РОСАТОМ

ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

ПРИМЕНЕНИЕ МЕТОДИКИ ОЦЕНКИ ДОВЕРИЯ К ИНФОРМАЦИОННЫМ СИСТЕМАМ, ЗАЩИЩЕННЫМ С ИСПОЛЬЗОВАНИЕМ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ, НА ПРИМЕРЕ СИСТЕМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ В АТОМНОЙ ОТРАСЛИ

Отдел криптографической защиты
АО «Гринатом»

Бинкис Ян

2017 г.

Организация и обеспечение

4. Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, обладатели которой не имеют лицензий ФСБ России, лицензиаты ФСБ России организуют и обеспечивают на основании договоров на оказание услуг по криптографической защите конфиденциальной информации.
5. Лицензиаты ФСБ России несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ, а также положениям настоящей Инструкции.
При этом лицензиаты ФСБ России должны обеспечивать комплексность защиты конфиденциальной информации, в том числе посредством применения некриптографических средств защиты.

Приказ ФАПСИ РФ от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения …»:

Соблюдение отраслевых требований по ИБ

ОЦЕНКА ДОВЕРИЯ

Высокий уровень доверия* обеспечивается

Доверием к технологии, реализующей инфраструктуру ключевой системы:

- Наличием лицензии ФСБ России на соответствующие виды деятельности;
- Наличием сертификата об аккредитации удостоверяющего центра;
- Использованием сертифицированных ключевых носителей.

Доверием к СКЗИ, входящих в состав системы обработки данных:

- Использованием сертифицированных СКЗИ;
- Подтверждением Органа криптографической защиты лицензиата ФСБ России выполнения условий использования СКЗИ.

Доверием к средствам обработки и отображения данных:

- Наличием Заключений о корректности встраивания СКЗИ в Систему;
- Выполнением Стандарта Банка России; или наличием аттестата соответствия ФСТЭК России на Систему.

Доверием к участникам процессов обработки данных:

- Наличием документов, подтверждающих квалификацию и допуск пользователей Системы к самостоятельной работе с СКЗИ;
- Наличием периодического контроля администраторами безопасности условий использования СКЗИ.

*допустим в Госкорпорации «Росатом» и ее организациях

Средний* уровень доверия обеспечивается

Доверием к технологии, реализующей инфраструктуру ключевой системы:

- Наличием лицензии ФСБ России на соответствующие виды деятельности.

Доверием к СКЗИ, входящих в состав системы обработки данных:

- Использованием сертифицированных СКЗИ.

Доверием к средствам обработки и отображения данных:

- Выполнением Стандарта Банка России или наличием аттестата соответствия ФСТЭК России на Систему.

