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

УТВЕРЖДАЮ
Директор по информационным технологиям
АО «Гринатом»

_____ В.В. Золотов

М.П.

ПОРЯДОК

оценки доверия к защищенным с использованием средств криптографической защиты информации системам дистанционного банковского обслуживания

Москва
2024

Содержание

1. Назначение и область применения

Настоящий порядок оценки доверия к защищенным с использованием средств криптографической защиты информации системам дистанционного банковского обслуживания (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 оценке доверия к защищенным с использованием средств криптографической защиты информации системам дистанционного банковского обслуживания, 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 средств криптографической защиты информации системы дистанционного банковского обслуживания 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 оценки доверия к защищенным с использованием средств криптографической защиты информации системам дистанционного банковского обслуживания:

Документ	Статус	Тип документа	Ответственный
Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686 Н от 19.01.2017 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных и	Действует	Лицензия	Начальник управления доверенных ИТ-сервисов

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 от 06.04.2011 № 63-ФЗ «Об электронной подписи»	Действует	Федеральный закон	Начальник управления доверенных ИТ-сервисов
Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»	Действует	Приказ	Начальник управления доверенных ИТ-сервисов
Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»	Действует	Приказ	Начальник управления доверенных ИТ-сервисов

Приказ Госкорпорации «Росатом» от 10.02.2021 №1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» (с пометкой «Для служебного пользования»)	Действует	Требование	Начальник управления доверенных ИТ-сервисов
Единые отраслевые методические указания по оценке доверия и приведению в соответствие требованиям по безопасности систем дистанционного банковского обслуживания в Госкорпорации «Росатом» и ее организациях, утвержденные приказом Госкорпорации «Росатом» от 28.02.2023 №1/326-П	Действует	Указания	Руководители организаций Госкорпорации «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	Защищенная с использованием средств криптографической защиты информации система дистанционного банковского обслуживания или Информационная система «Расчетный центр Корпорации»
Средства криптографической защиты информации	Средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче; средства имитозащиты - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации; средства электронной подписи; средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;

	средства изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств; ключевые документы - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах; аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;

	программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств; программно-аппаратные шифровальные (криптографические) средства - устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.
Услуга	Услуга CLB.21 «Оценка доверия к защищенным с использованием средств криптографической защиты информации системам дистанционного банковского обслуживания»
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

ЕОМУ	Единые отраслевые методические указания по оценке доверия и приведению в соответствие требованиям по безопасности систем дистанционного банковского обслуживания в Госкорпорации «Росатом» и ее организациях, утвержденные приказом Госкорпорации «Росатом» от 28.02.2023 №1/326-П
ООКИ	Организация-обладатель конфиденциальной информации
ОКЗ	Орган криптографической защиты АО «Гринатом»
Руководитель ООКИ	Руководитель организации-обладателя конфиденциальной информации
СКЗИ	Средства криптографической защиты информации

3. Описание процесса

3.1. Цель процесса

Предоставление услуги ОКЗ по оценке доверия к защищенным с использованием средств криптографической защиты информации системам дистанционного банковского обслуживания.

3.2. Задачи процесса

оценка доверия к системам;

периодическая (ежемесячная) контроль уровня доверия к системам;

выдача заключений по результатам оценки доверия к системам (далее – заключения);

контроль приведения систем в соответствие с требованиями ЕОМУ;

мониторинг актуальности документов ФСБ России, ФСТЭК России, Минцифры России, банков, производителей программного обеспечения.

3.3. Участники группы процессов и их роли

№ п.п.	Участники	Основные роли
1	Проверяющий	Оценивает доверие к системам; периодически (ежемесячно) контролирует уровень доверия к системам; составляет заключения; контролирует приведение систем в соответствие с требованиями ЕОМУ; осуществляет мониторинг актуальности документов ФСБ России, ФСТЭК России,

		Минцифры России, банков, производителей программного обеспечения.
2	Руководитель органа криптографической защиты АО «Гринатом»	Принимает решение об оказании/завершении оказания услуги; 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 оценки доверия к системе	Банк	Организация
2	Письмо в банк с запросом о приведении системы в соответствие с ЕОМУ	Банк	Организация
3	Заключение	ООКИ	Организация
4	Отчет о проведении регламентных работ	ООКИ	Организация
5	Выписка из заключения	Банк	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	Заявление на подключение/ отключение услуги	ООКИ	Организация

2	Скан-копии заключенных/проекты заключаемых договоров (доп. соглашений) на систему	ООКИ	Организация
3	Скан-копии документов, подтверждающих соответствие системы требованиям по безопасности информации	ООКИ	Организация
4	Единые отраслевые методические указания по оценке доверия и приведению в соответствие требованиям по безопасности систем дистанционного банковского обслуживания в Госкорпорации «Росатом» и ее организациях, утвержденные приказом Госкорпорации «Росатом» от 28.02.2023 №1/326-П	ГК «Росатом»	Корпорация
5	Выписка из заключения	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	АО «Гринатом»	Организация

3.6. Описание процесса

В случае если ООКИ подключается к услуге.

