Learn. Connect.
Collaborate. together.

5 дней Уральского форума за 15 минут!

Лукацкий Алексей, консультант по безопасности

Новости ФСТЭК

- Готовятся 2 национальных стандарта по ИБ виртуализации и облачных вычислений
  - Принятие - май 2014
- Готовится приказ с требованиями к АСУ ТП КВО
  - Принятие – март-апрель 2014
  - Законопроект по критически важным объектам планируется внести в Госдуму в апреле 2014
  - К КВО могут (по предварительному проекту) относиться организации, финансовый ущерб которым превышает 1 миллион рублей
  - Многие системно значимые банки (и не только) могут попасть под раздачу

Новости ФСТЭК

- 19 февраля на сайте ФСТЭК выложен методический документ, раскрывающий смысл 21/17-го приказов по защите ПДн и ГИС
  - 754 предложений и замечаний. Принято 500
- «Приказ трех» по классификации ИСПДн отменен на прошлой неделе
- Вскорости планируется реализация ФСТЭК и ФСБ надзорных функций в рамках ПП-584 по защите платежных систем
- Готовится методика определения актуальных угроз
- Планируется разработка РД с требованиями к средствам защиты виртуализации

Новости ФСБ

- В конце февраля проект приказа по защите ПДн будет опубликован
  - Из 120 предложений по проекту приказа ФСБ по ПДн принята только шестая часть
- Обязательная сертификация СКЗИ для ПДн остается и меняться не будет
  - Вопрос применения СКЗИ для банкоматов, АБС, межфилиальном взаимодействии остается открытым
- Актуальность типа угроз определяется оператором ПДн
- 8-й Центр не видит смысла в разработке методички по моделированию угроз при наличии лицензиатов, которые могут это сделать
  - ФСТЭК такую методичку уже сделала
- Изменение подхода к сертификации СКЗИ

Новости РКН / персданные

- В 2014-м году будет пересмотрен перечень "адекватных" стран по линии ПДн
  - Актуально для трансграничных денежных переводов и представительств иностранных банков
- Готовящиеся законопроекты
  - по штрафам за несоблюдение отдельных требований ФЗ-152
  - по изменению ФЗ-152
  - по ответственности за неуведомление об утечке
  - по запрету отказа от предоставления услуг при отказе от дачи согласия на обработку ПДн

Новости Банка России

- Развитие ИБ в финансовой отрасли Банк России видит за счет тематик ПДн и банковской тайны, банковского CERT, ИБ виртуализации и облаков
- ЦБ планирует расширить действие СТО на все отрасли, которые попали под ЦБ после слияния с ФСФР
- Постепенном идет сдвиг в сторону реального управления рисками
  - Обязательные требования по ИБ могут исчезнуть (исключая базовый минимум) и банки будут сами выбирать меры защиты (как в 379-П и т.п.)
- Новая версия СТО 1.0 гармонизирована с 382-П, ПП-1119, ФЗ-261 и 21-м приказом ФСТЭК
- Предположительно с 01.05.14 новые версии СТО и РС будут введены в действие

Новости Банка России

- Уже есть планы по очередному витку развития СТО
  - Расширение 7-го раздела
  - Пересмотр 8-го раздела в связи с изменениями в ISO27K
- Новая версия СТО 1.2 гармонизирована с 382-П
  - Полное соответствие по алгоритму, частным показателям и срокам оценки
- На ТК122 единогласно утверждены РС по менеджменту инцидентов и ИБ на этапах жизненного цикла АБС
- На ТК122 рассматриваются РС по ИБ виртуализации и ресурсному обеспечению ИБ
- ЦБ готовит РС по DLP-решениям и мониторингу информации в соцсетях
  - На ТК122 вынесут в мае, а принятие планируется к концу года

