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

|  |  |
| --- | --- |
|  | **УТВЕРЖДАЮ**  *<указывается должность>*  \_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_  (подпись) (Ф.И.О)  «\_\_\_»**\_\_\_\_\_\_\_\_\_\_** 20\_\_ г. |

**ЗАКЛЮЧЕНИЕ**

**по результатам оценки уровня доверия к**

*<указывается наименование Системы>*

г. Москва

1. **ВВОДНАЯ ЧАСТЬ**
   1. **Основание для выдачи заключения**

*Указываются реквизиты договора, на основании которого проводятся работы.*

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

*Указывается наименование Системы.*

* 1. **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;
* Риски информационной безопасности, связанные с договорными отношениями с <*указывается наименование Системы>*.

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).

* 1. **Методы исследования**
* Анализ представленной в Орган криптографической защиты АО «Гринатом» документации на Систему;
* Анализ договора на использование Системы на предмет наличия рисков информационной безопасности.

1. **В ПРОЦЕССЕ ИССЛЕДОВАНИЯ УСТАНОВЛЕНО**

Для проведения исследования письмом *<указать* *реквизиты письма с запросом информации к Владельцу Системы>* была запрошена информация в *<указать наименование Владельца Системы>*. В ответ был получен ответ *<указать реквизиты ответа Владельца Системы>*.

* 1. **Описание Системы**

*В данном разделе указывается описание Системы.*

* 1. **Схема сетевого взаимодействия**

*В данном разделе указывается схема сетевого взаимодействия Системы.*

**3.3. Классификация информации в Системе**

*Указываются заключения ПДТК о наличии или отсутствии в Системе конфиденциальной информации.*

**3.4. 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 методикой определения доверия к криптографическим сервисам, утв. Приказом от 22.10.2015 №1/1009-П (далее – Методика).*

* + 1. **Жизненный цикл ключей пользователей Системы**

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

* 1. **Жизненный цикл СКЗИ, использующихся в Системе**

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

* 1. **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 Методикой.*

* 1. **Выполнение требований по безопасности информации на стороне Владельца Системы и на стороне организации-обладателя конфиденциальной информации**

*Указываются реквизиты документов, подтверждающих выполнение требований по безопасности информации на стороне Владельца Системы и на стороне организации-обладателя конфиденциальной информации.*

* 1. **Риски информационной безопасности, связанные с договорными отношениями с Владельцем Системы**

*Указываются реквизиты договора или ссылка на проект договора между Владельцем Системы и организацией-обладателем конфиденциальной информации и риски, связанные с договорными отношениями, согласно ЕОМУ.*

**4. ОЦЕНКА СООТВЕТСТВИЯ**

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерий оценки | Наличие | Срок действия | Номер | Приложение № | Уровень доверия |
| Лицензия ФСБ России на соответствующие виды деятельности |  |  |  |  |  |
| Документ, подтверждающий право использования на средство реализующее инфраструктуру ключевой системы (договор, лицензия и пр.) |  |  |  |  |  |
| Документ, подтверждающий право использования на СКЗИ, использующееся в составе средства, реализующего инфраструктуру ключевой системы (договор, лицензия и пр.) |  |  |  |  |  |
| Действующий сертификат соответствия ФСБ России на средство, реализующие инфраструктуру ключевой системы, сертифицированное в соответствии с системой сертификации РОСС RU.0001.030001 по классу не ниже КС2 |  |  |  |  |  |
| Действующий сертификат соответствия ФСБ России на средство криптографической защиты информации, использующееся для работы средства, реализующего инфраструктуру ключевой системы с классом защиты не ниже КС2 |  |  |  |  |  |
| В Банке используются сертифицированные ФСТЭК ключевые носители |  |  |  |  |  |
| В Банке используются несертифицированные ФСТЭК ключевые носители |  |  |  |  |  |
| Клиент использует сертифицированные ФСТЭК ключевые носители |  |  |  |  |  |
| Клиент использует несертифицированные ФСТЭК ключевые носители |  |  |  |  |  |
| Журнал поэкземплярного учета Банка с отметками об учете средств, реализующих инфраструктуру ключевой системы |  |  |  |  |  |
| Документы, регламентирующие жизненный цикл ключевой системы |  |  |  |  |  |
| Свидетельство об аккредитации |  |  |  |  |  |
| Документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации) |  |  |  |  |  |
| Наличие дополнительных служб удостоверяющего центра (службы онлайновой проверки статусов сертификатов и службы штампов времени) |  |  |  |  |  |
| Поддержка формата усовершенствованной подписи |  |  |  |  |  |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерий оценки | Наличие | Срок действия | Номер | Приложение № | Уровень доверия |
| Используются сертифицированные средства криптографической защиты информации |  |  |  |  |  |
| Документ, подтверждающий право передачи СКЗИ, использующееся в работе Системы (договор, лицензия и пр.) |  |  |  |  |  |
| Сертификаты соответствия ФСБ России на средства криптографической защиты информации с актуальным сроком действия (эксплуатирующиеся на рабочих местах пользователей Системы) |  |  |  |  |  |
| Журнал поэкземплярного учета Банка с отметками об учете передаваемых Клиенту СКЗИ, эксплуатационной и технической документации к ним |  |  |  |  |  |
| Журнал поэкземплярного учета Клиента с отметками об учете полученных СКЗИ от Банка, эксплуатационной и технической документации к ним |  |  |  |  |  |
| Класс защиты применяющихся на рабочих местах пользователей Системы шифровальных (криптографических) средств не менее КС1 |  |  |  |  |  |
| 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 | Приложение № | Уровень доверия |
| Лицензия на программное обеспечение Системы |  |  |  |  |  |
| Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Банка |  |  |  |  |  |
| Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Клиента |  |  |  |  |  |
| Копия формуляра на СКЗИ, полученного Банком от производителя, с отметкой об учётном номере дистрибутива СКЗИ и подтверждение получения из доверенного источника (акт приема-передачи и пр.) |  |  |  |  |  |
| Копия формуляра на СКЗИ, полученного Клиентом от Банка, с отметкой об учётном номере дистрибутива СКЗИ и подтверждение получения из доверенного источника (акт приема-передачи и пр.) |  |  |  |  |  |
| Заключение о корректности встраивания СКЗИ в Систему |  |  |  |  |  |
| Документация на систему ДБО (техническое описание или техническая записка, инструкция пользователя, инструкция администратора безопасности) |  |  |  |  |  |
| Документ, фиксирующий (подтверждающий) версию программного обеспечения Системы и регламент обновления Системы |  |  |  |  |  |
| Аттестат соответствия ФСТЭК на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация или средство построения доверенной среды на стороне Банка |  |  |  |  |  |
| Аттестат соответствия ФСТЭК на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация или средство построения доверенной среды на стороне Клиента |  |  |  |  |  |
| Установлено сертифицированное антивирусное ПО на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы |  |  |  |  |  |
| Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Банка |  |  |  |  |  |
| Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Клиента |  |  |  |  |  |
| Установлено сертифицированное средство защиты от несанкционированного доступа (далее - СЗИ от НСД) на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы |  |  |  |  |  |
| Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Банка |  |  |  |  |  |
| Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Клиента |  |  |  |  |  |

