

Вопросы жизненного цикла СКЗИ с поддержкой старых и новых ГОСТов. Учет ограничений реального сектора ЭКОНОМИКИ

Дмитрий Левиев
Председатель Совета НП ПСИБ
Член рабочей группы по безопасности платежей
Комитета по безопасности предпринимательской
деятельности ТПП РФ

Обсуждаемые вопросы

- Текущий жизненный цикл СКЗИ
- Проблемы разнородных требований регуляторов для применения СКЗИ
- Проблемы жизненного цикла СКЗИ в крупных системах электронного документооборота
- Проблемы жизненного цикла СКЗИ защиты каналов связи
- Варианты жизненного цикла СКЗИ с учетом проблем реального сектора
- Внедрение ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012

Текущий жизненный цикл СКЗИ

- Заключение – срок действия 5 лет
- Необязательность цепочки заключение - сертификат
- Срок действия сертификата – 3 года максимально
- Непрозрачность процедуры сертификации СКЗИ:
 - Отсутствие открытых требований с СКЗИ
 - Отсутствие регламента сертификации СКЗИ
 - Отсутствие возможности контроля эксплуатирующей организацией действий разработчика по получению/продлению сертификата (проблема 6 ноября)

Проблемы применения СКЗИ

- Необходимость использования исключительно сертифицированных СКЗИ:
 - Наличие бумажного сертификата у разработчика
 - Наличие информации о наличии сертификата на официальном сайте ФСБ России
- Правильность применения СКЗИ:
 - Модель нарушителя
 - База уязвимостей (База ФСТЭК России)
 - База угроз
 - Модель угроз
 - Модель атак
 - Класс СКЗИ
 - Выполнение требований эксплуатационной документации

Жизненный цикл СКЗИ в крупных системах

- Разработка СКЗИ – до 2-х лет
- Сертификация СКЗИ – до 2-х лет
- Встраивание СКЗИ в конечную систему – до 1 года
- Опытная эксплуатация системы - до 1 года
- Распространение СКЗИ до 2 лет
- Промышленная эксплуатация – не менее 3 лет
- Модернизация – 1 год
- Вывод СКЗИ из эксплуатации - до 2-х лет

Предлагаемая схема жизненного цикла СКЗИ

- Разработка СКЗИ
- Сертификация СКЗИ – госуслуга (Административный регламент)
- Встраивание СКЗИ – формализация требований
- Сертификат на СКЗИ – 5 лет
- Дожитие СКЗИ – 2 года

Внедрение СКЗИ с ГОСТ 2012

- Срок замены ГОСТ – 31.12.2017
- Реальный срок окончания сертификатов на токены – 2016 год
- Сроки получения сертификатов на токены с ГОСТ 2012 – осень 2015 – весна 2016
- Сроки внедрения – до 1 года
- Сроки распространения – до 2-х лет (Банки ТОП-200)
- Необходимость нахождения финансирования в объеме не менее 7-14 млрд рублей.

Модель зрелости

- **Ребенок** - не понимает что говорит хотя уже знает слова «риск», «угроза», «нарушитель» и «атака». Не способен самостоятельно выполнять задачи по информационной безопасности (кроме «копать до обеда»)
- **Подросток** - понимает что говорит, ведет себя эгоистично. Обеспечение ИБ является первейшей целью бизнеса и все такое. Способен эффективно выполнять задачи по информационной безопасности без привлечения смежных подразделений

Модель зрелости

- **Юноша** - понимает что другим подразделениям сама по себе ИБ фиолетова. Переживает за это ("юношеский идеализм"). Способен эффективно выполнять задачи по информационной безопасности с привлечением смежных подразделений, способен определять задачи по ИБ в компании с существующей культурой ИБ
- **Молодой мужчина** - понимает цели других бизнес-подразделений, умеет интегрировать цели ИБ с целями бизнеса, способен определять и выполнять задачи по информационной безопасности. Не способен целенаправленно и быстро внедрять или изменять культуру информационной безопасности

Модель зрелости

- **Зрелый мужчина** - понимает цели других людей, вернее их интересы - бонус и грейд. Способен быстро и успешно внедрять культуру информационной безопасности, но не всегда считает целесообразным, ведь от этого не всегда повышается бонус и грейд
- **Старик (аксакал)** - понимает цели другого бизнеса, понимает и знает цели и ограничения регуляторов, умеет быстро и успешно внедрять ИБ в работу бизнеса, регуляторов и государства, способен определять направления развития по ИБ в рамках отрасли/государства.

Вопросы

- Клуб

<http://forum.npsib.org>

- Комитет по безопасности предпринимательской деятельности ТПП РФ

<http://tpprf.ru/ru/interaction/committee/kombez/>

- +7 (495) 971 8268