РОСАТОМ

ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

Оценка доверия информационным системам, защищенным с использованием шифровальных (криптографических) средств

Проблема доверия в информационных технологиях

Доверие по Ожегову:
Доверие - Уверенность в чьей-нибудь добросовестности, искренности, в правильности чего-нибудь

Доверие в ГОСТ Р ИСО/МЭК 15408-3-2013:
Доверие - основа для уверенности в том, что продукт или система ИТ отвечают целям безопасности.

Доверие в технике - это надежность. Доверие в праве – это ответственность

Технологии доверия vs технологии безопасности

Технологии отечественные и зарубежные.

Технологии доверия подразумевают организационно-технические меры.

Технологии безопасности – электронная подпись, аутентификация, шифрование

Л. Картер и В. Вираккоди уточнили понятие «доверия», разделив его на доверие к информационно-коммуникационным технологиям и доверие к органам власти, которые предлагают воспользоваться своими услугами в электронном виде

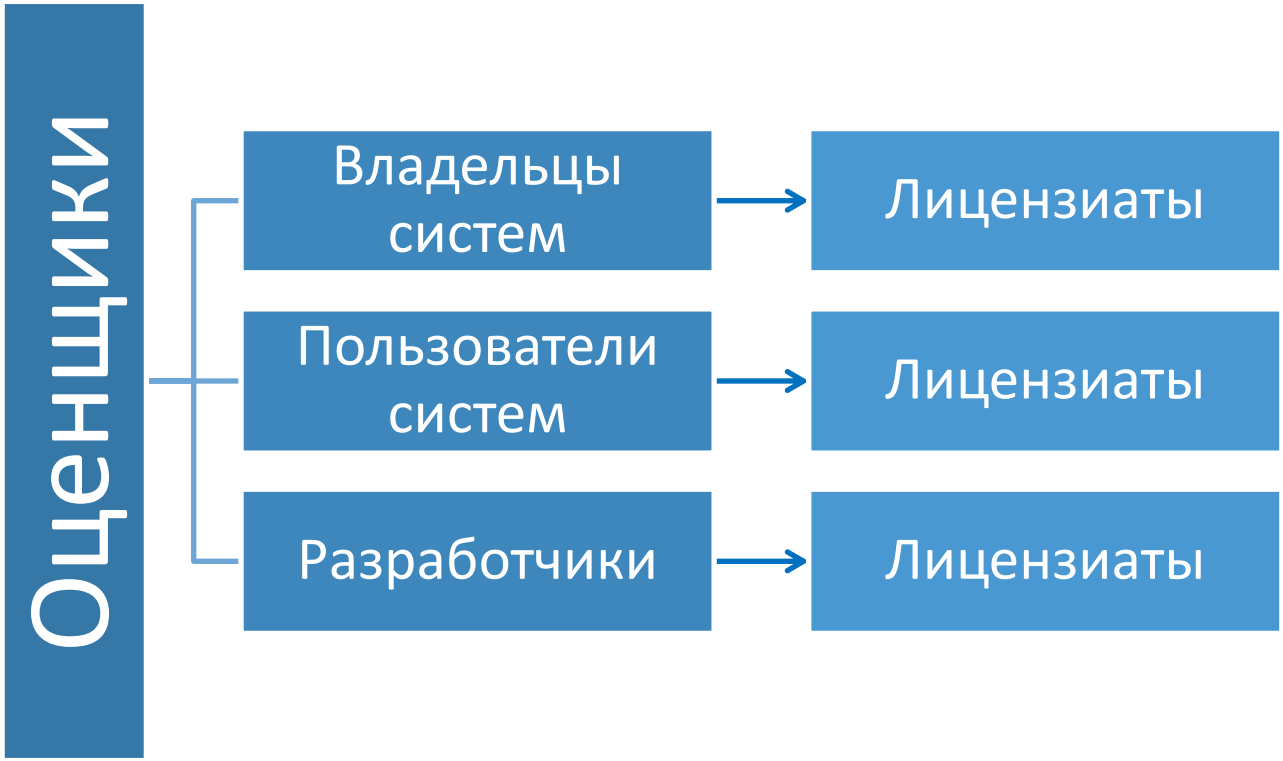
Оценка доверия

Методы оценки могут, в частности, включать в себя:
a) анализ и проверку процессов и процедур;
b) проверку того, что процессы и процедуры действительно применяются;
…
e) верификацию доказательств;
f) анализ руководств;
g) анализ разработанных функциональных тестов и полученных результатов;
h) независимое функциональное тестирование;
i) анализ уязвимостей, включающий в себя предположения о недостатках;
j) тестирование проникновения.

ГОСТ Р ИСО/МЭК 15408-3-2013

Оценка доверия

А судьи кто?


Оценщики
Владельцы систем
Пользователи систем
Разработчики
Лицензиаты
Лицензиаты
Лицензиаты

Перечень лицензируемых видов деятельности.

Регламентация применения СКЗИ:

- Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»
- Постановление Правительства РФ от 16.04.2012 N 313 "Об утверждении Положения о лицензировании деятельности…»
- Приказ ФАПСИ РФ от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения …» ,
- Приказ ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации…»
- Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных…»
- Приказ ФСБ России от 27 декабря 2011 г. N 796 «Об утверждении Требований к средствам электронной подписи..»
- И др.

Защищенные ИС и телекоммуникационные системы

Постановление Правительства РФ от 16.04.2012 N 313
"Об утверждении Положения о лицензировании деятельности…» определяет 28 лицензируемых видов деятельности.

1. Разработка шифровальных (криптографических) средств.
2. Разработка защищенных с использованием шифровальных (криптографических) средств информационных систем.
3. Разработка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
4. Разработка средств изготовления ключевых документов.
5. Модернизация шифровальных (криптографических) средств.
6. Модернизация средств изготовления ключевых документов.
7. Производство (тиражирование) шифровальных (криптографических) средств.
8. Производство защищенных с использованием шифровальных (криптографических) средств информационных систем.
9. Производство защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
10. Производство средств изготовления ключевых документов.
11. Изготовление с использованием шифровальных (криптографических) средств изделий, предназначенных для подтверждения прав (полномочий) доступа к информации и (или) оборудованию в информационных и телекоммуникационных системах.
12. Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств.
13. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем.
14. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
15. Монтаж, установка (инсталляция), наладка средств изготовления ключевых документов.
16. Ремонт шифровальных (криптографических) средств.
17. Ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств информационных систем.
18. Ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
19. Ремонт, сервисное обслуживание средств изготовления ключевых документов.
20. Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
21. Передача шифровальных (криптографических) средств.
22. Передача защищенных с использованием шифровальных (криптографических) средств информационных систем.
23. Передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
24. Передача средств изготовления ключевых документов.
25. Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.
26. Предоставление услуг по имитозащите информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.
27. Предоставление юридическим и физическим лицам защищенных с использованием шифровальных (криптографических) средств каналов связи для передачи информации.
28. Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

Проблема

Существуют проблемы с нормативным регулированием информационных и телекоммуникационных систем, защищённых с применением СКЗИ.

Не предусмотрена система формирования доверия к информационным и телекоммуникационным системам, защищенным с применением СКЗИ.

Использование «доверенных» сертифицированных СКЗИ в не доверенную информационную систему не гарантирует достижения состояния безопасности.

Примеры: Генерация ключа на рабочем месте, слабые или пустые пароли, отсутствие необходимых СЗИ, не правильные настройки среды функционирования и тд.

Приказ Государственной корпорации по атомной энергии "Росатом" «Об утверждении отраслевых требований по информационной безопасности…»

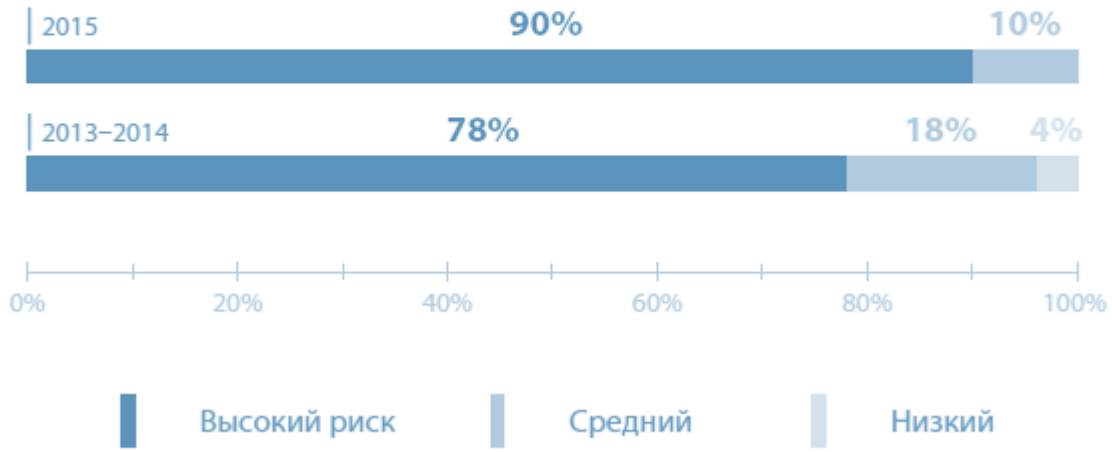
Приказ Государственной корпорации по атомной энергии "Росатом" от 22 октября 2015 года №1/1009-П «Об утверждении Единых отраслевых методических указаний по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и её организациях»

Созданные на их основе локальные нормативные акты:

- Приказы
- Регламенты
- Положения
- Инструкции

Уязвимости ДБО

В отличие от прошлых лет все исследованные системы ДБО содержали по меньшей мере недостатки среднего уровня риска, при этом практически в каждой из систем (90%) были обнаружены критически опасные уязвимости, что значительно хуже показателей 2013–2014 годов.



«Уязвимости приложений финансовой отрасли»
Positive Technologies, август 2016

Оценка доверия к технологии, реализующей инфраструктуру ключевой системы

Уровень доверия	Низкий	Средний	Высокий
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	-	-	+
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)	-	-	+

Оценка доверия к средствам криптографической защиты, входящим в состав системы обработки данных

Уровень доверия	Низкий	Средний	Высокий
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	+	-	-

Оценка доверия к СФК, средствам обработки и отображения данных

Уровень доверия	Низкий	Средний	Высокий
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 ИС	-	-	+
Документация на ИС	-	+	+
Зафиксирована версия Программного обеспечения ИС 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	-	-	+

Обеспечение доверия к участникам процессов обработки данных

Уровень доверия	Низкий	Средний	Высокий
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	-	+	+

Особенности методики

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

Плюсы:
Простота применения
Прозрачность для сторон
Конкретность критериев
Объективность оценки
Универсальность применения

Минусы
Не решает вопросы трансграничного обмена и взаимодействия с зарубежными системами
Требует дальнейшего расширения

Предложение

1. Регулятору (ФСБ России) разработать единую методику определения доверия к защищенным с использованием шифровальных (криптографических) средств информационным и телекоммуникационным системам)

2. Включить в перечень лицензируемых видов деятельности пункт «Оценка доверия защищенных с использованием шифровальных (криптографических) средств информационных систем и телекоммуникационных систем»

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

Спасибо за внимание

Ольшаников Алексей Владимирович,
Ведущий специалист
Отдел криптографической защиты
АО «Гринатом»
Общий центр обслуживания Госкорпорации «Росатом»
Тел: 8 (985) 998-44-84
avolshanikov@greenatom.ru