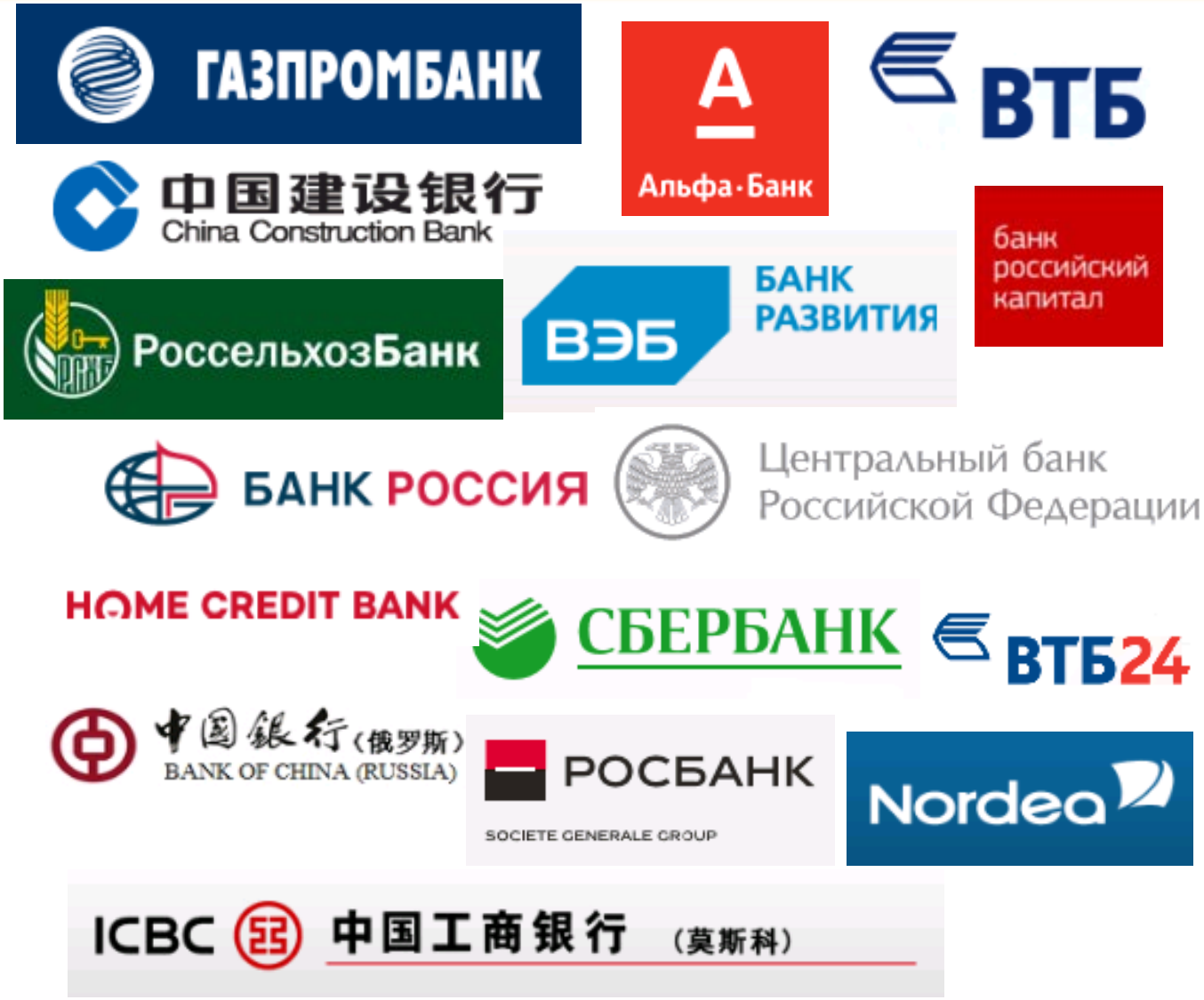
Доверием к участникам процессов обработки данных:

- Наличием документов, подтверждающих квалификацию и допуск пользователей Системы к самостоятельной работе с СКЗИ.

*допустим в организациях Госкорпорации «Росатом»

Системы
с низким уровнем доверия
ЗАПРЕЩЕНЫ
к использованию
в Госкорпорации «Росатом»
и ее организациях

Опыт применения



ОСОБЕННОСТИ ПРИМЕНЕНИЯ МЕТОДИКИ НА ПРЕДПРИЯТИЯХ АТОМНОЙ ОТРАСЛИ

В соответствии с Договором Присоединения №22/2143-Д на оказание услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств Орган криптографической защиты АО «Гринатом» работы по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

В ходе работ исследуются следующие вопросы:

