следующий комплект документов:

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

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

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

В случае если ООКИ отключается от услуги CLB.21:

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

Руководитель ОКЗ:

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

Если принято решение об оказании услуги CLB.21:

Проверяющий:

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

  Для оценки доверия к технологии, реализующей инфраструктуру ключевой системы:

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

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

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

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

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

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

Для оценки доверия к участникам процессов обработки данных:

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

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

Руководитель ОКЗ:

- Утверждает Заключение.

Если Система соответствует ЕОМУ:

Проверяющий:

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

Мониторинг актуальности документов ФСБ России:

– лицензии ФСБ России на соответствующие виды деятельности,

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

– сертификата соответствия ФСБ России на средства криптографической защиты информации,

– сертификата соответствия ФСБ на СПДС.

Мониторинг документов производителей программного обеспечения:

– заключения о корректности встраивания СКЗИ в систему,

– документации на программное обеспечение системы ДБО.

Мониторинг актуальности документов ФСТЭК:

– сертификата соответствия ФСТЭК на антивирусное ПО,

– сертификата соответствия ФСТЭК на СЗИ от НСД,

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

Мониторинг документов банка:

– генеральной лицензии на осуществление банковских операций,

– документа о выполнении Стандарта Банка России,

– заключения Органа криптографической защиты о возможности эксплуатации СКЗИ,

– лицензии на программное обеспечение,

– документов, регламентирующих жизненный цикл ключевой системы.

Мониторинг документов Минкомсвязи России:

– свидетельства об аккредитации,

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

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

Проверяющий:

- формирует, согласовывает и направляет в ООКИ новое Заключение.

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

Проверяющий:

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

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

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

4. Нормативные ссылки

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Приказ ФАПСИ № 152 от 13.06.2001г. «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ ФСБ № 66 от 09.02.2005г «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Федеральный закон Российской Федерации от 06.04.11 г. № 63-ФЗ "Об электронной подписи";
- Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности";

- Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686 Н от 19.01.2017 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» (с пометкой «Для служебного пользования»);
- Постановление №313 от 16.04.2012 г. Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- Единые отраслевые методические указания по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утв. Приказом от 22.10.2015 №1/1009-П.

5. Порядок внесения изменений

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

6. Контроль и ответственность

6.1 Порядок обязаны соблюдать все следующие участники процесса

Руководитель ОКЗ;
Проверяющий.

6.2. Ответственность работников за несоблюдение требований Порядка

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

7. Перечень приложений

Приложение №1. Матрица ответственности.
Приложение №2. Схема процесса.
Приложение №3. Дополнительные выходы и дополнительные входы.
Приложение №4. Форма Заявления на подключение/отключение услуги по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
Приложение №5. Форма письма в Банк с запросом о предоставлении информации, необходимой для контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
Приложение №6. Форма Заключения Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе.

