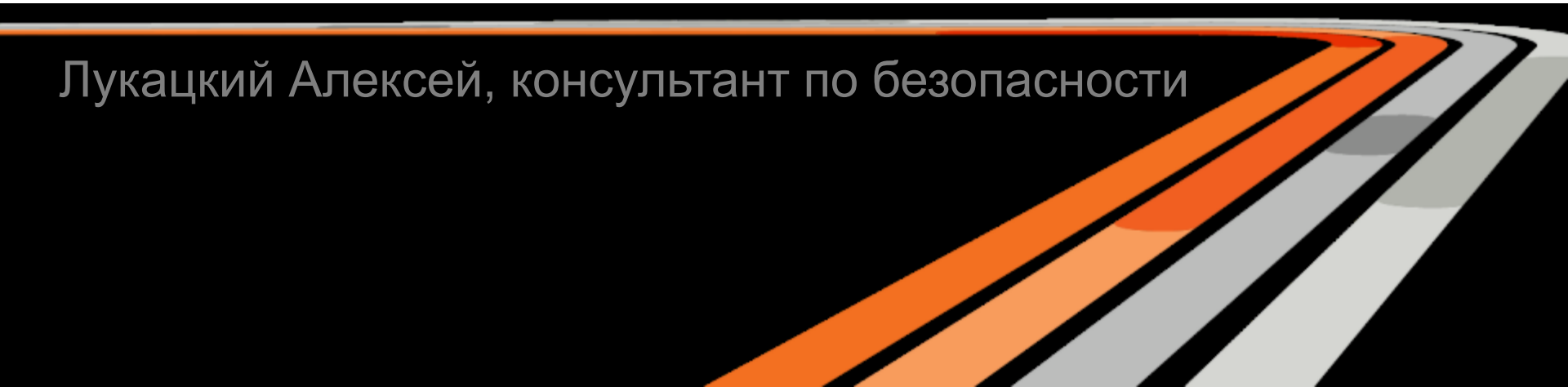
Learn. Connect.
Collaborate. together.

5 дней Уральского форума за 15 минут!

Лукацкий Алексей, консультант по безопасности



Кратко об Уральском Форуме

- +20% банков, участвующих в форуме
- 4 насыщенных дня контента
- 66 докладов
- ВПЕРВЫЕ 6 мастер-классов
- ВПЕРВЫЕ Круглый стол с регуляторами
- ВПЕРВЫЕ Доклады о смежных, но интересных темах для безопасников
- Выступления от всех основных регуляторов по ИБ
  - Банк России, ФСТЭК, ФСБ, РКН, МВД
- Выступления от основных отраслевых организаций
  - АРБ, НП НПС, АБИСС
- Выступления от всех основных департаментов Банка России
  - ГУБиЗИ, ДРР, ДИС (МЦИ), Главная инспекция КО, ДБР

КРАТКИЕ ИТОГИ: РЕГУЛЯТОРЫ

Кратко о регуляторах

- 91% банков занимаются ИБ, чтобы отчитаться перед регуляторами
  - Исследование АРБ по ИБ
- ЦБ и ФСФР сливаются – это накладывает свои особенности на срок и содержание выпускаемых документов Банка России
- Существует определенный конфликт по некоторым вопросам между ГУБиЗИ и ДРР
- Существует непонимание между ЦБ и банками по вопросам ст.9 ФЗ-161
  - Регуляторы не готовы вносить изменения в законодательство

Новости ФСТЭК

- Проект приказа ФСТЭК прошел все технические согласования
  - Сегодня должен быть подписан директором ФСТЭК и отправлен в Минюст на регистрацию
- ФСТЭК завершает разработку документов по защите виртуализации и облачных вычислений
- ФСТЭК работает над документами по защите беспроводного и удаленного доступа
- Идет работа с ФСБ и Минкомсвязи по определению границ сетей организаций и операторов связи с целью разделения ответственности и формированию единого пространства доверия

Новости РКН

- Число нарушений при проверках снижается
- 2 классических нарушения банков ФЗ-152 - работа с коллекторами и рассылка рекламы в нарушение требований ФЗ-152
- Проект приказа по обезличиванию РКН сейчас согласуется с ведомствами
  - Срок утверждения не определен
- Проект приказа по «адекватным странам» в стадии завершения

Новости ГУБиЗИ

- Развитие СТО БР ИББС продолжится
- Готовится обновленная отраслевая модель угроз по ПДн
  - Будет обсуждаться широко, с привлечением банковского сообщества
- Готовится обновление СТО БР в части ПДн
  - Будет переподписано «письмо шести»
- Готовится новая РС «Ресурсное обеспечение информационной безопасности»
  - Как объяснить руководству/акционерам, зачем нужна ИБ и сколько тратить?
- Готовится новая РС «Требования к банковским приложениям и разработчикам банковских приложений»
  - Минимальный набор требований к приложениям

