|  |  |
| --- | --- |
| Рег. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_  от \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Для служебного пользования |

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

**ЗАКЛЮЧЕНИЕ**

**по результатам оценки уровня доверия к**

**«SYSTEM\_NAME»**

**«BANK\_NAME»**

г. Москва

YEAR г

1. ВВОДНАЯ ЧАСТЬ

## Основание для выдачи заключения

Договор между АО «Гринатом» и «CLIENT\_NAME» от GA\_CLIENT\_DOGOVOR\_DATE № GA\_CLIENT\_DOGOVOR\_NUM «GA\_CLIENT\_DOGOVOR\_NAME».

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

«SYSTEM\_NAME» «BANK\_NAME»

(далее – Система).

## Вопросы для исследования

* Обеспечение доверия к технологии, реализующей инфраструктуру ключевой системы;
* Обеспечение доверия к средствам криптографической защиты, 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 Едиными отраслевыми методическими указаниями по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утвержденных Приказом от 22.10.2015 №1/1009-П (далее – ЕОМУ).

## Методы исследования

* Анализ представленной в Орган криптографической защиты АО «Гринатом» (далее – ОКЗ АО «Гринатом») документации на Систему;
* Анализ «ДОГОВОРА» [1].

1. В ПРОЦЕССЕ ИССЛЕДОВАНИЯ УСТАНОВЛЕНО

По результатам выполнения работ по оценке уровня доверия к Системе было выдано от REPORT\_DATE № REPOT\_NUM «Заключение по результатам оценки уровня доверия к автоматизированной системе «SYSTEM\_NAME» «BANK\_NAME».

Письмом от \_\_.\_\_.\_\_\_\_ №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ «О результатах оценки уровня доверия к автоматизированной системе «SYSTEM\_NAME» «BANK\_NAME» «CLIENT\_NAME» [2] направило рекомендации по приведению Системы к высокому уровню доверия.

Письмом от \_\_.\_\_.\_\_\_\_ №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [3] и по электронной почте «BANK\_NAME» предоставил информацию о Системе.

## Описание Системы



Система является автоматизированной системой лицензиата ФСБ России АО ««BANK\_NAME» [4], защищенной с использованием сертифицированных ФСБ России средств криптографической защиты информации (далее – СКЗИ) с клиент-серверной архитектурой, реализованной с использованием программного обеспечения «CORrect REliable Qualitative Technology Solution" (CORREQTS) фирмы разработчика лицензиата ФСБ России ООО «БCC» [5].

Пользователи Системы АО «Атомэнергопром» посредством браузера, производят подключение к серверу Банка по адресу <https://online.abr.ru>. После авторизации в Системе с помощью учетных данных, выданных АО ««BANK\_NAME», выполняют просмотр, подписание и печать документов.

Для шифрования данных при передачи между сервером АО ««BANK\_NAME» и АРМ пользователей применяется протокол TLS 1.2, сертификат выдан компанией GlobalSign. Все TCP-соединения инициируются с АРМ пользователей.

Подписание электронных документов для отправки в Банк происходит в браузере с использованием плагина BSSPluginSetup.

## Классификация информации в Системе

Заключения ПДТК о наличии или отсутствии в Системе конфиденциальной информации не составлялись.

## Инфраструктура ключевой системы

В Системе используется «ES\_TYPE» (п.3.7.1. [3]).

Проверка электронной подписи на стороне «BANK\_NAME» реализована с помощью «НАИМЕНОВАНИЕ СРЕДСТВА, РЕАЛИЗУЮЩЕГО ИНФРАСТРУКТУРУ КЛЮЧЕВОЙ СИСТЕМЫ», переданного «CLIENT\_NAME, ПЕРЕДАВШЕЙ СРЕДСТВО РЕАЛИЗУЮЩЕЕ ИНФРАСТРУКТУРУ КЛЮЧЕВОЙ СИСТЕМЫ» на основании «НАИМЕНОВАНИЕ И РЕКВИЗИТЫ ДОГОВОРА НА ИСПОЛЬЗОВАНИЕ СРЕДСТВА, РЕАЛИЗУЮЩЕГО ИНФРАСТРУКТУРУ КЛЮЧЕВОЙ СИСТЕМЫ» (п.1 [3]) и «НАИМЕНОВАНИЕ СКЗИ В СОСТАВЕ СРЕДСТВА, РЕАЛИЗУЮЩЕГО ИНФРАСТРУКТУРУ КЛЮЧЕВОЙ СИСТЕМЫ (вариант исполнения \_\_, сертификат соответствия ФСБ России №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, от \_\_.\_\_.20\_\_, действителен до \_\_.\_\_.20\_\_) [6].