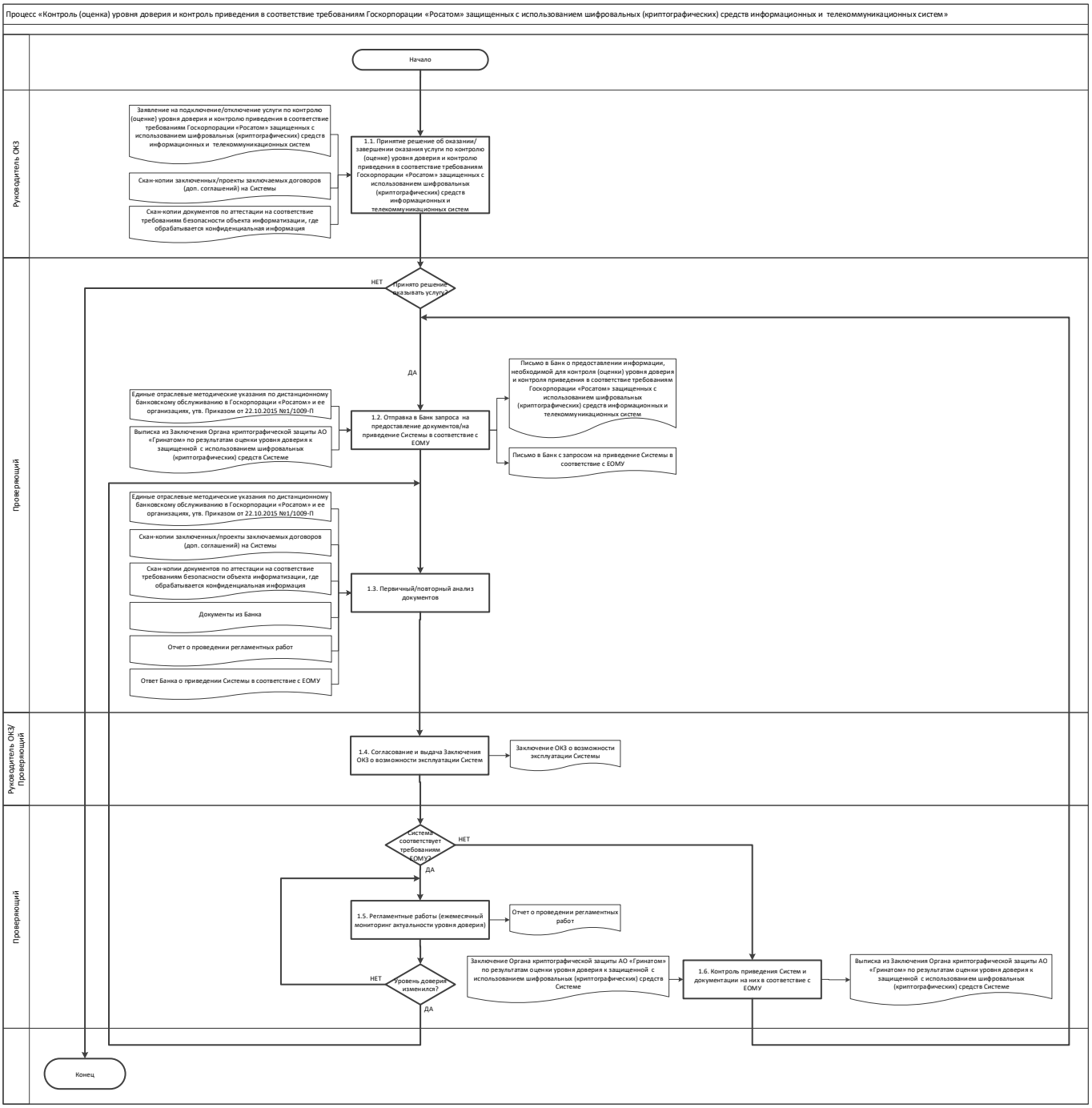
Приложение №1. Матрица ответственности

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

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 своей предметной области	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации

Утв	Утверждающий	Утверждает - принимает окончательное решение по результату подпроцессу/процедуре	Коллегиальные органы (Наблюдательный совет, Правление и прочие) Генеральный директор Корпорации, Руководители Корпорации /Дивизионов/Организаций
С	Согласовывающий	Согласовывает /одобряет результаты подпроцесса/процедуры для дальнейшего принятия решений	Коллегиальные органы Руководители Корпорации/ Дивизионов/ Организаций
Э	Экспертирующий	Осуществляет экспертизу по подпроцессу/процедуре	Коллегиальные органы Структурное подразделение Корпорации/Дивизиона/ Организации
Инф	Информируемый	Получает информацию о ходе/результате подпроцесса /процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации Коллегиальные органы

Приложение №2. Схема процесса



Приложение №3. Дополнительные выходы и дополнительные входы

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

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

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

ЗАЯВЛЕНИЕ
на
ПОДКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ

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

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

_____
наименование организации, включая организационно-правовую форму

в лице _____,
должность

_____,
фамилия, имя, отчество

действующего на основании _____

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

контроль (оценку) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем, указанных в таблице №1.

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

Таблица №1

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

Администратор безопасности

_____/_____
(подпись) (ФИО)

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ДОЛЖНОСТНОГО ЛИЦА>

_____ _____/_____
(подпись) (ФИО)

м.п.

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

Акционерное общество «Гринатом»
(АО «Гринатом»)

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

«ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ЛИЦА»
«НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ»

«И.О.ФАМИЛИЯ»

_____ № _____

На № _____ от _____

О проведении оценки уровня доверия
к «НАИМЕНОВАНИЕ СИСТЕМЫ»

Уважаемый(ая) <ИМЯ, ОТЧЕСТВО>!

