Противодействие мошенничеству в системах ДБО: Кто виноват и что делать? Попытка исторического анализа

Андрей Грициенко, независимый эксперт

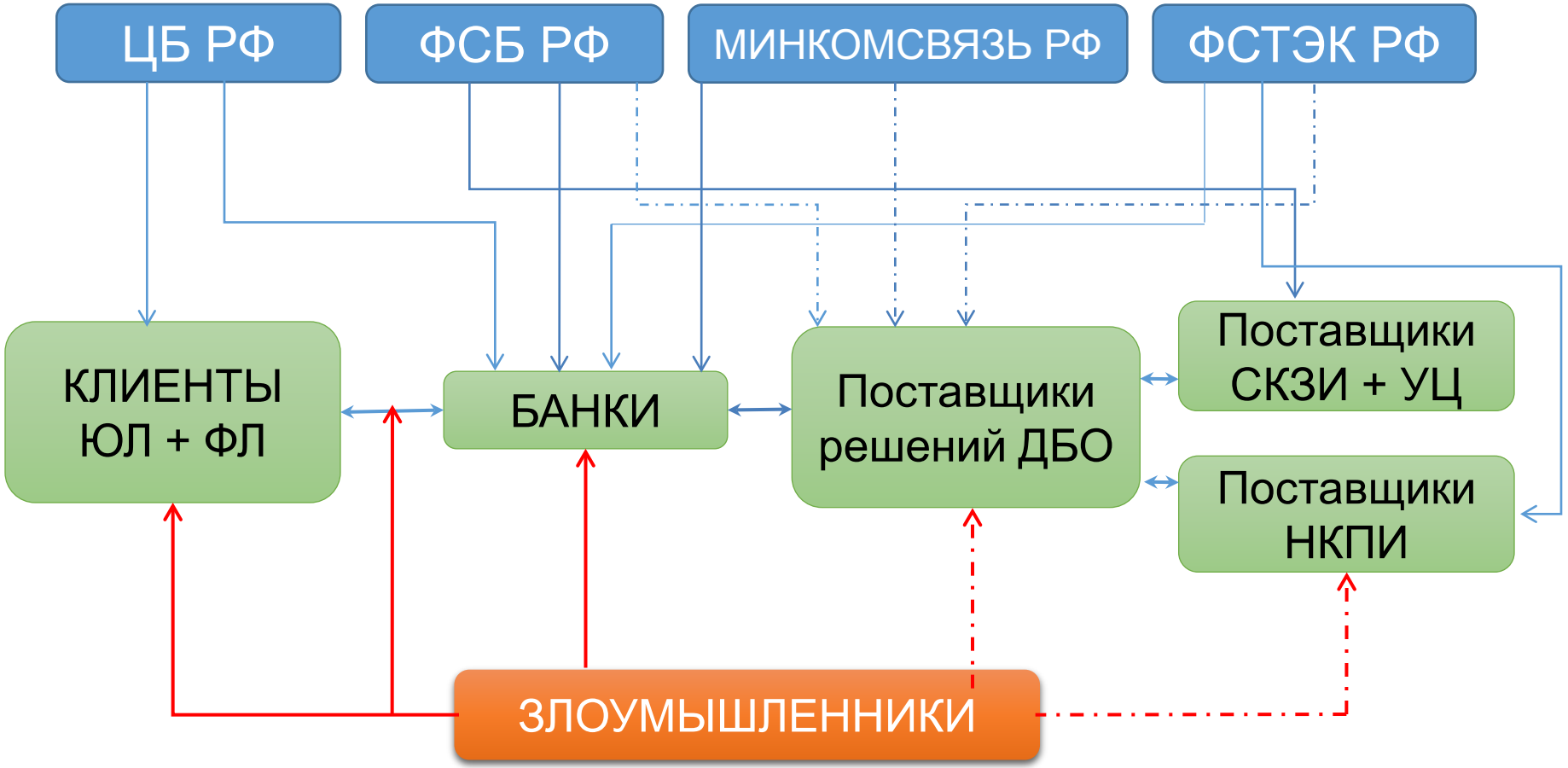
15 февраля 2018 года

Почему необходим ретроспективный анализ?

