Банк Москвы

Что предлагают и что дают вендоры антифродовых систем?

Окулесский Василий Андреевич, к.т.н.
Департамент по обеспечению безопасности
ОАО «Банк Москвы»
Начальник управления

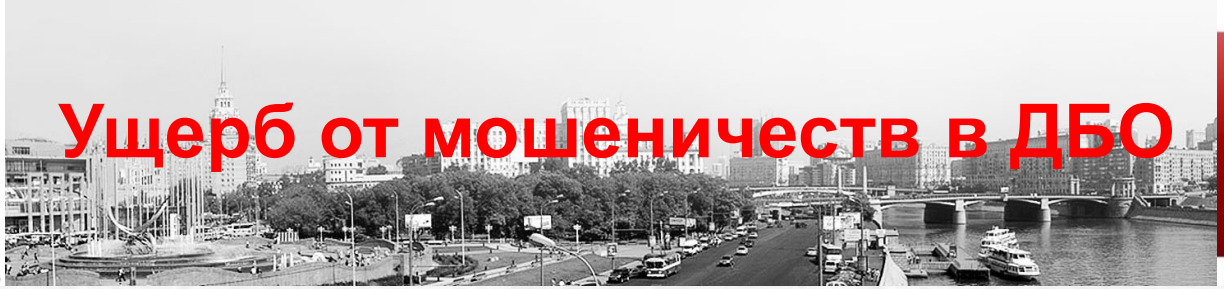
Урал, 2013

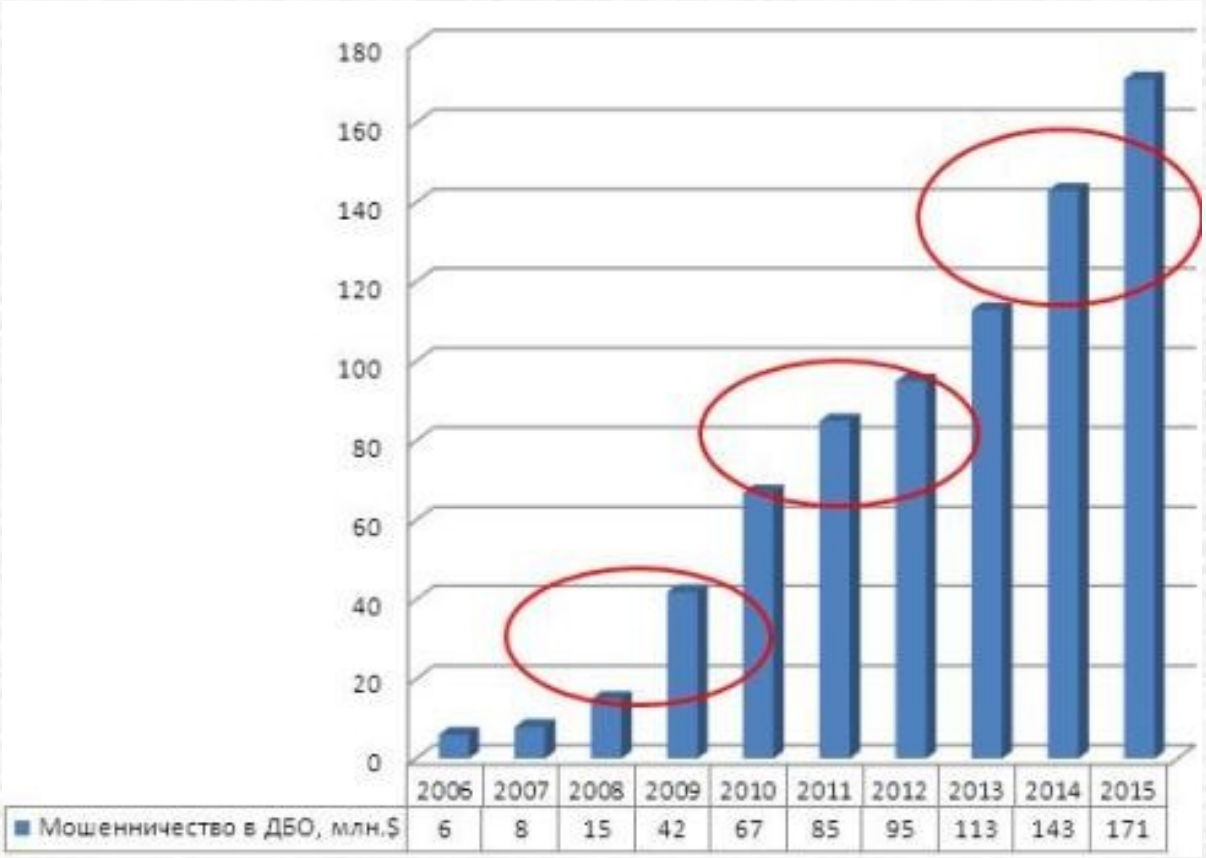
Банк Москвы

Банк Москвы — один из крупнейших универсальных банков России (входит в топ-5), предоставляющий диверсифицированный спектр финансовых услуг как для юридических, так и для частных лиц.
Основным акционером Банка является Группа ВТБ (95,52%). Стратегией развития Банка определено, что Банк Москвы будет развиваться как самостоятельный универсальный коммерческий банк в составе Группы ВТБ. Приоритетной зоной для развития бизнеса Банка являются Москва и Московская область.
В своем развитии Банк Москвы сделает особый акцент на инновационные, высокотехнологичные продукты и сервисы, в том числе одним из приоритетов Банка станет обслуживание субъектов малого и среднего бизнеса.
В настоящее время Банк Москвы обслуживает более 100 тыс. корпоративных и 9 млн частных клиентов. Среди клиентов — юридических лиц — крупнейшие отраслевые предприятия, предприятия среднего и малого бизнеса.
Банк представлен практически во всех экономически значимых регионах страны и насчитывает 285 обособленных подразделений, включая дополнительные офисы и операционные кассы. По состоянию на 1 декабря 2012 года в регионах России работало 155 подразделения Банка. В Москве и Московской области действует 130 офисов Банка. Кроме того, услуги населению оказываются в 474 почтово-банковских отделениях столичного региона.
В сеть Банка также входят 4 дочерних банка, находящихся за пределами России: АО «БМ Банк» (Украина), ОАО «Банк Москва-Минск» (Беларусь), Эстонский кредитный банк (Эстония) и АО «Банк Москвы» — (Белград) (Сербия).
В Банке Москвы действует собственный Процессинговый центр, сертифицированный международными платежными системами Visa International и MasterCard. Банк выпустил более 18 млн пластиковых карт и располагает широкой сетью собственных банкоматов (1,9 тыс. штук). При этом объединенная сеть банкоматов банков Группы ВТБ — Банка Москвы, ВТБ 24 и ТрансКредитБанка — превышает 10 тыс. устройств (в сети отменена комиссия за снятие собственных денежных средств).
Высокую надежность Банка Москвы подтверждают рейтинги международных рейтинговых агентств. Долгосрочный кредитный рейтинг Банка по версии Moody’s Investors Service — Ba2, по данным Fitch Ratings — BBB

Банк Москвы

Ущерб от мошенничеств в ДБО





