|  |  |
| --- | --- |
| Рег. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_  от \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

|  |  |
| --- | --- |
|  | **УТВЕРЖДАЮ**  Руководитель  органа криптографической защиты  АО «Гринатом»  **\_\_\_\_\_\_\_\_\_\_\_\_/**Н.И. Беленький  (подпись) (Ф.И.О)  «\_\_\_»**\_\_\_\_\_\_\_\_\_\_** 20\_\_ г. |

**ЗАКЛЮЧЕНИЕ**

**по результатам оценки уровня доверия**

**к «SYSTEM\_NAME»**

**в «CLIENT\_NAME»**

г. Москва

YEAR г.

1. Термины, определения и сокращения

|  |  |
| --- | --- |
| **Термин** | **Определение** |
| Ключевая информация | Специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока |
| Ключевой документ | Физический носитель определенной структуры, содержащий ключевую информацию |
| Орган криптографической защиты | Действующая на постоянной основе рабочая группа из числа сотрудников лицензиата ФСБ России |
| Регламент ОКЗ | 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», являющийся неотъемлемой частью договора присоединения от 06 июля 2012 г. №22/2143-Д на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств |
| 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 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 |
| 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** |
| АРМ | Автоматизированное рабочее место |
| Банк | «BANK\_NAME» |
| ДБО | Дистанционное банковское обслуживание |
| ЕОМУ | Единые отраслевые методические указания по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утвержденные Приказом от 22.10.2015 №1/1009-П |
| Журнал поэкземплярного учета СКЗИ | Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации) |
| Клиент | «CLIENT\_NAME» |
| ОКЗ АО «Гринатом» | Орган криптографической защиты АО «Гринатом» |
| Пользователь Клиента/Банка | Пользователь Системы на стороне Клиента/Банка, пользователь СКЗИ на стороне Клиента/Банка |
| СЗИ от НСД | Средство защиты информации от несанкционированного доступа |
| Система | «SYSTEM\_NAME» |
| СКЗИ | Средство криптографической защиты информации |
| УЦ | Удостоверяющий центр «BANK\_NAME» |

1. ВВОДНАЯ ЧАСТЬ

## Основание для выдачи заключения

Основанием для выдачи настоящего заключения являются **{{Вставка- 1}}**.

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

## «SYSTEM\_NAME»

## 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.

1. 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 «CLIENT\_BANK\_ORDER\_NAME» (Документ об использовании Системы) [1].

1. В ПРОЦЕССЕ ИССЛЕДОВАНИЯ УСТАНОВЛЕНО

## Описание Системы

Система является информационной системой лицензиата ФСБ России «BANK\_NAME» (лицензия ФСБ России «BANK\_FSB\_LICENSE\_NUM» (46,1) от «BANK\_FSB\_LICENSE\_DATE» (46,1) на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания 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) [2], защищенной с использованием СКЗИ. Работа в Системе осуществляется с использованием **{{Вставка- 2}}.**

**{{Вставка- 3}}**.

## Инфраструктура ключевой системы

УЦ осуществляет функции по созданию и выдаче сертификатов ключей проверки электронной подписи в соответствии с лицензией ФСБ России [2]. **{{Вставка- 4}}**.

Изготовление сертификатов ключей проверки электронной подписи осуществляется с использованием средств УЦ:

«BANK\_PAC\_UC\_NAME»;

«BANK\_PAC\_UC\_SKZI\_NAME».

**{{Вставка- 5}}**.

Совместно со средствами УЦ функционируют:

антивирусное средство - «BANK\_PAC\_UC\_AV\_NAME» (В таблице АНТИВИРУСОВ предусмотреть строку «информация не предоставлена» и «антивирус отсутствует»);

СЗИ от НСД - «BANK\_PAC\_UC\_SZI\_NAME» (В таблице СЗИ НСД предусмотреть строку «информация не предоставлена» и «СЗИ отсутствует, «в связи с отсутствием сертифицированного ФСБ России и ФСТЭК России решения для виртуальных серверов на аппаратных блейд-устройствах, данный параметр не оценивается»).