**4.4. Результаты исследований участников процессов обработки данных**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерий оценки | Наличие | Срок действия | Номер | Приложение № | Уровень доверия |
| Документ, подтверждающий допуск пользователей Банка к работе с СКЗИ в Системе |  |  |  |  |  |
| Документ, подтверждающий допуск пользователей Клиента к работе с СКЗИ в Системе |  |  |  |  |  |
| Документ, подтверждающий прохождение обучения пользователями Системы на стороне Банка |  |  |  |  |  |
| Документ, подтверждающий прохождение обучения пользователями Системы на стороне Клиента |  |  |  |  |  |
| Локальные нормативные акты, определяющие права и роли работников Банка в Системе (подписантов, администраторов безопасности) |  |  |  |  |  |
| Локальные нормативные акты, определяющие права и роли работников Клиента в Системе (подписантов, администраторов безопасности) |  |  |  |  |  |
| Контроль администраторами безопасности условий использования СКЗИ на стороне Банка |  |  |  |  |  |

**5. ВЫВОДЫ И РЕКОМЕНДАЦИИ**

**5.1. Выводы**

На момент составления Заключения по полученной от *<указывается наименование Владельца Системы>* информации Система обеспечивает *<указывается выявленный уровень* доверия> уровень доверия. Согласно ЕОМУ в организациях Госкорпорации «Росатом» допустим уровень доверия не ниже среднего.

**5.2. Рекомендации**

Для приведения Системы к среднему уровню доверия Орган криптографической защиты АО «Гринатом» рекомендует *<указывается наименование Владельца Системы>* 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 АО «Гринатом» рекомендует *<указывается наименование Владельца Системы>* 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 АО «Гринатом» рекомендует <*указывается наименование организации-обладателя конфиденциальной информации>* провести следующие работы в краткосрочной перспективе:

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

Для приведения Системы к высокому уровню доверия ОКЗ АО «Гринатом» рекомендует *<указывается наименование организации-обладателя конфиденциальной информации>* провести следующие работы в среднесрочной перспективе:

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

*Указываются рекомендации по изменению формулировок договора между Владельцем Системы и организацией-обладателем конфиденциальной информации для снижения рисков информационной безопасности, связанные с договорными отношениями, согласно ЕОМУ.*

**6. НОРМАТИВНАЯ И СПРАВОЧНАЯ ДОКУМЕНТАЦИЯ**

*Перечень нормативно-справочной документации и приложений.*

Заключение составил:

|  |  |
| --- | --- |
| *<указывается должность>* | **\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_**  (подпись) (Ф.И.О) |
|  |  |
|  |  |

Ознакомлен:

|  |  |  |  |
| --- | --- | --- | --- |
| *<указывается должность>* | **\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_**  (подпись) (Ф.И.О) | | |
|  |  | | |
|  |  | | |
|  |  | | |
|  | |  |

Исп: ФИО

Тел: