Уральский форум за 15 минут

Алексей Лукацкий
Бизнес-консультант по безопасности

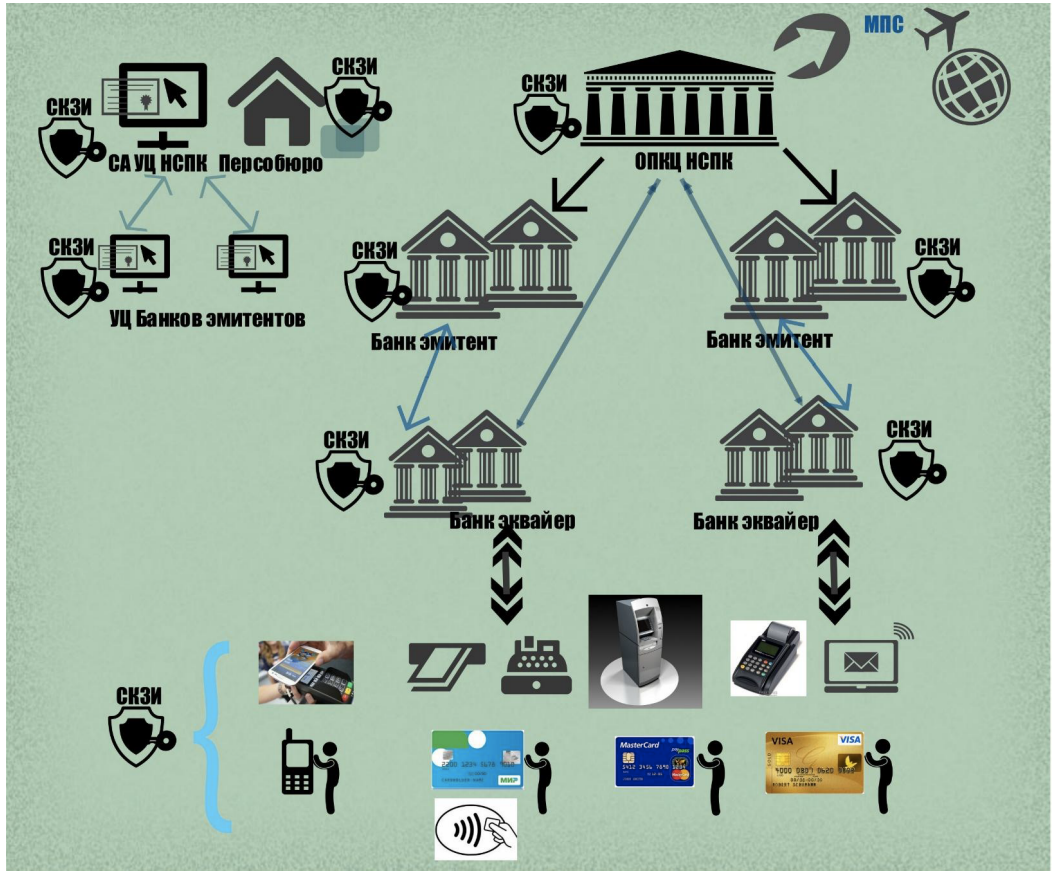
Посвящается всем, кому надо отчитаться за командировку и кто прогулял #ibbank

Число и спектр угроз растет

- Вредоносный код
- Санкционная тематика (для крупных игроков рынка)
- Смещение вектора атак на банк и АБС, а не на клиентов
  - Атаки на АРМ КБР
- DDoS
- Перспектива: Поиск и вербовка инсайдеров
- Перспектива: Проработка схем и технологий монетизации атак на биржи и страховые компании
- Перспектива: Поиск уязвимостей в платежных системах мобильных операторов

Планы ФСБ

- Разработана детальная модель угроз применения импортных HSM в НСПК
- Утвержден план поэтапной замены импортных HSM на отечественные
- На втором этапе планируется внедрение отечественных криптоалгоритмов на карте «Мир»
- Разработка отечественных аналогов стандарта PCI HSM, правил встраивания и аудита выполнения этих требований
- Сотрудников ФСБ не было на мероприятии и поэтому мы не услышали про планы интеграции FinCERT и ГосСОПКА



ФСБ: ответы на вопросы

- К 01.06.2016 будет подготовлен ответ на поручение Президента. Либерализации и усиления запретов по части иностранной криптографии не будет. Там совсем про другое (государственный УЦ???)
- Сейчас финализируются новые и открытые требования к СКЗИ. Они и будут применяться в рамках ЕАЭС
- Нестыковка требований по антивирусной защите в 49-Т и требований к СКЗИ в новых требованиях ФСБ устранена. Возможно применение несертифицированных антивирусов на СКЗИ
- Для устранения сложностей с вывозом СКЗИ за пределы РФ лучше сразу включать эту возможность в ТЗ разработчикам
- Чтобы клиент не страдал в случае внедрения СКЗИ с оканчивающим действие сертификатов ФСБ (3 года) надо сразу включать в договора на поддержку продление сертификата