## Жизненный цикл ключевых документов

### 4.3.1 Получение, создание и замена ключевых документов

В качестве ключевых носителей ключей электронной подписи на стороне Клиента используются «CLIENT\_KC\_NAME».

Администратор безопасности (сотрудник, назначенный документом «CLIENT\_ADMIN\_DOC\_NAME») от «CLIENT\_ADMIN\_DOC\_DATE» №«CLIENT\_ADMIN\_DOC\_NUM» получает ключевые документы с первичной ключевой информацией Пользователей Клиента лично в Банке, имея доверенность на получение ключевых документов Пользователей Клиента (п. 3.6.4 Регламента ОКЗ), или от самих Пользователей Клиента, которые ранее получили эти ключевые документы в Банке. После получения ключевых документов администратор безопасности учитывает их в Журнале поэкземплярного учета СКЗИ и передает Пользователям Клиента под расписку (п. 3.6.5 Регламента ОКЗ). После этого администратор безопасности в присутствии Пользователей Клиента и на их АРМ создает (производит генерацию) рабочие ключи электронной подписи Пользователей Клиента с использованием ключевых документов с первичной ключевой информацией, учитывает ключевые документы с рабочими ключами электронной подписи в Журнале поэкземплярного учета СКЗИ и передает их Пользователям Клиента под расписку (п. 3.6.7 Регламента ОКЗ). Пользователи Клиента отслеживают сроки действия своих сертификатов ключей проверки электронной подписи (срок действия - «Регл\_УЦ\_Срок\_действ\_серт\_кл\_пров\_ЭП» (новая сучьность) месяцев), при этом администратор безопасности отслеживает сроки действия сертификатов ключей проверки электронной подписи всех Пользователей Клиента и в случае необходимости производит замену ключей электронной подписи.

**{{Вставка- 6}}**.

### 4.3.2 Хранение ключевых документов

Хранение ключевых документов Пользователей Клиента осуществляется в личных опечатываемых личными печатями пеналах, хранящихся в запираемых ящиках столов или в личных металлических сейфах, закрывающихся на механический замок и опечатываемых личными печатями, или в металлических сейфах, имеющих кодовый замок, что «Акт\_гот\_Клиент\_Наим» (новая сучьность).

**{{Вставка- 7}}**.

### 4.3.3 Уничтожение ключевых документов

Уничтожение ключевых документов Пользователей Клиента производится администратором безопасности с проставлением соответствующих отметок в Журнале поэкземплярного учета СКЗИ (п.3.6.12 Регламента ОКЗ).

**{{Вставка- 8}}**.

## Жизненный цикл СКЗИ

### 4.4.1 Получение СКЗИ

Для работы в Системе «Кто\_передал\_СКЗИ\_для\_использования\_в\_Сис» (новая сущность) передает «СКЗИ\_целост\_Клиента\_Наим\_СКЗИ» (новая херня) и эксплуатационную и техническую документацию к нему.

**{{Вставка- 9}}**

Администратор безопасности получает СКЗИ и эксплуатационную и техническую документацию к нему (п.3.6.4 Регламента ОКЗ) и учитывает их в Журнале поэкземплярного учета СКЗИ (п.3.6.5 Регламента ОКЗ). Согласно схемы организации криптографической защиты информации ОКЗ АО «Гринатом» полученное СКЗИ и эксплуатационная и техническая документация к нему учтены в **{{Вставка- 10}}.**

### Проверка готовности, установка и эксплуатация СКЗИ

Администратор безопасности проверил АРМ Пользователей Клиента № «Номера\_АРМ\_Клиента» для работы с Системой на соответствие требованиям эксплуатационной и технической документации к «СКЗИ\_целост\_Клиента\_Наим\_СКЗИ», инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 №152, отраслевым требованиям по информационной безопасности от 09.01.2019 №1/4-П-дсп, **{{Вставка- 11}}**, произвел установку СКЗИ на АРМ Пользователей Клиента и передал установленные СКЗИ Пользователям Клиента под расписку **{{Вставка- 12}}**,

На АРМ Пользователей Клиента в качестве антивирусного средства используется «CLIENT\_ARM\_AV\_NAME\_AND\_VERSION» и в качестве СЗИ от НСД используется «CLIENT\_ARM\_SZI\_NAME\_AND\_VERSION».