На сервере Системы АО «BANK\_NAME» установлено антивирусное программное изделие «Kaspersky Endpoint Security для Windows» (версия 11.0.0.6499, сертификат соответствия ФСТЭК России от 22.01.2019 №4068, действителен до 22.01.2024) [7].

На АРМ пользователей системы на стороне АО «Атомэнергопром» установлена операционная система Windows, антивирусное программное средство «Dr.Web Enterprise Security Suite» (сертификат соответствия ФСТЭК России от 27.01.2016 №3509, действителен до 27.01.2024) [8] и средство защиты информации Secret Net Studio (сертификат соответствия ФСТЭК России от 16.05.2017 № 3745, действителен до 16.05.2020) [9].

Сертификаты ключей проверки электронной подписи формируются администратором безопасности АО «Атомэнергопром» (сотрудником ОКЗ АО «Гринатом», назначенным приказом [10]) на АРМ пользователей Системы с использованием СКЗИ «Рутокен ЭЦП 2.0» (исполнения 1, 2, сертификат соответствия ФСБ России №СФ/124-3523 от 20.11.2018, действителен до 01.12.2020) [11].

## Жизненный цикл ключей пользователей Системы

#### Создание ключей пользователей Системы

Администратор безопасности АО «Атомэнергопром» на АРМ пользователя Системы в присутствии пользователя Системы и под его контролем, с использованием СКЗИ «Рутокен ЭЦП 2.0» (исполнения 1, 2) [11] формирует рабочие ключи пользователя Системы. В процессе генерации ключа пользователя формируется электронный запрос на регистрацию сгенерированного ключа проверки электронной подписи, который средствами Системы направляется в АО «АБ Россия» (п.5.4.2 [1]).

После завершения генерации ключей проверки электронной подписи пользователь распечатывает из Системы «Бланк ключа проверки электронной подписи» (приложение №7 [1]), подписывает и направляет в АО ««BANK\_NAME».

После формирования рабочих ключей пользователей Системы, администратор безопасности учитывает их в «Журнале поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)» (далее – ЖПУ) и передает под роспись пользователю Системы (п.3.6.5 [12]).

#### Эксплуатация и хранение ключей пользователями Системы

Подписание документов осуществляется на рабочих местах пользователей Системы, с использованием СКЗИ «Рутокен ЭЦП 2.0» (исполнения 1, 2) [11] и рабочих ключей пользователей.

Хранение ключей пользователей Системы на стороне АО «Атомэнергопром» осуществляется в личных опечатываемых личными печатями пеналах, или в личных металлических сейфах, закрывающихся на механический замок и опечатываемых личными печатями, или  в металлических сейфах, имеющих кодовый замок.

#### Замена и уничтожения ключей пользователей Системы

Администратор безопасности следит за сроками действия ключей пользователей Системы и заблаговременно производит формирование новых ключей пользователей Системы (п.3.6.12 [12]).

Уничтожение ключей в АО «Атомэнергопром» производится администратором безопасности (п.3.6.12 [12]) с проставлением соответствующих отметок в ЖПУ.

## Жизненный цикл СКЗИ, использующихся в Системе

### Получение СКЗИ

СКЗИ «Рутокен ЭЦП 2.0» (исполнения 1, 2) [11] для использования в Системе предоставляет АО «АБ Россия» (п. 2 [3]).

Администратор безопасности АО «Атомэнергопром», имеющий доверенность на получение СКЗИ в АО ««BANK\_NAME», получает СКЗИ, эксплуатационную и техническую документацию к  СКЗИ и учитывает их в ЖПУ (п.3.6.5 [12]).

На стороне АО ««BANK\_NAME» ведется поэкземплярный учет СКЗИ и ключей электронной подписи в Журнале учета СКЗИ (п.5.2 «Порядка использования СКЗИ и ключевой информации при работе с системами дистанционного банковского обслуживания «Клиент-Банк» в АО ««BANK\_NAME»).

### Эксплуатация СКЗИ

На стороне АО «Атомэнергопром» СКЗИ эксплуатируют обученные и успешно прошедшие тестирование по результатам обучения пользователи Системы (п.3.6.8 [12]).