В ОКЗ из ООКИ поступает следующий комплект документов:

оригинал подписанного заявления на подключение услуги (Приложение №4),

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

скан-копии документов, подтверждающих соответствие системы требованиям по безопасности информации.

В случае если ООКИ отключается от услуги.

В ОКЗ из ООКИ поступает заявление на отключение от услуги (Приложение №4).

Руководитель ОКЗ:

Принимает решение об оказании/завершении оказания услуги в соответствии с поступившим заявлением на подключение, либо на отключение от услуги.

Если принято решение об оказании услуги:

Проверяющий:

Формирует и направляет в ООКИ проект письма в банк с запросом следующей документации (в случае необходимости):

– копию документа, подтверждающего право осуществлять лицензируемые виды деятельности (копия лицензии ФСБ России на виды деятельности в области криптографической защиты);

– копии документов, подтверждающих наличие законного основания для владения и использования программного обеспечения системы, средства, реализующего инфраструктуру ключевой системы (далее – ИКС), СКЗИ, в составе средства, реализующего ИКС, а также СКЗИ, эксплуатирующихся для обеспечения целостности и конфиденциальности информации на рабочих местах пользователей системы на стороне банка и клиента (копии договоров, заполненных формуляров, лицензий и пр.);

– копии сертификатов соответствия ФСБ России с актуальным сроком действия на средство, реализующее ИКС, СКЗИ в составе средства, реализующего ИКС, а также СКЗИ, эксплуатирующиеся для обеспечения целостности и конфиденциальности информации на рабочих местах пользователей системы на стороне банка (при наличии пользователей СКЗИ, работающих в системе, на стороне банка) и клиента;

– копию документа, регламентирующего жизненный цикл ключевой системы (копию актуального регламента удостоверяющего центра и пр.);

– копии сертификатов соответствия ФСБ России/ФСТЭК России с актуальным сроком действия на ключевые носители, эксплуатирующиеся в системе на стороне банка и клиента;

– копию заключения органа криптографической защиты о возможности эксплуатации СКЗИ на стороне банка в соответствии с инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 № 152;

– копию документа, подтверждающего выполнение положения от 04.06.2020 №719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» и результаты внешнего аудита;

– копии документов, подтверждающих использование алгоритмов ГОСТ и сертифицированных СКЗИ для обеспечения конфиденциальности информации в системе (в том числе при ее передаче в сети Интернет);

– копии документов, подтверждающих использование сертифицированного ФСТЭК России прикладного программного обеспечения системы и приложений (сертификаты соответствия и пр.);

– копии документов, подтверждающих использование в системе методов идентификации и аутентификации (копии регламента процесса идентификации пользователей в системе, технического задания/пояснительной записки на систему и пр.);

– копии документов о проведении оценки корректности встраивания СКЗИ в систему или использовании вызовов, использование которых при разработке систем на основе СКЗИ возможно без дополнительных тематических исследований (копия заключения о корректности встраивания СКЗИ в систему и пр.);

– копию документа, подтверждающего соответствие системы требованиям по безопасности информации на стороне банка (копию первой страницы аттестата соответствия системы требованиям по безопасности информации и пр.);

– копии документов, подтверждающих наличие сертифицированного антивирусного программного обеспечения на серверах, где функционирует средство, реализующее ИКС, СКЗИ, в составе средства, реализующего ИКС, а также на рабочих местах пользователей системы на стороне банка (при наличии пользователей СКЗИ, работающих в системе, на стороне банка);

– копии документов, подтверждающих наличие сертифицированных средств защиты информации от несанкционированного доступа на серверах, где функционирует средство, реализующее ИКС, СКЗИ, в составе средства, реализующего ИКС, а также на рабочих местах пользователей системы на стороне банка (при наличии пользователей СКЗИ, работающих в системе, на стороне банка);

– копию подписанного руководителем организации акта категорирования системы и приказа о создании комиссии по категорированию;

– копию ответного письма ФСТЭК России о согласовании присвоенной категории значимости (для значимого объекта критической информационной инфраструктуры (далее – ОКИИ) также номер реестра значимого ОКИИ);