От I Форума до X

- Трансформация Модели нарушителя
- Развитие технологий и сервисы дистанционного предоставления банковских услуг
- Выводы

Концептуальная схема проблем в системах ДБО



Трансформация модели нарушителя 2009 год

Глава 28 УК РФ: правоприменительная практика

Евгений Аникин: доказано похитил $10 млн у RBS – 5 лет условно

Игорь Блинников: взломал щит на Садовом кольце и крутил там порнографию – 6 лет колонии

Михаил Гаврилов: похитил с клумбы 20 кустов роз и 15 кустов лилий – 2 года строгого режима

Общество недопонимает опасности компьютерной преступности

Трансформация модели нарушителя

Как мы видели модель нарушителя в 2009 году

- Локальные, сравнительно немногочисленные, национальные группы кибермошенников
- Низкие риски наказания и вопиющая бездеятельность правоохранителей
- Главная цель – клиентский АРМ
- Пониженная «социальная ответственность» производителей банковского ПО за киберустойчивость своих продуктов
- Высокие лимиты на снятие наличных в АТМ
- Отсутствие контроля за открытием дроп счетов
- Практически полное отсутствие нормативно-правовых документов, регулирующих ИБ платежных сервисов и систем

Мошенникам удается успешно завершить почти каждое вторую попытку хищения

Трансформация модели нарушителя

Клиент среднего и малого бизнеса — «слабое» звено системы ДБО

Клиент среднего и малого бизнеса – самый значимый Клиент для розничного банка – «слабое» звено системы ДБО

- **Экономит на персонале**
- **Экономит на компьютере**
- **Экономит на лицензионной ОС**
- **Экономит на антивирусах и МСЭ**

Трансформация модели нарушителя

2018 год – ЗОЛОТЫЕ ДЕНЁЧКИ ДЛЯ МОШЕННИКОВ

5 лет тому назад мы предупреждали банковское сообщество об опасности почивать на лаврах достигнутого!

Мошенничества в банковской сфере примут комплексный характер и будут включать в себя:

- Кибермошенничества;
- Методы социальной инженерии;
- Эксплуатацию уязвимостей нормативной правовой базы и законодательства;
- Расширение спектра атакуемых АБС и сервисов;
- Разобщенность в действиях федеральных министерств и ведомств;
- Отсутствие единого центра противодействия мошенничествам

ТАНДЕМ

Положение Банка России №382-П от 9.06.2012г. «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

Указание Банка России №2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств»

Трансформация модели нарушителя

Как мы видим модель нарушителя в 2018 году

Украсть один раз 100 миллионов злоумышленникам проще, нежели чем украсть сто раз по 1 миллиону

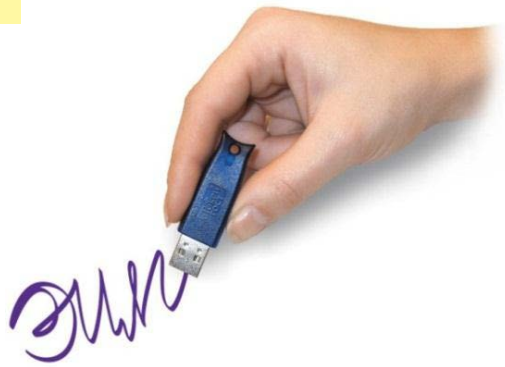
- Хорошо организованные высокопрофессиональные международные группы кибермошенников с ОЧЕНЬ большими финансовыми возможностями
- В роли заказчиков могут выступать государственные структуры иностранных государств
- Разделение обязанностей. Строгая конспирация. Юридическое обеспечение. Активное противодействие правоохранительным органам. Организация акций прикрытия.
- Главная цель – АБС банков, клиентский АРМ, банковские терминальные устройства, АТМ и мобильные устройства
- Активное использование социальных сетей для ведения разведки, обмена опытом и отмывания денег
- Отмывание денег с использованием криптовалют

Проблемы недоверенной среды на АРМ Клиента СМБ

Как получить квалифицированную электронную подпись Клиента, если:

1. Клиент работает в недоверенной среде?

2. Клиент на всем экономит?



Проект “Защищенный компьютер” под брендами Kraftway (РФ) и Fujitsu (Япония)

1. Собственный дизайн архитектуры и материнской платы
2. BIOS – в исходниках, удалены “проблемные” зоны
3. Функции, относящиеся к безопасности, собраны с одном месте – TSM (Trusted Security Module)
4. Собственное сертифицированное производство

ДОРОГО! Очевидно – это не решение для клиента СМБ!