Подтверждением выполнения условий использования СКЗИ на стороне АО «Атомэнергопром» является Заключение о возможности эксплуатации СКЗИ, выданное ОКЗ АО «Гринатом».

На стороне АО ««BANK\_NAME» СКЗИ эксплуатируют обученные и успешно прошедшие тестирование по результатам обучения пользователи Системы в соответствии с «Регламентом обучения, повышения и поддержания осведомленности работников АО ««BANK\_NAME» в области информационной безопасности (версия 3.0), утв. Приказом от 16.03.2017 №165-П8 (п.3 [3], [13]) и «Порядком использования СКЗИ и ключевой информации при работе с системами дистанционного банковского обслуживания «Клиент-Банк» в АО ««BANK\_NAME» (версия 1.2), утв. Приказом от 24.07.2018 №592-п (п.3 [3], [14]).

Администратор безопасности АО ««BANK\_NAME» выполняет контроль эксплуатации СКЗИ в соответствии с требованиями, приведенными в эксплуатационной и технической документации на СКЗИ (п.9.2 [14]).

### Уничтожение СКЗИ

Уничтожение СКЗИ и ключевых документов в АО «Атомэнергопром» производится Администратором безопасности (п.3.6.12 [12]) с проставлением соответствующих отметок в ЖПУ.

### Механизм обеспечения конфиденциальности и целостности информации в Системе

Для обеспечения конфиденциальности и целостности информации в процессе эксплуатации Системы на АРМ пользователей АО «Атомэнергопром» используется сертифицированные ФСБ России СКЗИ «Рутокен ЭЦП 2.0» (исполнения 1, 2) [11].

Конфиденциальность информации на этапе передачи ее через сеть Интернет обеспечивается путем применения протокола TLS. Сертификат предоставила компания GlobalSign nv-sa.

## Выполнение требований по безопасности информации на стороне АО ««BANK\_NAME» и на стороне АО «Атомэнергопром»

Выполнение требований по информационной безопасности на стороне АО ««BANK\_NAME» подтверждается информацией о наличии отчета о результатах проведения оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 09 июня 2012г. №382-П.

Выполнение требований по безопасности информации на стороне АО «Атомэнергопром» подтверждается аттестатом соответствия АСЗИ Госкорпорации «Росатом» требованиям безопасности информации № 28/12/2018 – АСЗИ/ГК от 28.12.2018.

## Анализ «Правил АО ««BANK\_NAME» обмена электронными документами с использованием Системы «Клиент-Банк» для корпоративных клиентов договора на эксплуатацию Системы

В Правилах предусмотреть ответственность АО ««BANK\_NAME» перед АО «Атомэнергопром» в сумме реально доказанного ущерба, который может быть нанесен в результате:

* несанкционированного доступа к сведениям АО «Атомэнергопром» на серверной части Системы;
* неправомерных действий злоумышленника по причине слабой аутентификации пользователей Системы;
* использования ключей электронной подписи неуполномоченным лицом АО ««BANK\_NAME» в результате нарушения конфиденциальности ключа;
* нарушения конфиденциальности и целостности передаваемых данных;
* отказа в обслуживании пользователей Системы по вине АО ««BANK\_NAME»;
* непризнания юридической силы электронных документов банка вследствие отсутствия обязательных реквизитов.