Орган криптографической защиты лицензиата ФСБ России АО «Гринатом» (лицензия ЛСЗ №0014254 Рег. №15686Н от 19.01.2017г.) в рамках контроля (оценки) уровня доверия и приведения в соответствие требованиям Госкорпорации «Росатом» «НАИМЕНОВАНИЕ СИСТЕМЫ» (договор от _____ №_____) просит Вас предоставить документацию:

копию лицензии ФСБ России на разработку, производство, распространение шифровальных(криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных(криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных(криптографических) средств;

копию лицензии на программное обеспечение, передаваемое Банком Клиенту в рамках договора от _____ №_____;

копию сертификата соответствия ФСБ России на средство, реализующее инфраструктуру ключевой системы;

копию документации на СКЗИ (копию учтенного формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника));

копию документации, регламентирующей жизненный цикл ключевой системы;

копию свидетельства Минкомсвязи России об аккредитации удостоверяющего центра Банка;

копию документа, подтверждающего соответствие Стандарту Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации СТО БР ИББС-1.0-2014»;

копию сертификата соответствия ФСБ России на средство автоматизации удостоверяющего центра;

копию регламентов служб TSP и OCSP (документацию на службу онлайновой проверки статусов сертификатов и службы штампов времени);

копию документации о поддержке формата усовершенствованной подписи;

копию сертификата соответствия ФСБ России на средства криптографической защиты информации, использующиеся в «НАИМЕНОВАНИЕ СИСТЕМЫ»;

копию сертификата соответствия ФСТЭК России на ключевые носители;

копию сертификата соответствия ФСТЭК России на СЗИ от НСД;

копию сертификата соответствия ФСТЭК России на антивирусное ПО;

копию заключения о корректности встраивания СКЗИ в «НАИМЕНОВАНИЕ СИСТЕМЫ»;

копию документации на «НАИМЕНОВАНИЕ СИСТЕМЫ»;

копию документа, подтверждающего оценку соответствия по требованиям безопасности информации (копия аттестата соответствия по требованиям безопасности информации на АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация);

копию сертификата соответствия ФСБ России на СПДС;

копию локальных нормативных актов, обеспечивающих повышение осведомленности работников в области обеспечения защиты информации;

копию локальных нормативных актов по порядку применения организационных мер защиты информации и использования технических средств защиты информации;

Непредоставление указанных документов будет рассматриваться как их отсутствие при контроле (оценке) уровня доверия, и приведении в соответствие требованиям Госкорпорации «Росатом» «НАИМЕНОВАНИЕ СИСТЕМЫ».

С уважением,

Начальник Отдела криптографической защиты <И.О. ФАМИЛИЯ>

(по дов. № _____-_____ от __.__.__)

Приложение №6. Форма Заключения Органа криптографической защиты АО «Гринатом» по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств Системе

УТВЕРЖДАЮ

Начальник
отдела криптографической защиты
АО «Гринатом»

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

ЗАКЛЮЧЕНИЕ

по результатам оценки уровня доверия
к *«наименование системы»*

Москва 20__ г.

1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

2. ВВОДНАЯ ЧАСТЬ

2.1. Основание для выдачи заключения

Основанием для выдачи настоящего заключения является договор от _____ № _____.

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

«Наименование системы».

2.3. Вопросы для исследования

– Обеспечение доверия к технологии, реализующей инфраструктуру ключевой системы;
– Обеспечение доверия к средствам криптографической защиты информации, входящим в состав системы обработки данных;
– Обеспечение доверия к средствам обработки и отображения данных;
– Обеспечение доверия к участникам процессов обработки данных.

3. ИССЛЕДОВАТЕЛЬСКАЯ ЧАСТЬ

Оценка уровня доверия к системе проводится в соответствии с ЕОМУ.
Методы исследования:
- анализ представленной в ОКЗ АО «Гринатом» документации на систему;
- анализ документа *«наименование договора/соглашения на использование системы»*.

4. В ПРОЦЕССЕ ИССЛЕДОВАНИЯ УСТАНОВЛЕНО

4.1. Описание системы

4.2. Инфраструктура ключевой системы

4.3. Жизненный цикл ключевых документов

4.3.1 Получение, создание и замена ключевых документов

4.3.2 Хранение ключевых документов

4.3.3 Уничтожение ключевых документов

4.4. Жизненный цикл СКЗИ

4.4.1 Получение СКЗИ

4.4.2 Проверка готовности, установка и эксплуатация СКЗИ

4.4.3 Уничтожение СКЗИ

4.5. Механизм обеспечения конфиденциальности и целостности информации в системе

4.6. Выполнение требований по безопасности информации на стороне Клиента и Банка

4.7. Анализ документа *«наименование договора/соглашения на использование системы»*

5. ОЦЕНКА СООТВЕТСТВИЯ

5.1. Результаты исследования технологии, реализующей инфраструктуру ключевой системы