Пользователи Клиента прошли обучение правилам работы с СКЗИ, сдали зачеты по программе обучения, **{{Вставка- 13}}**, и допущены к работе с СКЗИ, **{{Вставка- 14}}** (п. 3.6.8 Регламента ОКЗ).

**{{Вставка- 15}}**,

Периодический контроль администраторами безопасности условий использования СКЗИ на стороне Клиента проводится в соответствии с Регламентом ОКЗ (п. 3.6.10).

**{{Вставка- 16}}**,

**{{Вставка- 17}}**,

**{{Вставка- 18}}**,

**{{Вставка- 19}}**,

**{{Вставка- 20}}**,

**{{Вставка- 21}}**,

**{{Вставка- 22}}**,

**{{Вставка- 23}}**,

### Уничтожение СКЗИ

Уничтожение СКЗИ на АРМ Пользователей Клиента производится администратором безопасности с проставлением соответствующих отметок в Журнале поэкземплярного учета СКЗИ (п.3.6.12 Регламента ОКЗ).

**{{Вставка- 24}}**,

## 4.5 Механизм обеспечения конфиденциальности и целостности информации в Системе

Для обеспечения конфиденциальности информации при передаче через сеть интернет применяется **{{Вставка- 25}}**.

Для обеспечения целостности информации в Системе используется **{{Вставка- 26}}**, при этом дополнительные службы проверки статуса сертификата (online certificate status protocol) и штампов времени (time-stamp protocol) **{{Вставка- 27}}**.

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

**{{Вставка- 28}}**.

**{{Вставка- 29}}.**

**{{Вставка- 30}}.**

**{{Вставка- 31}}.**

**{{Вставка- 32}}.**

**{{Вставка- 33}}.**

**{{Вставка- 34}}.**

## Анализ документа ««CLIENT\_BANK\_ORDER\_NAME» (Документ об использовании Системы)»

В документе «CLIENT\_BANK\_ORDER\_NAME» (Документ об использовании Системы)» не предусмотрена ответственность Банка перед Клиентом в сумме реально доказанного ущерба, который может быть нанесен в результате:

* несанкционированного доступа к сведениям Клиента на серверной части Системы;
* неправомерных действий злоумышленника по причине слабой аутентификации пользователей Системы;
* использования ключей электронной подписи неуполномоченным лицом Банка в результате нарушения конфиденциальности ключа;
* нарушения конфиденциальности и целостности передаваемой информации;
* отказа в обслуживании Пользователей Клиента по вине Банка;
* непризнания юридической силы электронных документов в Системе вследствие отсутствия обязательных реквизитов.