4. ОЦЕНКА СООТВЕТСТВИЯ

## 4.1. Результаты исследования технологии, реализующей инфраструктуру ключевой системы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерий оценки | Наличие | Срок действия | Номер | Номер приложения | Уровень доверия |
| Лицензия ФСБ России на соответствующие виды деятельности | + | Бессрочно | ЛСЗ №0000823 Рег.986Н от 04.02.2016 | 4 | В |
| Документ, подтверждающий право использования на средство реализующее инфраструктуру ключевой системы (договор, лицензия и пр.) | Лицензионный договор | Бессрочно | №BSS-ABR/S-Correqts | п.1 прил.3 | В |
| Документ, подтверждающий право использования на СКЗИ, использующееся в составе средства, реализующего инфраструктуру ключевой системы (договор, лицензия и пр.) | Лицензионный договор | Бессрочно | №BSS-ABR/S-Correqts | п.1 прил.3 | В |
| 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 | Проверка электронной подписи, проверка ключа электронной подписи реализована с помощью программного обеспечения CORREQTS |  |  |  |  |
| СКЗИ «Рутокен ЭЦП 2.0» (исполнения 1, 2) | от 20.11.2018 до 01.12.2020 | № СФ/124-3523 | 11 | В |
| Действующий сертификат соответствия ФСБ России на средство криптографической защиты информации, использующееся для работы средства, реализующего инфраструктуру ключевой системы с классом защиты не ниже КС2 | СКЗИ «Крипто-Ком 3.4» (вариант исполнения 43) | от 11.01.2018 до 11.01.2021 | № СФ/124-3271 | 6 | В |
| В Банке используются сертифицированные ФСТЭК России ключевые носители | - | - | - | - | - |
| В Банке используются несертифицированные ФСТЭК России ключевые носители | - | - | - | - | - |
| Клиент использует сертифицированные ФСТЭК России ключевые носители | СКЗИ «Рутокен ЭЦП 2.0» (исполнения 1, 2) | от 20.11.2018 до 01.12.2020 | № СФ/124-3523 | 11 | В |
| Клиент использует несертифицированные ФСТЭК России ключевые носители | - | - | - | - | - |
| Документы, регламентирующие жизненный цикл ключевой системы | Порядок использования СКЗИ и ключевой информации при работе с системами дистанционного банковского обслуживания «Клиент-Банк» в АО ««BANK\_NAME» (версия 1.2) | от 24.07.2018  бессрочно | №592-п - | - | В |
| Свидетельство об аккредитации | - | - | - | - | С |
| В Системе для подписи используется усиленная квалифицированная ЭП | - | - | - | - | - |
| В Системе для подписи используется усиленная неквалифицированная ЭП | + | - | - | - | С |
| Документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации) | Отчет о результатах проведения оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 09 июня 2012г. №382-П. | - | - | - | В |
| Наличие дополнительных служб удостоверяющего центра (службы онлайновой проверки статусов сертификатов и службы штампов времени) | - | - | - | - | С |
| Поддержка формата усовершенствованной подписи | - | - | - | - | С |

## 4.2. Результаты исследований средств криптографической защиты, входящих в состав системы обработки данных.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерий оценки | Наличие | Срок действия | Номер | Номер приложения | Уровень доверия |
| Используются сертифицированные средства криптографической защиты информации на АРМ пользователей Системы на стороне Банка | Информация не предоставлена | - | - | - | Н |
| Для шифрования данных при передачи через сеть интернет применяется протокол TLS 1.2. сертификат предоставила компания GlobalSign nv-sa | - | - | - | Н |
| Используются сертифицированные средства криптографической защиты информации на АРМ пользователей Системы на стороне Клиента | Для подписания используется СКЗИ «Рутокен ЭЦП 2.0» (исполнения 1, 2) | от  20.11.2018 до 01.12.2020 | № СФ/124-3523 | 11 | В |
| Для шифрования данных при передачи через сеть интернет применяется протокол TLS 1.2. сертификат предоставила компания GlobalSign nv-sa | - | - | - | Н |
| Документ, подтверждающий право передачи СКЗИ, использующееся в работе Системы (договор, лицензия и пр.) | Сублицензионный договор | Бессрочно | №BSS-Security/  ABR-2016 | - | В |
| Класс защиты применяющихся на рабочих местах пользователей Системы шифровальных (криптографических) средств не менее КС1 | СКЗИ «Рутокен ЭЦП 2.0» (исполнения 1, 2) | от  20.11.2018 до 01.12.2020 | № СФ/124-3523 | 11 | С |
| Класс защиты применяющихся на рабочих местах пользователей Системы шифровальных (криптографических) средств не менее КС2 | - | - | - | - | - |