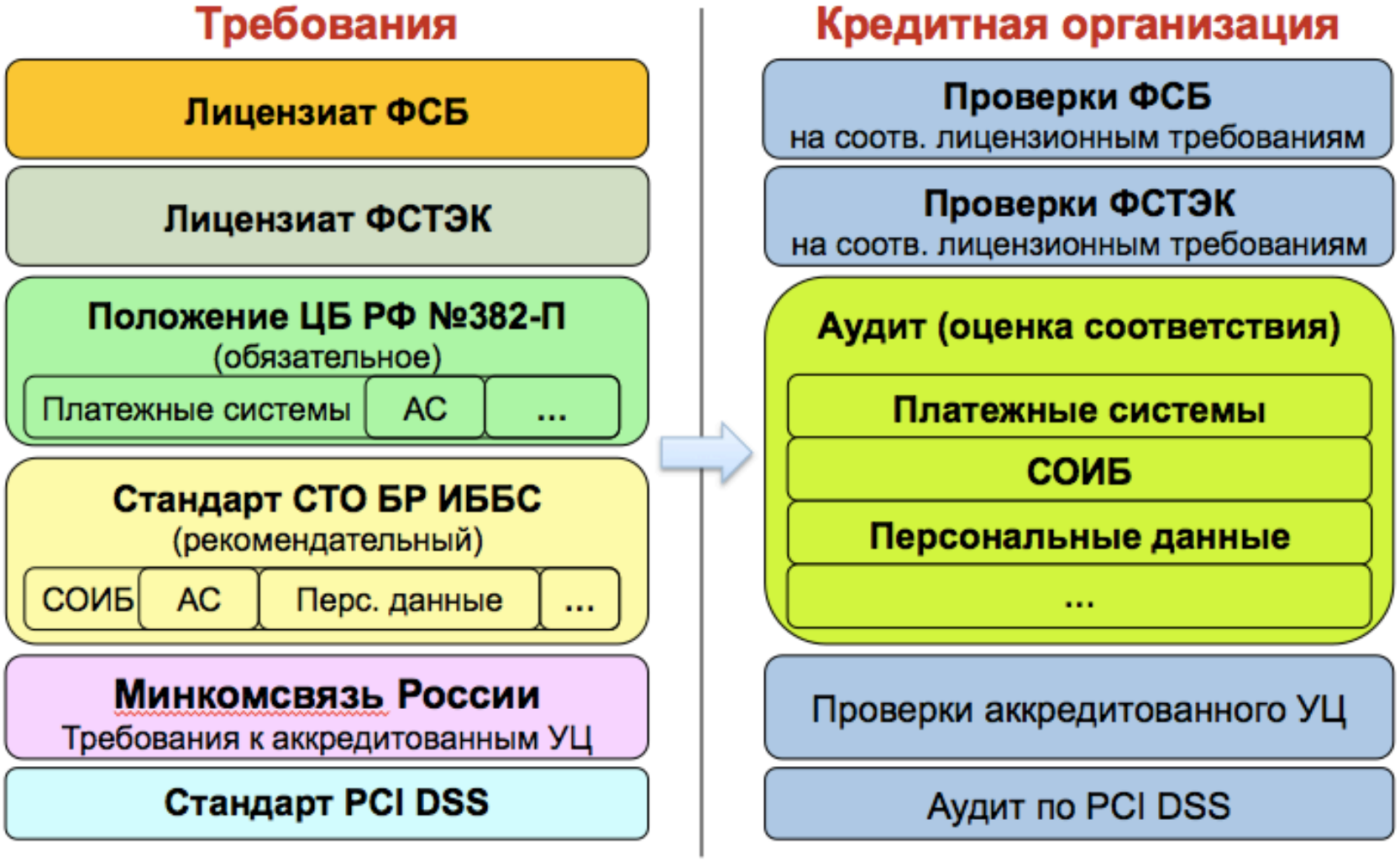
Новости Банка России

- Планируемые изменения в 382-П - банкоматы/платежные терминалы, платежные карты, интернет и мобильный банкинг
  - Требования к банкоматам сильно пересекаются с 34-Т
  - Требования к Интернет-банкингу похожи на 146-Т
  - Требования к мобильному банкингу похожи на предыдущий пункт + требования к распространению через репозитории
  - С 1-го января 2015 года вводится обязательное использование карт EMV (пока совмещенных с магнитной полосой)

Новости Банка России

- 258-ю форму отчетности планируется отменить и внести нужную информацию в 203-ю форму
  - Сроки пока не определены
- Внутренняя инструкция по проведению проверок 382-П (157-Т) может быть будет сделана открытой
- Изменение частоты подачи отчетности по 203-й форме не планируется
  - Но такая возможность рассматривается в перспективе
- Двойная нагрузка на банки по отправке отчетности в ЦБ и оператору платежной системы останется и отменять ее не будут
- Существующая частичная нестыковка требований 382-П и требований операторов платежных систем остается