1. 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 | «Лиц\_ФСБ\_России\_Налич» | «Лиц\_ФСБ\_России\_Срок\_нач\_действ» | «Лиц\_ФСБ\_России\_Срок\_оконч\_действ» | «Лиц\_ФСБ\_России\_Реквизиты» | «Лиц\_ФСБ\_России\_Ур\_дов» |
| 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.) | «Право\_на\_исп\_ПАК\_УЦ\_и\_СКЗИ\_Наличие» | «Право\_на\_исп\_ПАК\_УЦ\_и\_СКЗИ\_Дата\_нач\_дейс» | «Право\_на\_исп\_ПАК\_УЦ\_и\_СКЗИ\_Дата\_оконч\_де» | «Право\_на\_исп\_ПАК\_УЦ\_и\_СКЗИ\_Ном\_док» | «Право\_на\_исп\_ПАК\_УЦ\_и\_СКЗИ\_Ур\_дов» |
| 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 | «Серт\_ПАК\_УЦ\_Наличие» | «Серт\_ПАК\_УЦ\_Дата\_нач\_действ» | «Серт\_ПАК\_УЦ\_Дата\_оконч\_действ» | «Серт\_ПАК\_УЦ\_Ном» | «Серт\_ПАК\_УЦ\_Ур\_дов» |
| 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» | «Серт\_ПАК\_УЦ\_Наличие» | «Серт\_ПАК\_УЦ\_Дата\_нач\_действ» | «Серт\_ПАК\_УЦ\_Дата\_оконч\_действ» | «Серт\_ПАК\_УЦ\_Ном» | «Серт\_ПАК\_УЦ\_Ур\_дов» |
| Действующий сертификат соответствия ФСБ России на СКЗИ, применяемое для работы средства, реализующего инфраструктуру ключевой системы с классом защиты не ниже КС2 | «Серт\_СКЗИ\_УЦ\_Налич» | «Серт\_СКЗИ\_УЦ\_Дата\_нач\_действ» | «Серт\_СКЗИ\_УЦ\_Дата\_оконч\_действ» | «Серт\_СКЗИ\_УЦ\_Ном» | «Серт\_СКЗИ\_УЦ\_Ур\_дов» |
| Использование Клиентом сертифицированных ФСТЭК России/ФСБ России или несертифицированных (типа токен/смарт-карты или flash-носитель/жесткий диск ПЭВМ) ключевых носителей | «Ключ\_нос\_Кл\_Налич\_серт» | «Ключ\_нос\_Кл\_Дата\_нач\_действ» | «Ключ\_нос\_Кл\_Дата\_оконч\_действ» | «Ключ\_нос\_Кл\_Ном\_серт» | «Ключ\_нос\_Кл\_Ур\_дов» |
| Использование Банком сертифицированных ФСТЭК России/ФСБ России или несертифицированных (типа токен/смарт-карты или flash-носитель/жесткий диск ПЭВМ) ключевых носителей | «Ключ\_нос\_Банка\_Налич» | «Ключ\_нос\_Банка\_Дата\_нач\_действ\_серт» | «Ключ\_нос\_Банка\_Дата\_оконч\_действ\_серт» | «Ключ\_нос\_Банка\_Ном\_серт» | «Ключ\_нос\_Банка\_Ур\_дов» |
| Документы, регламентирующие жизненный цикл ключевой системы | «Регл\_УЦ\_Наличие» | «Регл\_УЦ\_Дата\_нач\_действ» | «Регл\_УЦ\_Дата\_оконч\_действ» | «Регл\_УЦ\_Номер» | «Регл\_УЦ\_Ур\_дов» |
| Свидетельство об аккредитации УЦ в Минкомсвязи России | «Аккредитация\_Налич» | «Аккредитация\_Дата\_нач\_действ» | «Аккредитация\_Дата\_оконч\_действ» | «Аккредитация\_Ном» | «Аккредитация\_Ур\_дов» |
| В Системе для подписи используется усиленная квалифицированная/ усиленная неквалифицированная электронная подпись | «Тип\_\_ЭП\_Тип\_ЭП» | «Тип\_\_ЭП\_Дата\_нач\_действ» | «Тип\_\_ЭП\_Дата\_оконч\_действ» | «Тип\_\_ЭП\_Ном\_док» | «Тип\_\_ЭП\_Ур\_дов» |
| Документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации) | «Стандарт\_БР\_Наличие» | «Стандарт\_БР\_Дата\_нач\_действ» | «Стандарт\_БР\_Дата\_оконч\_действ» | «Стандарт\_БР\_Номер» | «Стандарт\_БР\_Ур\_дов» |
| 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 | «Формат\_усоверш\_ЭП\_Наличие» | «Формат\_усоверш\_ЭП\_Дата\_нач\_действ» | «Формат\_усоверш\_ЭП\_Дата\_оконч\_действ» | «Формат\_усоверш\_ЭП\_Номер» | «Формат\_усоверш\_ЭП\_Ур\_дов» |