## 4.3. Результаты исследований СФК, средств обработки и отображения данных

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерий оценки | Наличие | Срок действия | Номер | Номер приложения | Уровень доверия |
| Лицензия на программное обеспечение Системы | + | Бессрочно | №BSS-ABR/S-Correqts | - | В |
| Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Клиента | - | - | - | - | С |
| Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Клиента | + | - | - | [12] | В |
| Заключение о корректности встраивания СКЗИ в Систему | Информация не предоставлена | - | - | - | С |
| Документация на систему ДБО (техническое описание или техническая записка, инструкция пользователя, инструкция администратора безопасности) | + | - | - | https://online.abr.ru/ru/help/html/ | В |
| Аттестат соответствия ФСТЭК России на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация или средство построения доверенной среды на стороне Банка | Отчет о результатах проведения оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 09 июня 2012г. №382-П. | - | - | - | В |
| Аттестат соответствия ФСТЭК на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация или средство построения доверенной среды на стороне Клиента | Аттестат соответствия АСЗИ Госкорпорации «Росатом» требованиям безопасности информации | от 28.12.2018  до 28.12.2021 | № 28/12/2018 – АСЗИ/ГК | - | В |
| Установлено сертифицированное антивирусное ПО на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы | Kaspersky Endpoint Security для Windows (версия 11.0.0.6499) | от 22.01.2019 до 22.01.2024 | №4068 | 7 | В |
| Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Банка | В связи с отсутствием сертифицированного ФСБ России и ФСТЭК России решения для виртуальных серверов на аппаратных блейд-устройствах, данный параметр не оценивается | - | - | - | - |
| Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Клиента | Dr.Web Enterprise Security Suite | от 27.01.2016 до 27.01.2024 | №3509 | 8 | В |
| Установлено сертифицированное СЗИ от НСД на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы |  | - | - | - | В |
| Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Банка | Информация не предоставлена | - | - | - | Н |
| Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Клиента | СЗИ Secret Net Studio | от 16.05.2017 до 16.05.2020 | № 3745 | 12 | В |

## 4.4. Результаты исследований участников процессов обработки данных

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерий оценки | Наличие | Срок действия | Номер | Номер приложения | Уровень доверия |
| Документ, подтверждающий допуск пользователей Банка к работе с СКЗИ в Системе | Регламент обучения, повышения и поддержания осведомленности работников АО ««BANK\_NAME» в области информационной безопасности (версия 3.0) | Бессрочно | Приказ №165-П | 12 | В |
| Документ, подтверждающий допуск пользователей Клиента к работе с СКЗИ в Системе | 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» | Бессрочно | - | [12] | В |
| Документ, подтверждающий прохождение обучения пользователями Системы на стороне Банка | Регламент обучения, повышения и поддержания осведомленности работников АО ««BANK\_NAME» в области информационной безопасности (версия 3.0) | Бессрочно | Приказ №165-П | 12 | В |
| Документ, подтверждающий прохождение обучения пользователями Системы на стороне Клиента | 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» | Бессрочно | - | [12] | В |
| Локальные нормативные акты, определяющие права и роли работников Банка в Системе (подписантов, администраторов безопасности) | + | - | - | - | В |
| Локальные нормативные акты, определяющие права и роли работников Клиента в Системе (подписантов, администраторов безопасности) | + | - | - | - | В |
| Контроль администраторами безопасности условий использования СКЗИ на стороне Банка | Порядок использования СКЗИ и ключевой информации при работе с системами дистанционного банковского обслуживания «Клиент-Банк» в АО ««BANK\_NAME» (версия 1.2) | от 24.07.2018 | №592-П | 14 | В |
| Контроль администраторами безопасности условий использования СКЗИ на стороне Клиента | + | - | - | - | В |

5. ВЫВОДЫ И РЕКОМЕНДАЦИИ

## 5.1. Выводы

На момент составления Заключения по полученной от АО ««BANK\_NAME» информации Система соответствует низкому уровню доверия[[1]](#footnote-1). Согласно ЕОМУ в организациях Госкорпорации «Росатом» допустима эксплуатация систем с уровнем доверия не ниже среднего.

## 5.2. Рекомендации

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

Для шифрования данных при передаче через сеть интернет использовать алгоритмы ГОСТ, реализуемые с использованием сертифицированных ФСБ России средств криптографической защиты информации;

Использовать сертифицированные СКЗИ, антивирусное программное обеспечение и средства защиты информации от несанкционированного доступа на АРМ пользователей Системы на стороне Банка, либо предоставить информацию об отсутствии таких пользователей.

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

Использовать в Системе усиленную квалифицированную электронную подпись усовершенствованного формата;

Органу криптографической защиты провести проверку условий использования СКЗИ, выдать заключение о возможности эксплуатации СКЗИ на стороне Банка ГПБ (АО);

Провести оценку корректности встраивания СКЗИ в Систему.