– копию приказа (для значимого ОКИИ), утверждающего план, или плана реагирования на инциденты, приказа, утверждающего план, или плана мероприятий по обеспечению безопасности значимого ОКИИ;

– копии документов, подтверждающих прохождение регулярного обучения пользователей системы правилам работы с СКЗИ на стороне банка (при наличии пользователей СКЗИ на стороне банка копии порядка периодического обучения, сертификатов об обучении и пр.);

– копии документов, подтверждающих допуск пользователей к работе с СКЗИ в системе на стороне банка (при наличии пользователей СКЗИ на стороне банка копии приказа о допуске пользователей к работе с СКЗИ в системе с указанием полномочий и ответственности, матрицы доступа и пр.);

– копию документа, регламентирующего проведение администраторами безопасности периодического контроля условий использования СКЗИ на стороне банка (копию порядка проведения контроля и пр.).

Анализирует полученную от банка документацию;

Составляет и согласовывает заключение (Приложение №5).

Руководитель ОКЗ:

Утверждает заключение.

Если система соответствует ЕОМУ:

Проверяющий:

Отправляет заключение в ООКИ;

Осуществляет регламентные работы (ежемесячно):

мониторинг актуальности документов ФСБ России (лицензий ФСБ России на соответствующие виды деятельности, сертификатов соответствия ФСБ России на средства, реализующие инфраструктуру ключевой системы, сертификатов соответствия ФСБ России на средства криптографической защиты информации), мониторинг актуальности документов ФСТЭК России (сертификатов соответствия ФСТЭК России на антивирусное программное обеспечение, сертификатов соответствия ФСТЭК России на средства защиты информации от несанкционированного доступа, аттестатов соответствия требованиям по безопасности информации на систему), мониторинг актуальности документов Минцифры России (свидетельств об аккредитации), мониторинг актуальности документов банка (документов, подтверждающих выполнение требований Банка России по обеспечению зашиты информации, заключений органа криптографической защиты о возможности эксплуатации СКЗИ, лицензий на программное обеспечение, документов, регламентирующих жизненный цикл ключевой системы), мониторинг документов производителей программного обеспечения (заключения о корректности встраивания СКЗИ в систему, документации на программное обеспечение системы);

формирует и отправляет в ООКИ отчет о проведении регламентных работ.

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

Проверяющий:

формирует, согласовывает и направляет в ООКИ новое заключение.

Если система не соответствует высокому уровню согласно ЕОМУ, либо если в ходе проведения регламентных работ выяснилось, что уровень доверия к системе понизился, то

Проверяющий:

Формирует выписку из заключения;

Направляет в ООКИ проект письма в банк с запросом о приведении системы в соответствие с ЕОМУ и выпиской из заключения;

Анализирует полученный ответ от банка о приведении 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»;

Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»;

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;

Постановление Правительства Российской Федерации от 16.04.2012 №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

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»);

Приказ Госкорпорации «Росатом» от 28.02.2023 №1/326-П «Об утверждении Единых отраслевых методических указаний по оценке доверия и приведению в

соответствие требованиям по безопасности систем дистанционного банковского обслуживания в Госкорпорации «Росатом» и ее организациях».