НСПК, МПС, PCI DSS

- Регулировать технические вопросы защиты данных платежных карт ЦБ отдельно не будет
  - Но в новой редакции 382-П в разделе про платежные карты включен пункт о применимости международных стандартов, если они утверждены правилами международной платежной системы
- НСПК готовит свой документ по защите данных карты «Мир»
- Требований по ИБ к чипам платежных карт, а также к системе (протоколам) подтверждения платежей в электронной коммерции (3D Secure) в России нет – никто никогда про это не думал
  - Сейчас задумались
- Признания PCI DSS в России не будет

Персональные данные

- Указание Банка России от 10 декабря 2015 года №3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных»
  - 10 угроз
  - Повторно направлено в Минюст на регистрацию
- К вопросу актуализации «письма шести» Банк России вернется после регистрации Указания 3889-У в Минюсте
- РКН не видит проблемы в агрегировании ПДн клиентов банков из разных источников, включая и социальные сети. Клиент сам дает согласие на доступ к своим ПДн всех желающих. И вообще это проблема не РКН, а Минкомсвязи
- РКН придет ко всем крупным банкам в части ФЗ-242. Никаких рекомендаций нет – ждите
  - ЦБ рекомендует хранить как минимум копию БД кредитной организации в России

Некредитные финансовые организации

- Разработаны проекты стандартов:
  - Обеспечение информационной безопасности некредитных финансовых организаций. Общие положения (СТО БР ИБНФО Б-1.0)
  - Обеспечение информационной безопасности некредитных финансовых организаций, соответствующих критериям отнесения к малым предприятиям и микропредприятиям (СТО БР ИБНФО М-1.0)
- Разработка указанных проектов стандартов осуществлялась на основе СТО БР ИББС-1.0-2014
  - Организована работа по согласованию проектов стандартов
- Отличия
  - СМИБ
  - Модели угроз и нарушителей
  - Обработка ПДн
  - Проведение оценки соответствия