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

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

ОКЗ АО «Гринатом» рекомендует в Правилах предусмотреть ответственность АО ««BANK\_NAME» перед АО «Атомэнергопром» в сумме реально доказанного ущерба, который может быть нанесен в результате:

* несанкционированного доступа к сведениям АО «Атомэнергопром» на серверной части Системы;
* действий злоумышленников по причине слабой аутентификации пользователей Системы;
* использования ключей электронной подписи неуполномоченным лицом АО ««BANK\_NAME» в результате нарушения конфиденциальности ключа;
* нарушения конфиденциальности и целостности передаваемых данных;
* отказа в обслуживании пользователей Системы по вине АО ««BANK\_NAME»;
* непризнания юридической силы электронных документов банка вследствие отсутствия обязательных реквизитов.

**6. НОРМАТИВНАЯ И СПРАВОЧНАЯ ДОКУМЕНТАЦИЯ**

* 1. Правила АО ««BANK\_NAME» обмена электронными документами с использованием Системы «Клиент-Банк» для корпоративных клиентов (Приложение №1);
  2. Письмо АО «Атомэнергопром от 28.10.2019 №5-Д2/30.8/918 «О результатах оценки уровня к автоматизированной системе «ДБО BS-Client» АО ««BANK\_NAME» (Приложение №2);
  3. Письмо АО ««BANK\_NAME» от 09.01.2020 №00-12-исх (Приложение №3);
  4. Лицензия ФСБ России ОАО ««BANK\_NAME» ЛСЗ №0000823 Рег. №986Н от 04 февраля 2016 г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание 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) (Приложение №4),
  5. Лицензия ФСБ России ООО «БСС» ЛСЗ №0014278 Рег. №15712Н от 31 января 2017г. 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) (Приложение №5);
  6. Сертификат соответствия ФСБ России от 11.01.2018 № СФ/124-3271, действителен до 11.01.2021 на средство криптографической защиты (СКЗИ) «Крипто-Ком 3.4» (вариант исполнения 43) (Приложение №6);
  7. Сертификат соответствия ФСТЭК России на программное изделие «Kaspersky Endpoint Security для Windows» (версия 11.0.0.6499) от 22.01.2019 №4068, действителен до 22.01.2024 (Приложение №7);
  8. Сертификат соответствия ФСТЭК России на программное средство «Dr.Web Enterprise Security Suite» от 27.01.2016 №3509, действителен до 27.01.2024 (Приложение №8);
  9. Сертификат соответствия ФСТЭК России на средство защиты информации Secret Net Studio от 16.05.2017 № 3745, действителен до 16.05.2020 (Приложение №9);
  10. Приказ АО «Гринатом» от 20.10.2020 №22/46-П «О внесении изменений в Приказ ЗАО «Гринатом» от 16.02.2016 №22/126-П «О возложении дополнительных функциональных обязанностей сотрудников Органа криптографической защиты ЗАО «Гринатом» на штатных сотрудников» (Приложение №10);
  11. Сертификат соответствия ФСБ России от 20.11.2018 № СФ/124-3523, действителен до 01.12.2020 на средство криптографической защиты (СКЗИ) «Рутокен ЭЦП 2.0» (исполнения 1, 2) (Приложение №11);
  12. 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» к Договору Присоединения от (http://crypto.rosatom.ru/dokumentatsiya/reglamenty/reglament-okz);
  13. Регламент обучения, повышения и поддержания осведомленности работников «BANK\_NAME» в области информационной безопасности (версия 3.0) утв. Приказом от 16.03.2017 №165-П (Приложение №12);
  14. Порядок использования СКЗИ и ключевой информации при работе с системами дистанционного банковского обслуживания «Клиент-Банк» в АО ««BANK\_NAME» (версия 1.2), утв. Приказом от 24.07.2018 №592-п (Приложение №13).

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) |

Ознакомлен:

|  |  |
| --- | --- |
| Помощник директора по работе с банками и финансовыми рынками  АО «Атомэнергопром» | **\_\_\_\_\_\_\_\_\_\_\_\_/**И.И. Данилова  (подпись) (Ф.И.О) |

В.А. Силкин

(499) 949-49-19 доб. 5420

**НАИМЕНОВАНИЕ СИСТЕМЫ – SYSTEM\_NAME**

**BANK\_NAME – BANK\_NAME**

1. Срок действия Заключения – 1 год при сохранении уровня доверия к Системе [↑](#footnote-ref-1)