Создание изолированной безопасной среды на АРМ Клиента, которая:

1. Не подлежит изменению клиентом Банка

2. Имеет возможность централизованного управления со стороны Банка

3. Имеет в своем составе предустановленные и настраиваемые средства межсетевого экранирования

4. Имеет возможность запуска только разрешенного ПО

Средства создания изолированной безопасной среды на АРМ Клиента

Check Point GO (Abra)

1. Безопасное защищенное рабочее пространство
2. Изоляция рабочего пространства от хостовой машины
3. Изоляция временных и рабочих файлов
4. Шифрование файлов рабочей среды
5. Блокировка печати
6. Контроль запуска ПО

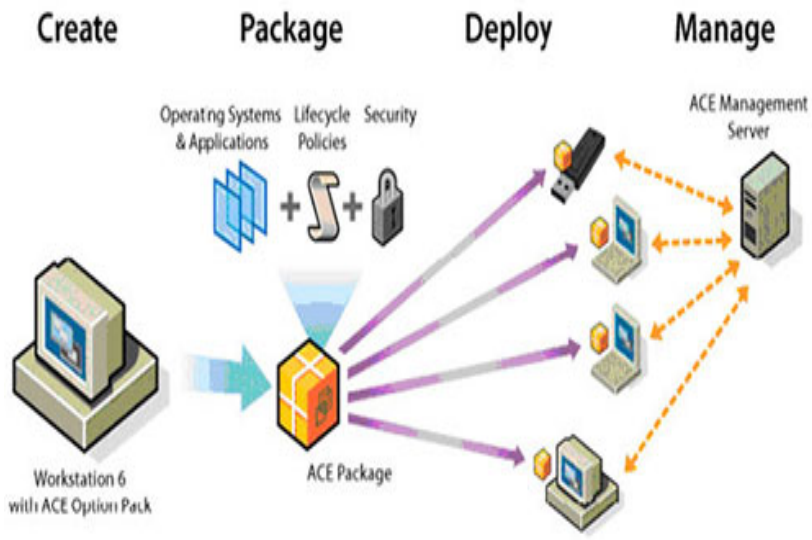
Средства создания изолированной безопасной среды на АРМ Клиента

S-terra Марш

1. Целостность программной среды терминального доступа
2. Изоляция вычислительного процесса
3. Встроенные возможности построения VPN
4. Исполнение в виде флэш-накопителя
5. Встроенный сертифицированный криптопровайдер
6. Встроенная память объемом 4 ГБ
7. Несколько вариантов исполнения – с веб-браузером и клиентом терминального доступа

Средства создания изолированной безопасной среды на АРМ Клиента

VMware Pocket ACE



1. Интеграция с VMware Workstation 6.5
2. Готовый образ виртуальной машины со всем необходимым ПО
3. Изоляция временных и рабочих файлов
4. Блокирование USB и DVD/CD устройств на основании ID
5. Полная виртуализация операционной системы
6. Централизованное управление правилами безопасности
7. Защита от копирования. Управление сроком действия

161-ФЗ от 27.06.2011 «О национальной платежной системе»

Требования №161-ФЗ от 27.06.2011 «О национальной платежной системе» вступающие в силу с 30.12.12:

1. **Статья 9, часть 4. Порядок использования электронных средств платежа**

***Оператор по переводу денежных средств обязан информировать клиента о совершении каждой операции с использованием электронного средства платежа путем направления клиенту соответствующего уведомления* в порядке, установленном договором с клиентом**

2. **Статья 9, часть 13. Порядок использования электронных средств платежа**

В случае, если оператор по переводу денежных средств не исполняет обязанность по информированию клиента о совершенной операции в соответствии с частью 4 настоящей статьи, оператор по переводу денежных средств обязан возместить клиенту сумму операции, о которой клиент не был проинформирован и которая была совершена без согласия клиента

Система «FRAUD-Анализа»

1. Сокращает потери времени на обеспечение взаимодействия между системой «FRAUD-Анализ» и внешними системами, а также гарантирует доставку и безопасность передачи данных

2. Схема функционирования системы «FRAUD-Анализ»:
   - Клиент отправляет платежный документ в банк;
   - платежный документ выгружается из системы ДБО в систему «FRAUD-Анализ»;
   - система «FRAUD-Анализ» проводит проверки по правилам, настроенным банком, и выдает результат.

3. Варианты результата, получаемого по каждому отдельному документу:
   - документ успешно прошел проверку;
   - подозрительный документ, требуется вмешательство оператора
   - документ является мошенническим.