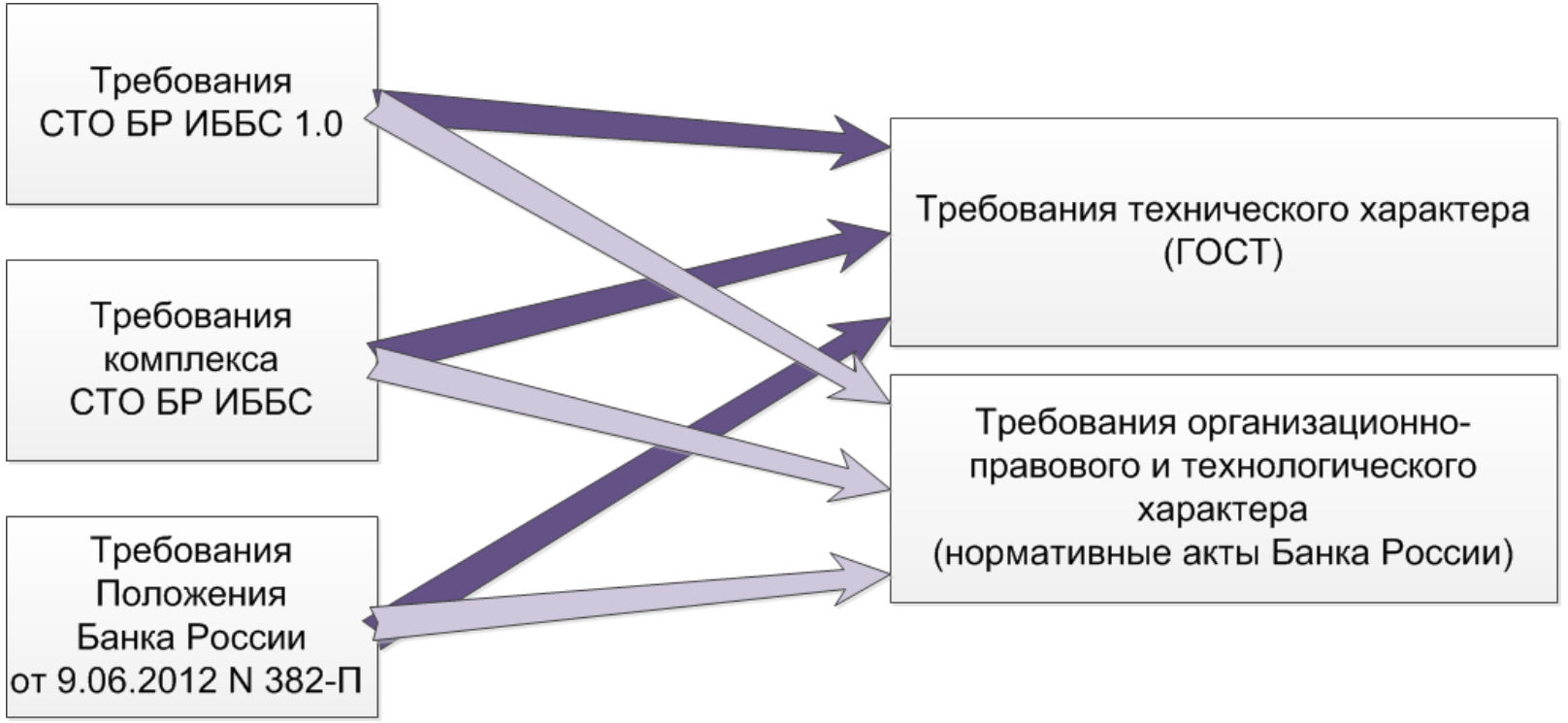
Новая редакция 382-П

- Основные изменения:
  - Установление правил организации работ и оценки соответствия автоматизированных банковских систем и приложений, применяемых в национальной платежной системе
  - Формирование правовой основы для применения средств, обеспечивающих разделение контуров подготовки и подтверждения поручений на осуществление перевода денежных средств
  - Возможна альтернатива – путем введения ряда ограничений на перевод денежных средств
- Планируется к вводу в действие в первой половине 2016 года
  - В части оценки соответствия вступает в силу по истечении 360 дней со дня опубликования
  - В части разделения разделение контуров вступает в силу по истечении 720 дней со дня опубликования
- Изменение идеологии
  - Исключение технических вопрос обеспечения информационной безопасности
  - Установление нормативных ссылок на ГОСТ (ГОСТ будут обязательны к применению)
  - Установление только технологических и организационных требований

От ОСТа к ГОСТу

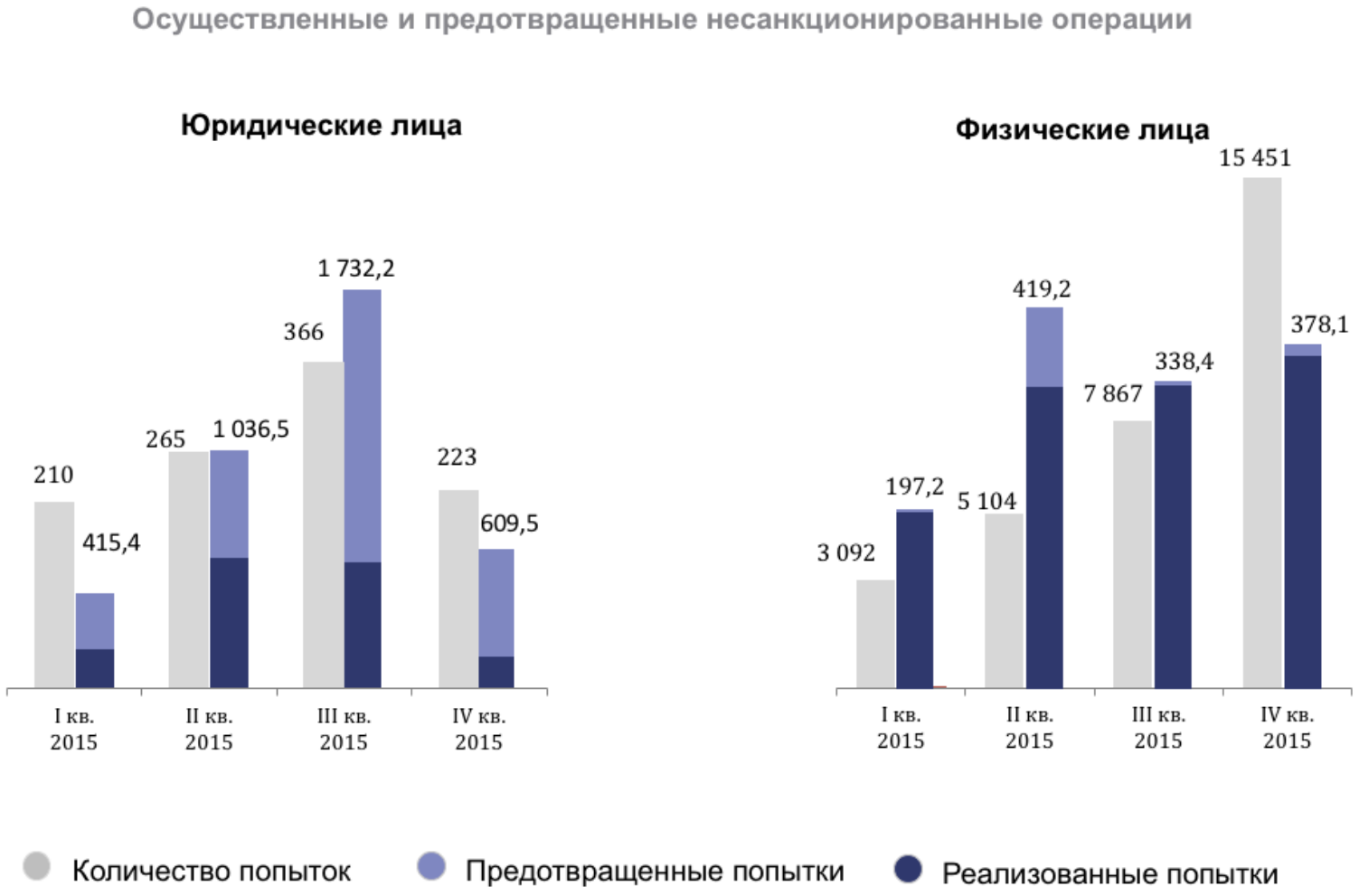
- Планы: Обеспечить наличие национальных стандартов, регулирующих технические вопросы обеспечения информационной безопасности в организациях кредитно-финансовой сферы

