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

ГРИНАТОМ

АКЦИОНЕРНОЕ ОБЩЕСТВО «ГРИНАТОМ»

Лицензия ФСБ России рег. ЛСЗ № 0014254 Рег. №15686 Н
от 19 января 2017 года.

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
<ДОЛЖНОСТЬ ПРОВЕРЯЮЩЕГО>	<ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ ОРГАНА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ>
_____/_____ (подпись) (Ф.И.О)	_____/_____ (подпись) (Ф.И.О)
«___»_____ 20__ г.	«___»_____ 20__ г.

м.п.

ЗАКЛЮЧЕНИЕ ОРГАНА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ АО «ГРИНАТОМ»

по результатам оценки уровня доверия к защищенной с использованием шифровальных (криптографических) средств
«НАИМЕНОВАНИЕ СИСТЕМЫ»

Москва

20__ г.

1. ВВОДНАЯ ЧАСТЬ

1.1. Основание для исследования

Заявление от … г. на контроль (оценку) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

1.2. Наименование защищенной с использованием шифровальных (криптографических) средств информационной или телекоммуникационной системы

_____

Наименование Системы

1.3. Вопросы для исследования

1.3.1. Исследование договора на эксплуатацию «НАИМЕНОВАНИЕ СИСТЕМЫ» между организацией-обладателем конфиденциальной информации и Банком на наличие рисков информационной безопасности;
1.3.2. Наличие в договоре рисков для клиента в области информационной безопасности;
1.3.3. Юридическая значимость документов в «НАИМЕНОВАНИЕ СИСТЕМЫ»;
1.3.4. Доверие криптографическим сервисам «НАИМЕНОВАНИЕ СИСТЕМЫ»;
1.3.5. Доверия к СФК, средствам обработки и отображения данных;
1.3.6. Доверие к технологии, реализующей инфраструктуру ключевой системы;
1.3.7. Доверие к участникам процессов обработки данных.

2. ИССЛЕДОВАТЕЛЬСКАЯ ЧАСТЬ

2.1. Материально-технические средства (приборы, оборудование и пр.), применяемые при подготовке заключения

- Программное обеспечение;
- Средства защиты информации;
- Средства криптографической защиты информации;
- Проект договора/подписанный договор на «НАИМЕНОВАНИЕ СИСТЕМЫ»;
- Лицензии на лицензируемые виды деятельности;
- Сертификаты соответствия;
- Свидетельства об аккредитации;
- Эксплуатационная документация.
- Локальные нормативные акты

2.2.Нормативная и справочная документация

- [1] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
- [2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- [3] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- [4] Федеральный закон от 06.04 2011 № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями).
- [5] Федеральный закон от 04.05.2011 № 99-ФЗ (ред. от 21.07.2014) «О лицензировании отдельных видов деятельности» (04.05.2011).
- [6] Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» (в редакции постановления Правительства Российской Федерации от 20.07.2012 № 740).
- [7] Постановление Правительства Российской Федерации от 15.05.2010 № 330 «Об утверждении Положения об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов её проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения».
- [8] Постановление Правительства Российской Федерации от 03.02.2012 № 79 «Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации».
- [9] 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)»;
- [10] Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- [11] ГОСТ Р ИСО 15489-1—2007 Управление документами. Общие требования.

- [12] Национальный стандарт Российской Федерации ограниченного распространения ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».
- [13] «Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждённое Председателем Гостехкомиссии России 25.11.1994.
- [14] «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждённые приказом Гостехкомиссии России от 30.08.2002 № 282.
- [15] «Методические рекомендации по технической защите информации, составляющей коммерческую тайну», утверждённые заместителем директора ФСТЭК России 25.12.2006.
- [16] «Пособие по организации технической защиты информации, составляющей коммерческую тайну», утверждённое заместителем директора ФСТЭК России 25.12.2006.
- [17] 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».
- [18] Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- [19] Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
- [20] Приказ Госкорпорации «Росатом» от 28.03.2011 № 1/238-П «Об утверждении Единой политики защиты коммерческой тайны в атомной отрасли».
- [21] Приказ Госкорпорации «Росатом» от 20.06.2012 № 1/540-П «Об оценке видов информации ограниченного доступа при создании, модернизации и эксплуатации автоматизированных систем в защищённом исполнении и прикладных информационных систем».
- [22] Приказ Госкорпорации «Росатом» от 23.09.2014 № 1/910-П-дсп. «Об утверждении Отраслевых требований по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию, составляющую коммерческую тайну, служебную информацию ограниченного распространения (с пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации «Росатом» и её организациях».
- [23] Приказ Госкорпорации «Росатом» от 13.10.2015 № 1/978-П «Об утверждении Единых отраслевых методических указаний по управлению расчётно-кассовым обслуживанием в Госкорпорации «Росатом» и её организациях».

- [24] Приказ Госкорпорации «Росатом» от 22.10.2015 №1/1009-П «Об утверждении Единых отраслевых методических указаний по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях.