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

Приложение №5. Форма заключения

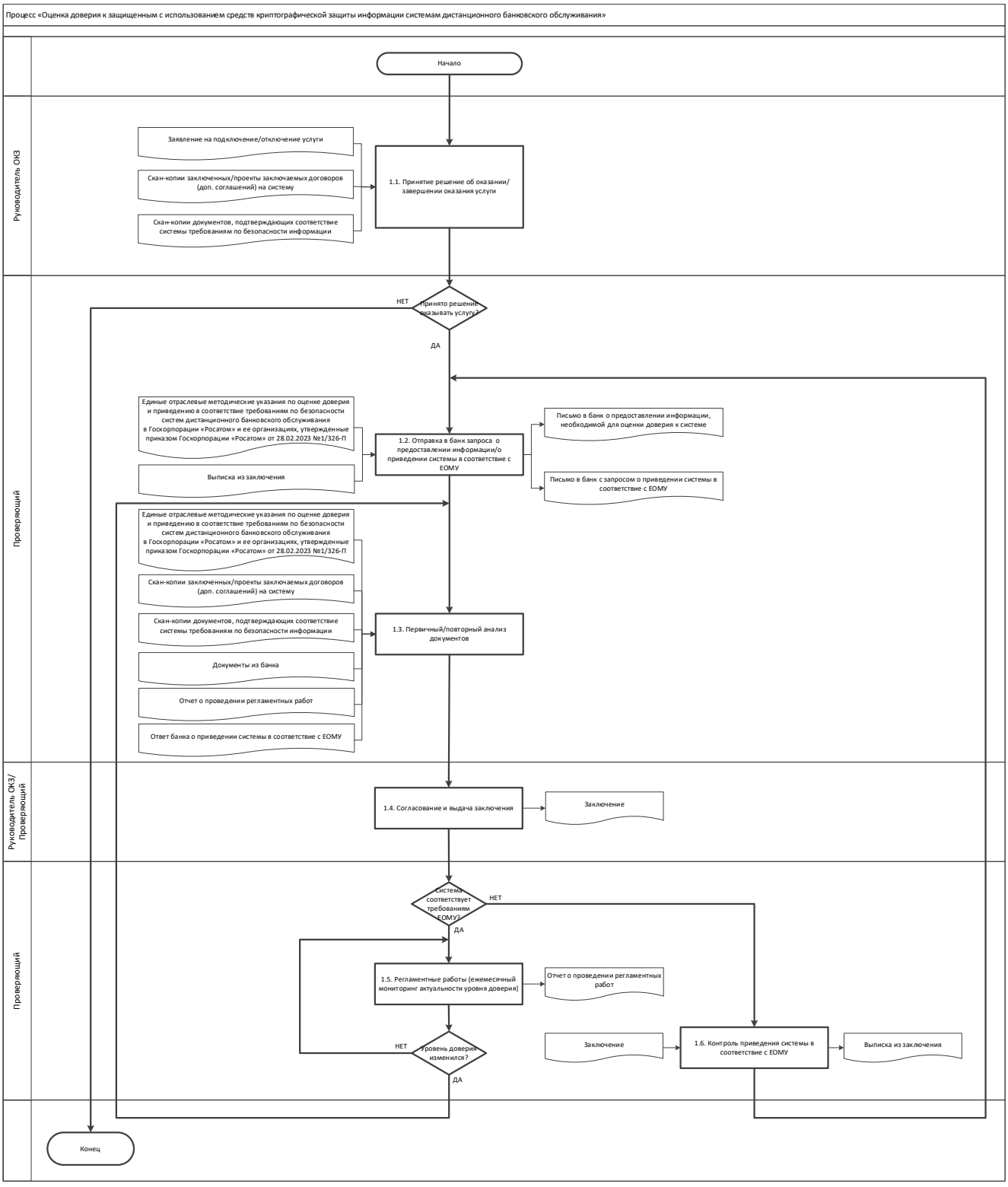
Приложение №1. Матрица ответственности

Процесс	**Участники процесса**	
	Руководитель ОКЗ	**Проверяющий**
Оценка доверия к системам	Утв.	О

Сокращение	Название роли	Определение	Исполнитель Роли
М	Методолог	Формирует требования к организации деятельности в рамках подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации
И	Интегратор	Интегрирует результаты подпроцесса/процедуры и отвечает за организацию подпроцесса/процедуры, включая взаимодействие участников	Структурное подразделение Корпорации/Дивизиона/ Организации
К	Контролер	Осуществляет контроль выполнения и достижения результатов подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
О	Ответственный	Несет ответственность за достижение результата по подпроцессу/процедуре в своей предметной области	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации

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

Приложение №2. Схема процесса



Приложение №3. Дополнительные выходы и дополнительные входы

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

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

Приложение №4. Форма заявления на подключение/отключение услуги

Заявление
на услугу по оценке доверия к защищенным с использованием средств криптографической защиты информации системам дистанционного банковского обслуживания

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

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____

в рамках оказания услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств запрашивает предоставление услуги по оценке доверия к защищенным с использованием средств криптографической защиты информации системам дистанционного банковского обслуживания (код услуги CLB.21), указанных в таблице.

№ п/п	Наименование системы, защищенной с использованием СКЗИ	ФИО пользователя	Учетный номер АРМ, на котором установлена/ планируется установка системы	Адрес месторасположения АРМ, на котором установлена/ планируется установка системы	Наименование и версия СКЗИ, установленного на АРМ (используемого в системе)	Наименование и версия ключевого носителя, используемого в системе для хранения ключевой информации	Операционная система, антивирусные средства, средства защиты информации от несанкционированного доступа, установленные на АРМ	Реквизиты аттестата соответствия системы требованиям по безопасности информации	Наименование и реквизиты договора на систему (копия договора прилагается)

Копии заключаемых/заключенных договоров на систему(ы), приложений и дополнительных соглашений прилагаются.

Администратор безопасности _____/_____
(подпись) (Ф.И.О)

<указывается должность уполномоченного лица> _____/_____
(подпись) (Ф.И.О)

М.П.

Приложение №5. Форма заключения

Рег. № _____
от _____

УТВЕРЖДАЮ

<указывается должность>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

ЗАКЛЮЧЕНИЕ
по результатам оценки доверия

<указывается наименование Системы>

г. Москва

1. Термины, определения и сокращения

2. Вводная часть

2.1. Основание для выдачи заключения

Указываются реквизиты договора, на основании которого проводятся работы.

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

Указывается наименование системы.

2.3. Вопросы для исследования

доверие к ключевой системе;
доверие к СКЗИ, входящим в состав системы;
доверие к среде функционирования СКЗИ;
доверие к системе, как к ОКИИ;
доверие к участникам процессов обработки данных.

3. Исследовательская часть

Оценка доверия к системе проводится в соответствии с ЕОМУ.

Методы исследования:
анализ представленной в орган криптографической защиты <указывается наименование лицензиата ФСБ России> документации на систему;
анализ договора на эксплуатацию системы.

4. В процессе исследования установлено

4.1. Описание системы

В данном разделе указывается описание системы.

4.2. Инфраструктура ключевой системы

Указывается используемая ключевая система, программно-аппаратный комплекс удостоверяющего центра, дополнительные службы удостоверяющего центра, аккредитация удостоверяющего центра и другая информация в соответствии с ЕОМУ.

4.3. Жизненный цикл ключевых документов

Указывается жизненный цикл ключей пользователей системы (процессы создания, передачи/получения, эксплуатации, хранения, замены и уничтожения), типы ключевых носителей и другая информация в соответствии с ЕОМУ.

4.4. Жизненный цикл СКЗИ

Указывается жизненный цикл СКЗИ, использующихся в системе (процессы передачи/получения, эксплуатации, хранения, замены и уничтожения), и другая информация в соответствии с ЕОМУ.

4.5. Механизм обеспечения конфиденциальности и целостности информации в системе

Указывается механизм обеспечения конфиденциальности и целостности информации в системе (используемые СКЗИ, протоколы) и другая информация в соответствии с ЕОМУ.

4.6. Выполнение требований по безопасности информации

Указываются реквизиты документов, подтверждающих выполнение требований по безопасности информации на стороне банка и на стороне Госкорпорации «Росатом» или организации Госкорпорации «Росатом», планирующими заключить или заключившими договор с банком на услугу по дистанционному банковскому обслуживанию.

5. Оценка соответствия

5.1. Результаты исследования доверия к ключевой системе

Критерии оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия

5.2. Результаты исследования доверия к СКЗИ, входящим в состав системы

Критерии оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия

5.3. Результаты исследования доверия к среде функционирования СКЗИ

Критерии оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия

5.4. Результаты исследования доверия к системе, как к ОКИИ

Критерии оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия

5.5. Результаты исследования доверия к участникам процессов обработки данных

Критерии оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия

6. Выводы и рекомендации

6.1. Выводы

На момент составления настоящего заключения уровень доверия к системе <указывается выявленный уровень доверия>.

6.2. Рекомендации

Для приведения Системы к среднему уровню доверия орган криптографической защиты <указывается наименование лицензиата ФСБ России> рекомендует <указывается Госкорпорация «Росатом» или организация Госкорпорации «Росатом», планирующие заключить или заключившие договор с банком на услугу по дистанционному банковскому обслуживанию> провести следующие работы в краткосрочной перспективе:

<указывается перечень мероприятий по приведению Системы к среднему уровню доверия>.

Для приведения Системы к высокому уровню доверия орган криптографической защиты <указывается наименование лицензиата ФСБ России> рекомендует <указывается Госкорпорация «Росатом» или организация Госкорпорации «Росатом», планирующие заключить или заключившие договор с банком на услугу по дистанционному банковскому обслуживанию> провести следующие работы в среднесрочной перспективе:

<указывается перечень мероприятий по приведению Системы к высокому уровню доверия>.

Для приведения системы к среднему уровню доверия орган криптографической защиты <указывается наименование лицензиата ФСБ России> рекомендует <указывается наименование банка> провести следующие работы в краткосрочной перспективе:

<указывается перечень мероприятий по приведению Системы к среднему уровню доверия>.

Для приведения Системы к высокому уровню доверия орган криптографической защиты <указывается наименование лицензиата ФСБ России> рекомендует <указывается наименование банка> провести следующие работы в среднесрочной перспективе:

<указывается перечень мероприятий по приведению Системы к высокому уровню доверия>.

Заключение составил:

<указывается должность> _____/_____
(подпись) (Ф.И.О)