  Сроки – 2-3 года



Отчетность

- Результаты по 203-й форме отчетности опубликованы не будут
  - Частично это делает FinCERT
- О гармонизации 203-й и 258-й форм ни слова
- Были прецеденты, когда результаты оценки по 202-й форме недействительными
- Отчетность по СТО БР в будущем отомрет



FinCERT

- Принцип работы – 2Д (Доверие и добровольность)
  - Пока присоединение к работе FinCERT осуществляется на добровольных началах
  - 203 кредитных организации присоединились (по состоянию на 15.02.2016)
  - 76% присоединившихся банки пассивны
- Использование ГОСТа ФСТЭК по описанию уязвимостей
- Планы: создание системы противодействия хищениям денежных средств (Антифрод)
  - I этап - для АРМ КБР
- Планы: взаимодействие с КЦ национального домена сети Интернет
- Планы: Усиление технической экспертизы в части расследования инцидентов

Оценка соответствия

- Поручение Совета Безопасности РФ в начале 2015 года

  ФСТЭК, ФСБ и Минкомсвязь сначала посчитали, что ничего не надо, потом изменили свое мнение, но конкретных предложений пока не дали

- Планы: сформировать «Систему сертификации» и реализовать совместно с ФСБ и ФСТЭК в части обеспечения ИБ в поднадзорных Банку России организациях кредитно-финансовой сферы

  Как будет выглядеть система оценки соответствия пока никто не знает. Возможно интегральный показатель (ущерб + уровень соответствия) и привязка к экономике (например, снижение показателя достаточности капитала при должном уровне обеспечения ИБ)

- Обязательность

  Либо внесение поправок в закон о техническом регулировании, либо уходить под статью 5 ФЗ-184, либо через Постановление Правительства

  Обязательная сертификация проблемы не решит – это нецелесообразно. ЦБ хочет контролировать процесс, но пока непонятно как

Контроль и надзор

- Планы: реализовать систему надзорных мер, учитывающую результаты контроля информационной безопасности
- ДНПС планирует во второй половине 2016 года выпустить «Рекомендации по обеспечению устойчивости инфраструктуры финансовых рынков к угрозам кибербезопасности» (в развитие Письма Банка России №94-Т)
  - Корпоративное управление
  - Идентификация
  - Защита
  - Обнаружение
  - Реагирование и восстановление
  - Тестирование
  - Ситуационная осведомленность
  - Обучение и совершенствование

Что еще?

- Планы: модификация АРМ КБР с целью усиления мер по обеспечению ИБ
- Планы: законодательно закрепить право Банка России по нормативному регулированию вопросов, связанных с обеспечением информационной безопасности всей информационной инфраструктуры кредитной организации и всех видов информации, обрабатываемой в кредитной организации, в том числе информации, отнесенной к категории банковской тайны
  - По аналогии с 27-й статьей ФЗ-161 «О национальной платежной системе»
- Планы: законодательно закрепить основы деятельности по антифроду
  - Законопроект находится в Министерстве финансов Российской Федерации
- Планы: РС по квалификации персонала

Благодарю за внимание