161-ФЗ от 27.06.2011
О национальной платежной системе»

Сервер нотификации

Требования №161-ФЗ от 27.06.2011 «О национальной платежной системе»

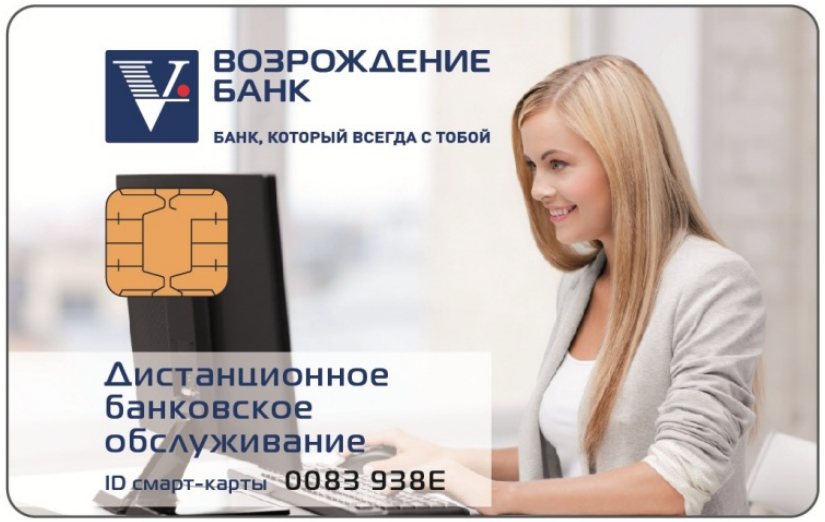
Контроль содержимого подписываемых документов

SafeTouch от компании SafeTech

Contra

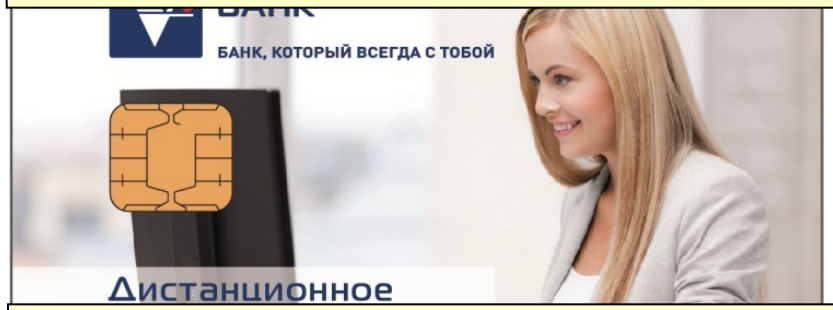
Рутокен PINPad от компании Актив

Использование подсистемы «Token security» от компании BSS



Что обеспечивает подсистема «Token security»:

- **Поддержку системой ЦС ДБО 17.9 совместного решения компаний КриптоПро и SafeTech. Сочетание технологий КриптоПро eToken CSP и считывателей смарт-карт SafeTouch позволяет защититься от всех известных хакерских атак на счета клиентов систем ДБО, в том числе самых опасных – удаленного доступа к компьютеру клиента и подмены платежного документа;**