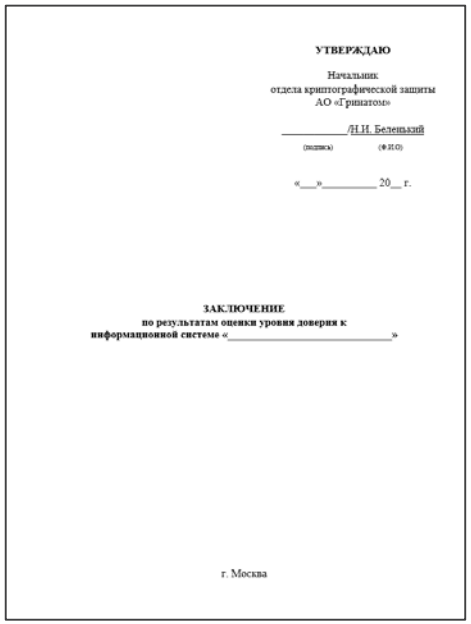
- Обеспечение доверия к технологии, реализующей инфраструктуру ключевой системы;
- Обеспечение доверия к средствам криптографической защиты, входящим в состав системы обработки данных;
- Обеспечение доверия к средствам обработки и отображения данных;
- Обеспечение доверия к участникам процессов обработки данных;
- Риски информационной безопасности, связанные с договорными отношениями на Систему.

Работа ведется постоянно в режиме мониторинга

Этапы проверки:

- Анализ представленной в Орган криптографической защиты АО «Гринатом» документации на Систему;
- Анализ договора и дополнительных соглашений на использование Системы на предмет наличия рисков информационной безопасности;
- Выдача Заключения по результатам оценки уровня доверия к Системе;
- Мониторинг на основании периодического (ежемесячного) контроля (оценки) уровня доверия к Системам контроль приведения Систем и документации на них в соответствие с требованиями по информационной безопасности;
- Осуществляет ежемесячный мониторинг актуальности документов Минкомсвязи России, ФСБ России, ФСТЭК России, производителей программного обеспечения, органа по аттестации объекта информатизации, владельца системы, органа криптографической защиты.

АНАЛИЗ ВЫЯВЛЕННЫХ НЕДОСТАТКОВ СИСТЕМ



УТВЕРЖДАЮ

Начальник
отдела криптографической защиты
АО «Гринатом»

_____/Н.И. Беленький
(подпись) (Ф.И.О)

«___»_____ 20__ г.

ЗАКЛЮЧЕНИЕ
по результатам оценки уровня доверия к
информационной системе «_____»

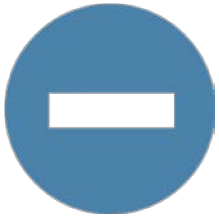
г. Москва

- Использование неквалифицированных сертификатов ключей проверки электронной подписи;
- Отсутствие подтверждения соответствия Стандарту Банка России;
- Отсутствие Заключения Органа криптографической защиты о возможности эксплуатации СКЗИ;
- Отсутствие оценки корректности встраивания СКЗИ в Систему;
- Отсутствие или не актуальность аттестатов соответствия ФСТЭК России на Систему ДБО, где обрабатывается конфиденциальная информация;
- Использование в Системе несертифицированных ключевых носителей;
- Нарушение установленного порядка передачи Клиенту СКЗИ с действующими сертификатами соответствия ФСБ России.

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ МЕТОДИКИ

Представленная методика имеет как плюсы, так и минусы и требует дальнейшего развития.

Плюсы:
Простота применения;
Прозрачность для сторон;
Конкретность критериев;
Универсальность применения.



Минусы:
Отсутствие нормативного закрепления уровней доверия в отечественных нормативных правовых актах.
Корпоративный подход. Отсутствие единых требований.

РЕКОМЕНДАЦИИ ПО РАЗВИТИЮ И СОВЕРШЕНСТВОВАНИЮ

1. Лицензиатам ФСБ России обеспечить проведение оценки доверия к защищенным с использованием шифровальных (криптографических) средств информационным и телекоммуникационным системам

2. Усовершенствовать методику в соответствии с полученным опытом оценки Систем

КОНТАКТЫ

СПАСИБО ЗА ВНИМАНИЕ!

Бинкис Ян

+7 (499) 949-49-19, доб. 6705

yabinkis@greenatom.ru

crypto.rosatom.ru