Новости ГУБиЗИ

- Готовится новая РС «Управление инцидентами информационной безопасности»
  - Не просто реагирование, а весь жизненный цикл инцидента
  - Дополнит методичку АРБ и НПС
- 3 новых РС будут рассматриваться в ТК122 в первом полугодии 2013, чтобы к концу года иметь уже готовые и согласованные документы
- В дальней перспективе - требования по облакам и виртуализации, мобильный доступ, DLP с банковской спецификой, пересмотр методики оценки в СТО БР ИББС, кросс-отраслевые стандарты с операторами связи по формированию «пространства доверия»
- По срокам оценка соответствия в СТО БР и 382-П (3 и 2 года соответственно) будут синхронизированы

Новости ДРР

- Ответственность за мошенничество пока регулируется в рамках ЗоЗПП и договорных отношений
  - Пока не принята 9-я статья ФЗ-161
  - Банк должен сначала провести расследование мошеннической транзакции, а потом уже решать вопрос с возвратом средств. Не торопитесь!
  - 9-я статья – большая проблема для банков, но не для ЦБ
- Как информировать клиентов об угрозах?!
  - Колоссальная проблема
- Сертификация систем ДБО и финансовых приложений по вопросам ИБ
  - Вероятно при АБИСС

Новости ДРР

- Краткие итоги отчетности по 2831-У
  - 50% - это мошенничества (фрод)
  - 15% - сбои и ошибки персонала
  - 7% - компрометация ключей ЭП
  - 7% - подмена экрана
  - 0.7% - Отказ в обслуживании
- В перспективе - регулирование ДБО и ЭСП, совершенствование отчетности, новые документы по ИБ, требования к разработчикам ДБО и ЭСП
- Будет меняться отчетность по инцидентам
  - Будет уточняться и детализироваться
  - Будут расширяться объекты инфраструктуры
  - Будет вводиться сумма ущерба по инцидентам

Новости ДРР

- Отчетность по инцидентам с платежными картами скорее всего будет разработана в конце 1-го квартала 2013 года
  - Ввод с 1-го апреля
- Разрабатываются методические рекомендации по однозначной интерпретации 382-П
  - Разработка ведется вместе с сообществом
- Разработана методика пересчета показателей 382-П к показателям, используемым в надзорной деятельности Банка России
- Доработки 382-П
  - Устраняются технические погрешности
  - Устанавливаются сроки и требования по хранению информации, требуемой правоохранительным органам
  - Уточняются требования к аудиторам и оценщикам 382-П

Новости ДРР

- Разработан проект методики для надзора ЦБ по проверке 382-П
- Доработки 2831-У
  - Детализация классификации инцидентов
  - Введение суммы похищенных и намеченных к хищению средств

Спорные темы

- Сертификация систем ДБО и финансовых приложений по вопросам ИБ
- Рейтинг банков по уровню надежности с точки зрения ИБ
- Передача банковских информационных активов на аутсорсинг и в облака
- Если в рамках НПС встречается обработка ПДн, то приоритет у ФСТЭК и ФСБ, а не у ЦБ с его требованиями
- Будущее статуса PCI DSS в контексте требований ИБ НПС
  - Перевод PCI DSS на русский язык будет закончен к 1-му апреля

Новости аутсорсинга и публичных облаков

- Если банк передал на аутсорсинг свою ИТ и ИБ, то аутсорсера ЦБ не может проверить
  - Все должно решаться договором между банком и аутсорсером (Инспекция)
  - Статью 26 о передаче банковской тайны в случае с облаками и аутсорсингом никто не отменял (ГУБиЗИ)
  - У банка передавшего на аутсорсинг или в облако свои ИТ-активы будут проблемы в рамках надзора на 100% (ГУБиЗИ)
- Основные претензии Банка России к передаче банковской тайны организациям, ее не имеющим, и к публичным облакам
- ГУБЗИ сформировал предварительный перечень угроз облачной среды
  - Насчитывает 13 наименований

ВЕНДОРЫ, ИНТЕГРАТОРЫ И БАНКИ

Из интересного и активно упоминаемого

- Построение Security Operations Centers
- Защита мобильных устройств и удаленный доступ
- СКЗИ для мобильных устройств
- Несертифицированные СКЗИ
  - ФСБ считает, что возможно, но есть куча «но»
- Анализ качества программного обеспечения
- О терминальном доступе практически никто не упоминает
- Federated Identity в крупных организациях
- Электронная подпись и аутентификация
- Создание доверенной среды ДБО
  - ВНИИ ПВТО, Актив, Код Безопасности, Потанин
- Антифрод

Особенности выступлений

- 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
- Воровство иллюстративного материала у других компаний

security-request@cisco.com

Благодарю вас за внимание