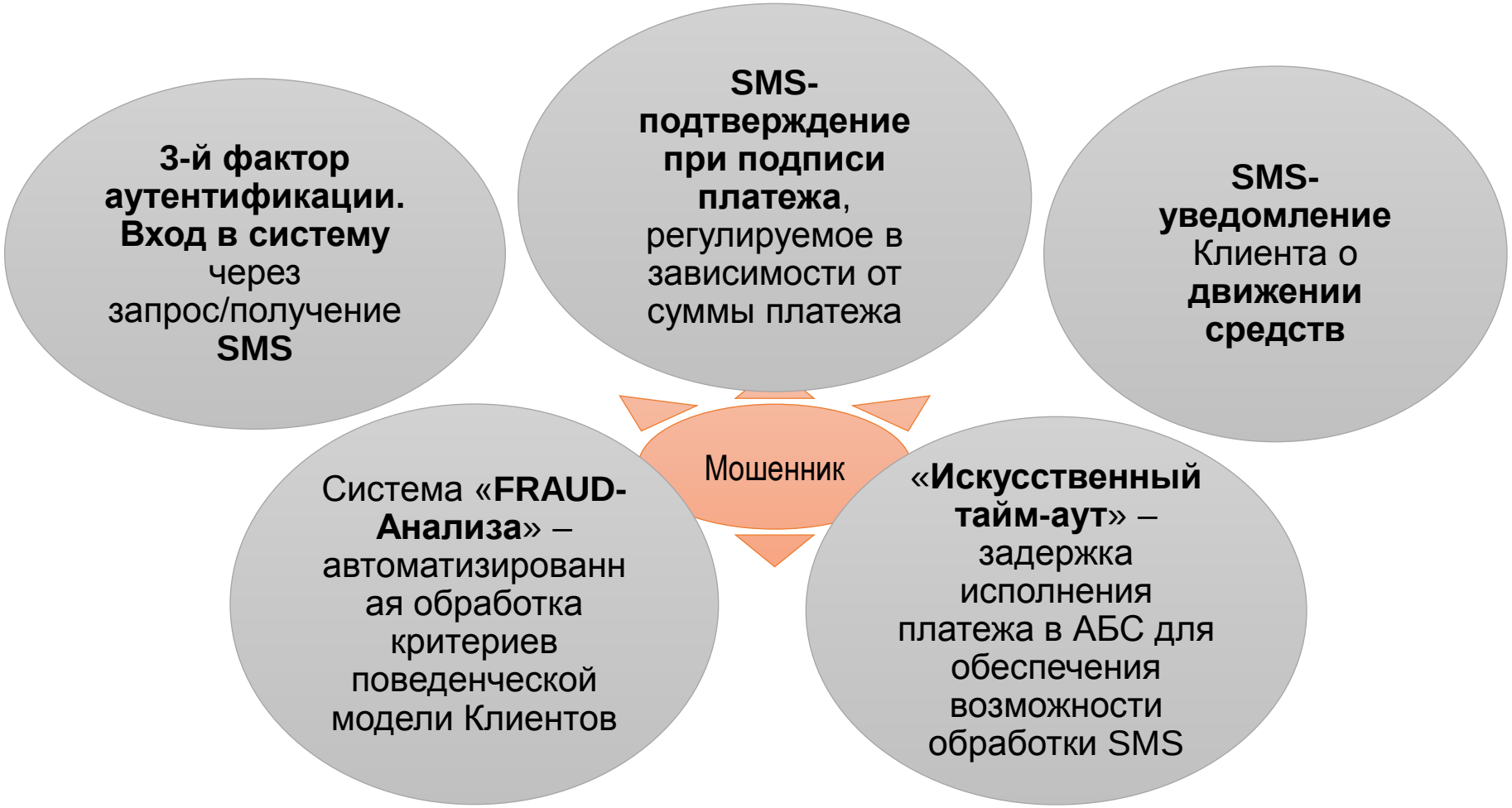
- **Аппаратно-программное СКЗИ КриптоПро eToken CSP реализовано с использованием архитектуры функционального ключевого носителя (ФКН) и обеспечивает безопасное хранение и использование ключей электронной подписи в защищённой памяти смарткарты;**

Что обеспечивает подсистема «Token security»:

Считыватель смарт-карт SafeTouch обеспечивает выполнение требований ст. 12 Федерального закона «Об электронной подписи» от 06.04.2011 № 63-ФЗ к средствам электронной подписи, которые должны:

1) показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
2) создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;
3) однозначно показывать, что электронная подпись создана.

Дополнительные сервисы безопасности



Дополнительный контроль платежей

Краткие выводы

Взрывной рост платежных систем и сервисов дает большие возможности преступникам для мошеннических платежей

Расширяется спектр информационных систем, попадающих в зону интереса мошенников

- Атаки на брокерские системы
- Атаки на POS-терминалы
- Атаки на мобильные устройства и средства бесконтактных платежей
- Атаки на системы электронных торгов
- Атаки на традиционные системы Банк-клиент
- Атаки на клиентские места платежной системы ЦБ

Ограбление банков

Краткие выводы

Применение сертифицированной криптографии становится насущной необходимостью. Никто теперь не может сказать, что финансовые транзакции в РФ не интересны АНБ США, Министерству Финансов США или другим заинтересованным организациям

Правоохранители и законодатели по-прежнему отстают от кибермошенников

Регулятор не стимулирует Банки в должной мере совершенствовать свои системы ИБ дистанционных платежей

На сегодняшний день не существует универсального технического средства (системы), которая в полной мере обеспечила защиту систем ДБО от мошеннических атак.