Большое количество требований (без КВО)



Новости Банка России

- Подготовлены поправки в законодательство в части упрощенного возврата незаконно списанных средств
  - Подготовленные в прошлом году рекомендации по возврату незаконно списанных средств натолкнулись на недостатки действующего законодательства
- Банки не имеют права возлагать на клиентов возмещение затрат на расследование мошенничества

Отчетность

- Отчетность по "письму шести" ввиду выхода 382-П не нужна
  - Мнение 8-го Центра
- Отчетность ради отчетности не нужна. Нужна обратная связь от регулятора по коррекции поведения отчитывающихся
  - Мнение ФСТЭК
- Основная задача отчетности – стимулирование повышения защищенности банков
  - Мнение ФСТЭК и ФСБ
- Отчетность нужна для оценки факта отправки уведомления в РКН
  - Мнение РКН
- Зачем нужно две отчетности (по СТО и 382-П)?
  - А отчетность в банковский CERT будет отличаться от них или нет?

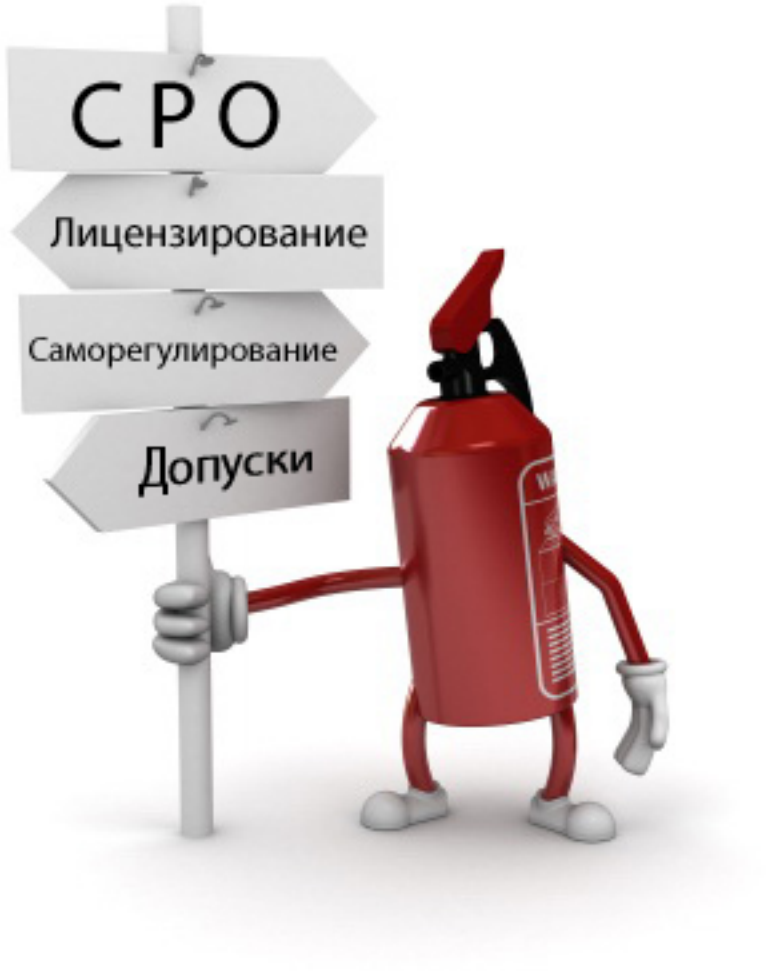
Банковский CERT

- Задача CERT (по крупному) - снижать число инцидентов. Для этого надо и причины надо знать, и реагировать, и для фрода правила писать
- У ЦБ уже есть предварительная финансовая оценка создания банковского CERT
- Банкам не хватает реагирования и нормальной аналитики. Если обсуждаемый CERT это решит, будет хорошо. Но нужно и законодательство править
- Идея поддержана ДНПС, ГУБиЗИ, АРБ