## 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 | «СКЗИ\_конфиденц\_Клиента\_Наличие» | «СКЗИ\_конфиденц\_Клиента\_Дата\_нач\_действ\_с» | «СКЗИ\_конфиденц\_Клиента\_Дата\_оконч\_действ» | «СКЗИ\_конфиденц\_Клиента\_Ном\_серт» | «СКЗИ\_конфиденц\_Клиента\_Ур\_дов» |
| Использование сертифицированных ФСБ России СКЗИ на АРМ Пользователей Клиента для обеспечения целостности информации | «СКЗИ\_целост\_Клиента\_Наличие» | «СКЗИ\_целост\_Клиента\_Дата\_нач\_действ\_серт» | «СКЗИ\_целост\_Клиента\_Дата\_оконч\_действ\_се» | «СКЗИ\_целост\_Клиента\_Ном\_серт» | «СКЗИ\_целост\_Клиента\_Ур\_дов» |
| Использование сертифицированных ФСБ России СКЗИ на АРМ Пользователей Банка для обеспечения целостности информации | «СКЗИ\_конфиденц\_Банка\_Наличие» | «СКЗИ\_конфиденц\_Банка\_Дата\_нач\_действ\_сер» | «СКЗИ\_конфиденц\_Банка\_Дата\_оконч\_действ\_с» | «СКЗИ\_конфиденц\_Банка\_Ном\_серт» | «СКЗИ\_конфиденц\_Банка\_Ур\_дов» |
| Документы, подтверждающие право передачи Банком Клиенту СКЗИ и эксплуатационной и технической документации к ним, использующихся в работе Системы (договор, лицензия и пр.) | «Подтв\_права\_перед\_СКЗИ\_Наличие» | «Подтв\_права\_перед\_СКЗИ\_Клиенту\_Дата\_нач\_» | «Подтв\_права\_перед\_СКЗИ\_Клиенту\_Дата\_окон» | «Подтв\_права\_перед\_СКЗИ\_Клиенту\_Ном\_док» | «Подтв\_права\_перед\_СКЗИ\_Клиенту\_Ур\_дов» |
| Класс защиты применяющихся на рабочих местах пользователей Клиента Системы шифровальных (криптографических) средств | «КС1КС2\_Клиента» | «СКЗИ\_целост\_Клиента\_Дата\_нач\_действ\_серт» | «СКЗИ\_целост\_Клиента\_Дата\_оконч\_действ\_се» | «СКЗИ\_целост\_Клиента\_Ном\_серт» | «КС1КС2\_Клиента\_Ур\_дов» |
| Класс защиты применяющихся на рабочих местах пользователей Банка Системы шифровальных (криптографических) средств | «КС1КС2\_Банка» | «СКЗИ\_конфиденц\_Банка\_Дата\_нач\_действ\_сер» | «СКЗИ\_конфиденц\_Банка\_Дата\_оконч\_действ\_с» | «СКЗИ\_конфиденц\_Банка\_Ном\_серт» | «КС1КС2\_Банка\_Ур\_дов» |