Только комплексное использование организационно-технических мероприятий в системах ИБ ДБО может обеспечить приемлемый уровень безопасности

Подавляющее большинство банков не имеют собственных Служб ИБ, позволяющих организовать работу по защите платежей на должном уровне

Краткие выводы

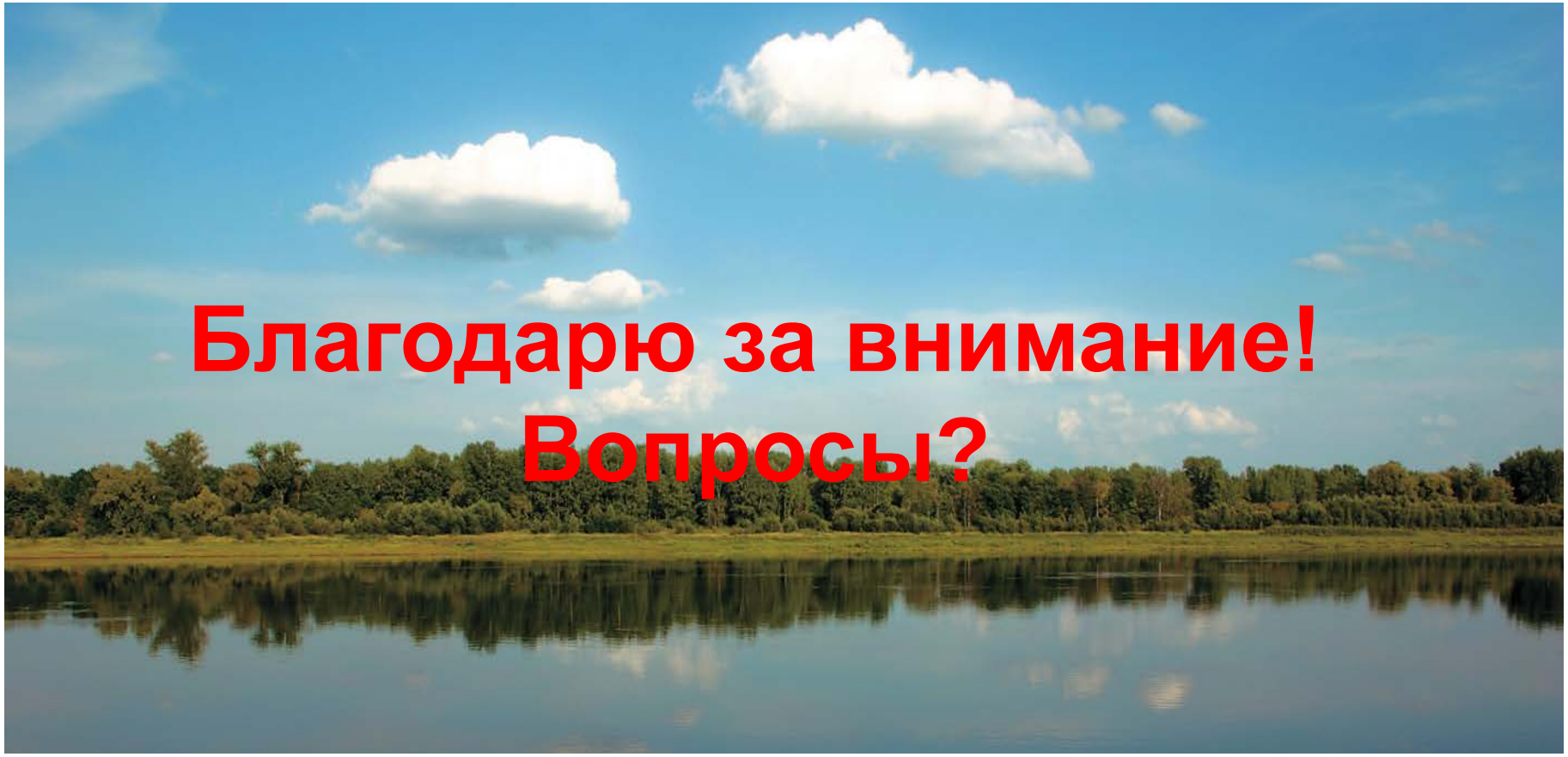
Финансирование расходов на ИБ в банках непрерывно растет, но этого сегодня явно недостаточно.
Применение сложных комплексных решений по обеспечению соответствующего уровня ИБ в платёжных системах требует такого уровня затрат, который явно недоступен большинству банков РФ.

Серьезной проблемой у банков становится комплектование СИБ высококвалифицированными специалистами в области ИБ

Требования новой редакции 382П будут для большинства банков НЕВЫПОЛНИМЫ

АУТСОРСИНГ ИБ ДБО?

Что делать?


Благодарю за внимание!
Вопросы?