Правоприменительная практика

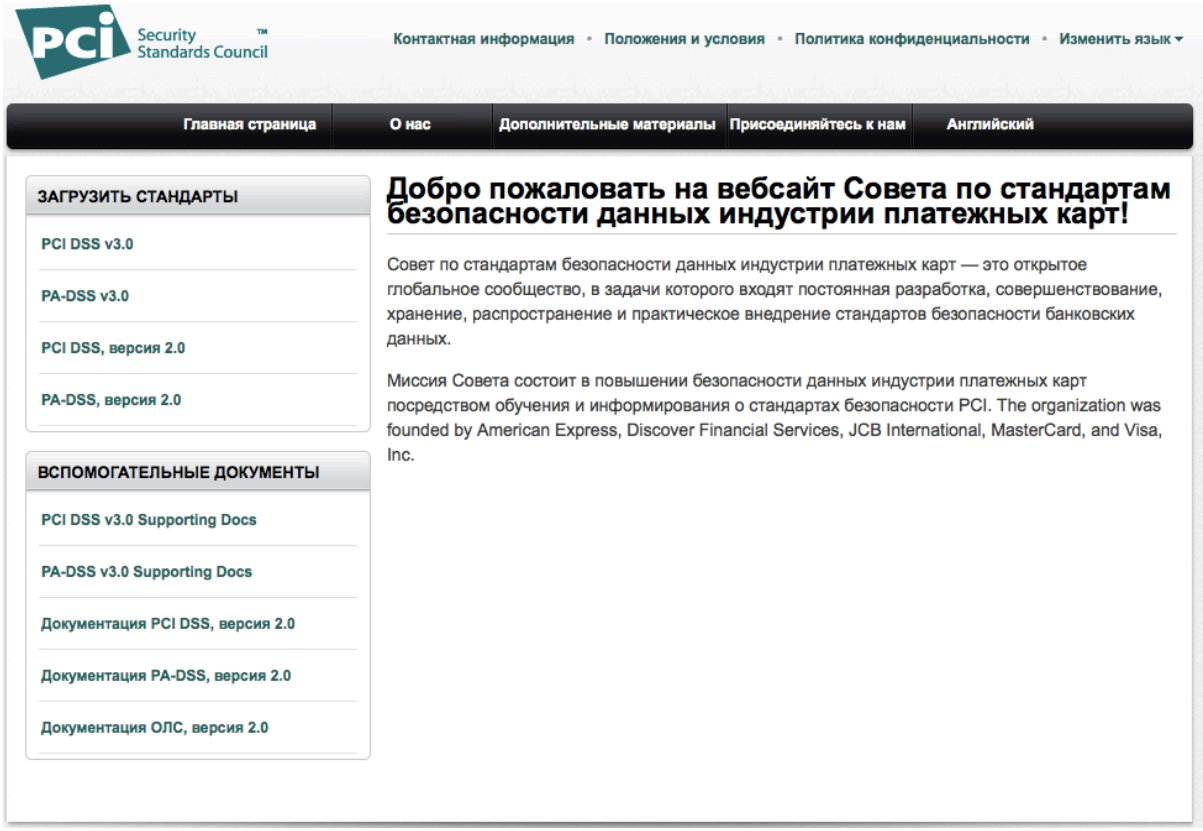
- По мнению ДНПС опасения по поводу 9-й статьи пока не сбылись и уже не сбудутся
- Проблемы с правоприменительной практикой остаются
  - Блокирование средств (если только не в рамках 115-ФЗ)
  - Возврат средств
  - Обмен информацией о мошенниках
  - Невысокая квалификация судей и следователей
- У Сбербанка интересный опыт применения различных статей УК РФ в части наказания мошенников и нарушителей

Саморегулируемая организация



За кадром

- Перевод PCI DSS 3.0 и PA DSS 3.0 на сайте PCI Council
  - ru.pcisecuritystandards.org



Особенности выступлений: ничего не поменялось

- Непонимание потребностей целевой аудитории со стороны интеграторов и производителей
- Непонимание банковской специфики аудитории со стороны интеграторов и производителей
- Неумение выступать публично
- Выступление не на оговоренную ранее тему
- Незнание интеграторами и производителями СТО БР и 382-П и отсутствие хоть какой-нибудь привязки своих решений к банковским стандартам
- Голимая реклама

security-request@cisco.com

Благодарю вас за внимание