Критерий оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия
Лицензия ФСБ России Банка на осуществление лицензируемых видов деятельности					
Документ, подтверждающий наличие прав Банка на использование средства, реализующего инфраструктуру ключевой системы и СКЗИ, применяемого в составе средства, реализующего инфраструктуру ключевой системы (договор, лицензия и пр.)					
Действующий сертификат соответствия ФСБ России на средство, реализующие инфраструктуру ключевой системы, сертифицированное в соответствии с системой сертификации РОСС RU.0001.030001 по классу не ниже КС2					
Действующий сертификат соответствия ФСБ России на средство, реализующее инфраструктуру ключевой системы с указанием на соответствие «Требованиям к средствам удостоверяющего центра» (приложение №2 к приказу ФСБ России от 27.12.2011 №796 «Об утверждении Требований к средствам электронной подписи и требований к средствам удостоверяющего центра»					
Действующий сертификат соответствия ФСБ России на СКЗИ, применяемое для работы средства, реализующего инфраструктуру ключевой системы с классом защиты не ниже КС2					
Использование Клиентом сертифицированных ФСТЭК России/ФСБ России или несертифицированных (типа токен/смарт-карты или flash-носитель/жесткий диск ПЭВМ) ключевых носителей					
Использование Банком сертифицированных ФСТЭК России/ФСБ России или несертифицированных (типа токен/смарт-карты или flash-носитель/жесткий диск ПЭВМ) ключевых носителей					
Документы, регламентирующие жизненный цикл ключевой системы					
Свидетельство об аккредитации УЦ в Минкомсвязи России					

В Системе для подписи используется усиленная квалифицированная/ усиленная неквалифицированная электронная подпись					
Документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации)					
Наличие дополнительных служб удостоверяющего центра (службы проверки статуса сертификата (online certificate status protocol) и штампов времени (time-stamp protocol)) и использование формата усовершенствованной электронной подписи в Системе					

5.2. Результаты исследования СКЗИ, входящих в состав системы обработки данных

Критерий оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия
Использование сертифицированных ФСБ России СКЗИ на АРМ Пользователей Клиента для обеспечения конфиденциальности информации					
Использование сертифицированных ФСБ России СКЗИ на АРМ Пользователей Клиента для обеспечения целостности информации					
Использование сертифицированных ФСБ России СКЗИ на АРМ Пользователей Банка для обеспечения целостности информации					
Документы, подтверждающие право передачи Клиенту СКЗИ и эксплуатационной и технической документации к ним, использующихся в работе Системы (договор, лицензия и пр.)					
Класс защиты применяющихся на рабочих местах пользователей Клиента Системы шифровальных (криптографических) средств					
Класс защиты применяющихся на рабочих местах пользователей Банка Системы шифровальных (криптографических) средств					

5.3. Результаты исследования средств обработки и отображения данных

Критерий оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия
Лицензия на программное обеспечение Системы					
Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Клиента					
Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Банка					
Заключение о корректности встраивания СКЗИ в Систему					
Документация на систему дистанционного банковского обслуживания (техническое описание или техническая записка, инструкция пользователя, инструкция администратора безопасности)					
Аттестат соответствия ФСТЭК на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация на стороне Клиента					

Аттестат соответствия ФСТЭК России на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация на стороне Банка					
Установлено сертифицированное антивирусное ПО на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы					
Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Клиента					
Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Банка					
Установлено сертифицированное СЗИ от НСД на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы					
Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Клиента					
Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Банка					

5.4. Результаты исследования участников процессов обработки данных

Критерий оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия
Документ, подтверждающий допуск пользователей Клиента к работе с СКЗИ в Системе					
Документ, подтверждающий допуск пользователей Банка к работе с СКЗИ в Системе					
Документ, подтверждающий прохождение обучения пользователями Системы на стороне Клиента					
Документ, подтверждающий прохождение обучения пользователями Системы на стороне Банка					
Локальные нормативные акты, определяющие права и роли работников Клиента в Системе (подписантов, администраторов безопасности)					
Локальные нормативные акты, определяющие права и роли работников Банка в Системе (подписантов, администраторов безопасности)					
Контроль администраторами безопасности условий использования СКЗИ на стороне Клиента					
Контроль администраторами безопасности условий использования СКЗИ на стороне Банка					

6. ВЫВОДЫ И РЕКОМЕНДАЦИИ

6.1. Выводы

«Наименование системы» обеспечивает _____ уровень доверия, согласно ЕОМУ.

6.2. Рекомендации

7. Список приложений