2.3. Методы исследования

- Анализ представленной в ответ на запрос от «___» _____ 20___г. документации;
- Изучение и обобщение информации в представленной документации на «НАИМЕНОВАНИЕ СИСТЕМЫ».
- Опрос специалистов АО «Гринатом»;

2.4. Риски для клиента в области информационной безопасности в договоре

2.5. Результаты исследований на предмет юридической значимости документов в «НАИМЕНОВАНИЕ СИСТЕМЫ»

2.6. Результаты исследований на предмет доверия криптографическим сервисам «НАИМЕНОВАНИЕ СИСТЕМЫ»

Критерий оценки	Наличие	Срок действия	Номер	Приложение №
Используются средства криптографической защиты информации				
Сертификаты соответствия ФСБ России на средства криптографической защиты информации с актуальным сроком действия				
Документация на СКЗИ				
СКЗИ соответствует «Требованиям к средствам электронной подписи» (приложение № 1 к приказу ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»)				
Соответствуют требованиям ГОСТ 28147-89				
Соответствуют требованиям ГОСТ Р 34.11-94				
Соответствуют требованиям ГОСТ Р 34.11-2012				
Соответствуют требованиям ГОСТ Р 34.10-2001				

Соответствуют требованиям ГОСТ Р 34.10-2012				
Класс защиты применяемых шифровальных (криптографических) средств не менее КС1				
Класс защиты применяемых шифровальных (криптографических) средств не менее КС2				
Используются сертифицированные ключевые носители				
Используются ключевые носители типа Токен или Смарт-карты				
Используются ключевые носители типа Сменный Flash-носитель или Жесткий диск ПЭВМ				

2.7. Результаты исследований на предмет доверия к СФК, средствам обработки и отображения данных

Критерий оценки	Наличие	Срок действия	Номер	Приложение №
Защита информации производится средствами операционной системы				
Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ				
Копия формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника)				
Заключение о корректности встраивания СКЗИ в «НАИМЕНОВАНИЕ СИСТЕМЫ»				
Документация на систему ДБО				
Зафиксирована версия Программного обеспечения «НАИМЕНОВАНИЕ СИСТЕМЫ» и ОС				
Наличие аттестата соответствия на соответствие требованиям по информационной безопасности				
Используется сертифицированное антивирусное ПО				
Установлено сертифицированное СЗИ от НСД				
Сертификат соответствия ФСБ на СПДС				
Аттестат соответствия ФСТЭК на АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация				

2.8. Результаты исследований на предмет доверия к технологии, реализующей инфраструктуру ключевой системы

Критерий оценки	Наличие	Срок действия	Номер	Приложение №
Лицензия ФСБ России на соответствующие виды деятельности				
Лицензия на программное обеспечение				
Средство, реализующие инфраструктуру ключевой системы сертифицировано в соответствии с системой сертификации РОСС RU.0001.030001 по классу КС2				
Средство, реализующие инфраструктуру ключевой системы сертифицировано в соответствии с системой сертификации РОСС RU.0001.030001 по классу КС3				
Документация на СКЗИ				
Документы, регламентирующие жизненный цикл ключевой системы				
Свидетельство об аккредитации				
Документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации)				
Средство автоматизации удостоверяющего центра соответствует «Требованиям к средствам удостоверяющего центра» (приложение № 2 к приказу ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»)				
Наличие дополнительных служб удостоверяющего центра (службы онлайновой проверки статусов сертификатов и службы штампов времени)				
Поддержка формата усовершенствованной подписи				

2.9. Результаты исследований на предмет доверия к участникам процессов обработки данных

Критерий оценки	Наличие	Срок действия	Номер	Приложение №
Локальные нормативные акты, обеспечивающие повышение осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации и использования технических средств защиты информации.				
Локальные нормативные акты, определяющие права и роли работников в системе				

3. ВЫВОДЫ И РЕКОМЕНДАЦИИ

«НАИМЕНОВАНИЕ СИСТЕМЫ» обеспечивает _____ уровень доверия к криптографическим сервисам.

Приложение:

Приложение №1. Лицензия ФСБ России на соответствующие виды деятельности.

Приложение №2. Лицензия на программное обеспечение.

Приложение №3. Сертификаты соответствия в соответствии с системой сертификации РОСС RU.0001.030001 по классу КС2 или КС3 на средство, реализующем инфраструктуру ключевой системы.

Приложение №4. Документация на СКЗИ (копия формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника)).

Приложение №5. Документация, регламентирующая жизненный цикл ключевой системы;

Приложение №6. Свидетельство об аккредитации.

Приложение №7. Документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации).

Приложение №8. Сертификат соответствия на средство автоматизации удостоверяющего центра (соответствует/не соответствует «Требованиям к средствам удостоверяющего центра» (приложение № 2 к приказу ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»).

Приложение №9. Документация о наличии дополнительных служб удостоверяющего центра (службы онлайновой проверки статусов сертификатов и службы штампов времени).

Приложение №10. Документация о поддержке формата усовершенствованной подписи.

Приложение №11. Сертификаты соответствия ФСБ России на средства криптографической защиты информации, использующиеся в Системе (класс защиты применяемых шифровальных (криптографических) средств).

Приложение №12. Документация на СКЗИ (копия формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника)).

Приложение №13. Сертификаты соответствия на ключевые носители.

Приложение №14. Локальные нормативные акты, обеспечивающие повышение осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации и использования технических средств защиты информации.

Приложение №15. Локальные нормативные акты, определяющие права и роли работников в «НАИМЕНОВАНИЕ СИСТЕМЫ».