## 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 | «Лиц\_на\_ПО\_Системы\_Наличие» | «Лиц\_на\_ПО\_Системы\_Дата\_нач\_действ» | «Лиц\_на\_ПО\_Системы\_Дата\_оконч\_действ» | «Лиц\_на\_ПО\_Системы\_Ном\_док» | «Лиц\_на\_ПО\_Системы\_Ур\_дов» |
| Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Клиента | «Заключ\_ОКЗ\_о\_возм\_экспл\_СКЗИ\_Клиент\_Нали» | «Заключ\_ОКЗ\_о\_возм\_экспл\_СКЗИ\_Клиент\_Дата» | «Заключ\_ОКЗ\_о\_возм\_экспл\_СКЗИ\_Клиент\_Дат1» | «Заключ\_ОКЗ\_о\_возм\_экспл\_СКЗИ\_Клиент\_Ном\_» | «Заключ\_ОКЗ\_о\_возм\_экспл\_СКЗИ\_Клиент\_Ур\_д» |
| Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Банка | «Заключ\_ОКЗ\_о\_возм\_экспл\_СКЗИ\_Банк\_Наличи» | «Заключ\_ОКЗ\_о\_возм\_экспл\_СКЗИ\_Банк\_Дата\_н» | «Заключ\_ОКЗ\_о\_возм\_экспл\_СКЗИ\_Банк\_Дата\_о» | «Заключ\_ОКЗ\_о\_возм\_экспл\_СКЗИ\_Банк\_Ном\_до» | «Заключ\_ОКЗ\_о\_возм\_экспл\_СКЗИ\_Банк\_Ур\_дов» |
| Заключение о корректности встраивания СКЗИ в Систему | «Кор\_встраив\_СКЗИ\_в\_Систему\_Наличие» | «Кор\_встраив\_СКЗИ\_в\_Систему\_Дата\_нач\_дейс» | «Кор\_встраив\_СКЗИ\_в\_Систему\_Дата\_оконч\_де» | «Кор\_встраив\_СКЗИ\_в\_Систему\_Ном\_док» | «Кор\_встраив\_СКЗИ\_в\_Систему\_Ур\_дов» |
| Документация на систему дистанционного банковского обслуживания (техническое описание или техническая записка, инструкция пользователя, инструкция администратора безопасности) | «Докум\_на\_Систему\_Наличие» | «Докум\_на\_Систему\_Дата\_нач\_действ» | «Докум\_на\_Систему\_Дата\_оконч\_действ» | «Докум\_на\_Систему\_Ном\_док» | «Докум\_на\_Систему\_Ур\_дов» |
| Аттестат соответствия ФСТЭК на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация на стороне Клиента | «Аттестат\_на\_Систему\_Клиент\_Наличие» | «Аттестат\_на\_Систему\_Клиент\_Дата\_нач\_дейс» | «Аттестат\_на\_Систему\_Клиент\_Дата\_оконч\_де» | «Аттестат\_на\_Систему\_Клиент\_Ном» | «Аттестат\_на\_Систему\_Клиент\_Ур\_дов» |
| Аттестат соответствия ФСТЭК России на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация на стороне Банка | «Аттестат\_на\_Систему\_Банк\_Наличие» | «Аттестат\_на\_Систему\_Банк\_Дата\_нач\_действ» | «Аттестат\_на\_Систему\_Банк\_Дата\_оконч\_дейс» | «Аттестат\_на\_Систему\_Банк\_Ном\_док» | «Аттестат\_на\_Систему\_Банк\_Ур\_дов» |
| Установлено сертифицированное антивирусное ПО на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы | «Антивир\_ПО\_на\_УЦ\_Банка\_Наличие» | «Антивир\_ПО\_на\_УЦ\_Банка\_Дата\_нач\_действ\_с» | «Антивир\_ПО\_на\_УЦ\_Банка\_Дата\_оконч\_действ» | «Антивир\_ПО\_на\_УЦ\_Банка\_Номер\_серт» | «Антивир\_ПО\_на\_УЦ\_Банка\_Ур\_дов» |
| Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Клиента | «Антивир\_ПО\_на\_АРМ\_Клиента\_Налич» | «Антивир\_ПО\_на\_АРМ\_Клиента\_Дата\_нач\_дейст» | «Антивир\_ПО\_на\_АРМ\_Клиента\_Дата\_оконч\_дей» | «Антивир\_ПО\_на\_АРМ\_Клиента\_Ном\_серт» | «Антивир\_ПО\_на\_АРМ\_Клиента\_Ур\_дов» |
| Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Банка | «Антивир\_ПО\_на\_АРМ\_Банка\_Налич» | «Антивир\_ПО\_на\_АРМ\_Банка\_Дата\_нач\_действ\_» | «Антивир\_ПО\_на\_АРМ\_Банка\_Дата\_оконч\_дейст» | «Антивир\_ПО\_на\_АРМ\_Банка\_Ном\_серт» | «Антивир\_ПО\_на\_АРМ\_Банка\_Ур\_дов» |
| Установлено сертифицированное СЗИ от НСД на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы | «СЗИ\_от\_НСД\_на\_УЦ\_Банка\_Налич» | «СЗИ\_от\_НСД\_на\_УЦ\_Банка\_Дата\_нач\_действ\_с» | «СЗИ\_от\_НСД\_на\_УЦ\_Банка\_Дата\_оконч\_действ» | «СЗИ\_от\_НСД\_на\_УЦ\_Банка\_Ном\_серт\_соотв» | «СЗИ\_от\_НСД\_на\_УЦ\_Банка\_Ур\_дов» |
| Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Клиента | «СЗИ\_от\_НСД\_на\_АРМ\_Клиента\_Наличие» | «СЗИ\_от\_НСД\_на\_АРМ\_Клиента\_Дата\_нач\_дейст» | «СЗИ\_от\_НСД\_на\_АРМ\_Клиента\_Дата\_оконч\_дей» | «СЗИ\_от\_НСД\_на\_АРМ\_Клиента\_Ном\_серт» | «СЗИ\_от\_НСД\_на\_АРМ\_Клиента\_Ур\_дов» |
| Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Банка | «СЗИ\_от\_НСД\_на\_АРМ\_Банка\_Налич» | «СЗИ\_от\_НСД\_на\_АРМ\_Банка\_Дата\_нач\_действ\_» | «СЗИ\_от\_НСД\_на\_АРМ\_Банка\_Дата\_оконч\_дейст» | «СЗИ\_от\_НСД\_на\_АРМ\_Банка\_Ном\_серт» | «СЗИ\_от\_НСД\_на\_АРМ\_Банка\_Ур\_дов» |

## 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 | «Допуск\_польз\_Клиента\_Наличие» | «Допуск\_польз\_Клиента\_Дата\_нач» | «Допуск\_польз\_Клиента\_Срок\_оконч» | «Допуск\_польз\_Клиента\_Ном\_док» | «Допуск\_польз\_Клиента\_Уровень\_доверия» |
| Документ, подтверждающий допуск пользователей Банка к работе с СКЗИ в Системе | «Допуск\_польз\_Банка\_Наличие» | «Допуск\_польз\_Банка\_Дата\_нач» | «Допуск\_польз\_Банка\_Срок\_оконч» | «Допуск\_польз\_Банка\_Ном\_док» | «Допуск\_польз\_Банка\_Уровень\_доверия» |
| Документ, подтверждающий прохождение обучения пользователями Системы на стороне Клиента | «Обуч\_польз\_СКЗИ\_Клиент\_Налич» | «Обуч\_польз\_СКЗИ\_Клиент\_Дата\_нач» | «Обуч\_польз\_СКЗИ\_Клиент\_Дата\_оконч» | «Обуч\_польз\_СКЗИ\_Клиент\_Ном\_док» | «Обуч\_польз\_СКЗИ\_Клиент\_Ур\_дов» |
| Документ, подтверждающий прохождение обучения пользователями Системы на стороне Банка | «Обуч\_польз\_СКЗИ\_Банк\_Наличие» | «Обуч\_польз\_СКЗИ\_Банк\_Дата\_нач» | «Обуч\_польз\_СКЗИ\_Банк\_Срок\_оконч» | «Обуч\_польз\_СКЗИ\_Банк\_Ном\_док» | «Обуч\_польз\_СКЗИ\_Банк\_Ур\_дов» |
| Локальные нормативные акты, определяющие права и роли работников Клиента в Системе (подписантов, администраторов безопасности) | «Права\_и\_роли\_раб\_Клиента\_Налич» | «Права\_и\_роли\_раб\_Клиента\_Дата\_нач» | «Права\_и\_роли\_раб\_Клиента\_Дата\_оконч» | «Права\_и\_роли\_раб\_Клиента\_Ном\_док» | «Права\_и\_роли\_раб\_Клиента\_Ур\_дов» |
| Локальные нормативные акты, определяющие права и роли работников Банка в Системе (подписантов, администраторов безопасности) | «Права\_и\_роли\_раб\_Банка\_Наличие» | «Права\_и\_роли\_раб\_Банка\_Дата\_нач» | «Права\_и\_роли\_раб\_Банка\_Срок\_оконч» | «Права\_и\_роли\_раб\_Банка\_Ном\_док» | «Права\_и\_роли\_раб\_Банка\_Ур\_дов» |
| Контроль администраторами безопасности условий использования СКЗИ на стороне Клиента | «Контр\_АБ\_усл\_исп\_СКЗИ\_Клиент\_Налич» | «Контр\_АБ\_усл\_исп\_СКЗИ\_Клиент\_Дата\_нач\_д» | «Контр\_АБ\_усл\_исп\_СКЗИ\_Клиент\_Срок\_оконч\_» | «Контр\_АБ\_усл\_исп\_СКЗИ\_Клиент\_Ном\_док» | «Контр\_АБ\_усл\_исп\_СКЗИ\_Клиент\_Ур\_дов» |
| Контроль администраторами безопасности условий использования СКЗИ на  стороне Банка | «Контр\_АБ\_усл\_исп\_СКЗИ\_Банк\_Налич» | «Контр\_АБ\_усл\_исп\_СКЗИ\_Банк\_Дата\_нач» | «Контр\_АБ\_усл\_исп\_СКЗИ\_Банк\_Срок\_оконч» | «Контр\_АБ\_усл\_исп\_СКЗИ\_Банк\_Ном\_док» | «Контр\_АБ\_усл\_исп\_СКЗИ\_Банк\_Ур\_дов» |

1. ВЫВОДЫ И РЕКОМЕНДАЦИИ

## 6.1 Выводы

На момент составления настоящего заключения уровень доверия к Системе «Уровень\_доверия»[[1]](#footnote-1). Согласно ЕОМУ в организациях Госкорпорации «Росатом» допустима эксплуатация Систем с уровнем доверия не ниже среднего.

## 6.2 Рекомендации

Для приведения Системы к среднему уровню доверия ОКЗ АО «Гринатом» рекомендует Клиенту провести следующие работы:

Для приведения Системы к высокому уровню доверия ОКЗ АО «Гринатом» рекомендует Клиенту провести следующие работы:

Для повышения класса защиты применяемых на рабочих местах Пользователей Клиента шифровальных (криптографических) средств до КС2 установить на рабочие места Пользователей Клиента СЗИ от НСД согласно эксплуатационной и технической документации к СКЗИ.

Для приведения Системы к высокому уровню доверия ОКЗ АО «Гринатом» рекомендует Банку провести следующие работы[[2]](#footnote-2):

Использовать в Системе усиленную квалифицированную электронную подпись усовершенствованного формата.

ОКЗ АО «Гринатом» рекомендует в документе «CLIENT\_BANK\_ORDER\_NAME» (Документ об использовании Системы)» определить ответственность Банка перед Клиентом в сумме реально доказанного ущерба, который может быть нанесен в результате:

* несанкционированного доступа к сведениям Клиента на серверной части Системы;
* неправомерных действий злоумышленника по причине слабой аутентификации пользователей Системы;
* использования ключей электронной подписи неуполномоченным лицом Банка в результате нарушения конфиденциальности ключа;
* нарушения конфиденциальности и целостности передаваемой информации;
* отказа в обслуживании Пользователей Клиента по вине Банка;
* непризнания юридической силы электронных документов в Системе вследствие отсутствия обязательных реквизитов.

1. НОРМАТИВНАЯ И СПРАВОЧНАЯ ДОКУМЕНТАЦИЯ
   1. (Приложение №1);
   2. (Приложение №2);

Заключение составил:

|  |  |
| --- | --- |
| Старший специалист группы аудита отдела криптографической защиты АО «Гринатом» | \_\_\_\_\_\_\_\_\_\_\_\_**/**В.А. Силкин  (подпись) (Ф.И.О) |
| Руководитель группы аудита отдела криптографической защиты АО «Гринатом» | \_\_\_\_\_\_\_\_\_\_\_\_**/**Я.А. Бинкис  (подпись) (Ф.И.О) |

Силкин Виктор Александрович

(499) 949-49-19 доб. 5420

1. Срок действия Заключения – 1 год при сохранении уровня доверия к Системе. [↑](#footnote-ref-1)
2. Рекомендации по приведению в соответствие Системы с требованиями ЕОМУ на стороне Банка указаны для информации. Работы по приведению Системы в соответствие с требованиями ЕОМУ на стороне Банка проводятся в рамках договора АО «Гринатом» с Госкорпорацией «Росатом». [↑](#footnote-ref-2)