Источник: Аналитический центр компании "Техносерв", 2012 г.

Подробнее: http://banks.cnews.ru/reviews/index.shtml?2013/02/05/517975

Банк Москвы

Что такое современный Интернет-банкинг

- Рублевые внутрибанковские и межбанковские переводы;
- Осуществление предопределённых платежей (таких как оплата ЖКУ, мобильного телефона, услуг коммерческого телевидения, услуг Интернет-провайдеров и пр.)
- Валютные межбанковские переводы
- Переводы между своими счетами/картами, в том числе с конвертацией из одной валюты в другую
- Возврат перевода
- Различные заявления, в т.ч. об утере/краже карты
- Создание шаблонов и расписаний платежей и переводов
- Просмотр информации о начислении по жилищно-коммунальным услугам, выставленным ГУ ИС
- Просмотр информации и получение выписки по всем открытым в Банке счетам/вкладам/картам
- Получение информации о задолженности по кредитам

Банк Москвы

Почему возможны Интернет - мошенничества

- Недостаточная осведомленность клиентов об опасности использования Интернет - среды для финансовых операциях
- Недостаточное внимание клиентов к обеспечению собственной безопасности в Интернете
- Использование нелицензионного программного обеспечения
- Использование неадекватных уровней безопасности в системах ДБО
- Технологические ошибки в разработке систем ДБО
- Использование в системах ДБО не сертифицированных СКЗИ
- **Отсутствие доверенной среды в на рабочих местах клиентов систем ДБО**

Банк Москвы

Что чаще всего угрожает системам ДБО

- Кража персональных ключевых данных клиентов с использованием троянских программ
- Использование фишинговых сайтов для «добровольного» получения персональных данных клиентов
- Захват управления персональным компьютером клиента
- Использование инсайдерской информации

=

Кража денежных средств клиентов с несанкционированным использованием персональных данных клиентов для управления банковскими счетами

Банк Москвы

Что мы чаще всего используем

- Логин
- Долговременный пароль
- Одноразовый пароль (OTP-token, SMS, скретч-карты и т.д.)
- ЭЦП
- Виртуальная клавиатура
- Технология "каптча"
- Пользовательский индивидуальный интерфейс
- SMS – информирование
- Штатные средства WEB
- Антивирусные средства

Банк Москвы

Что можно сделать еще

Компенсация недостаточного уровня защищенности рабочих мест клиентов

Создание доверенной среды На рабочем месте клиента

Технический путь

Создание системы контентного анализа транзакций

Риск-ориентированное направление

Банк Москвы

Создание системы

1. Формирование профиля клиента
2. Формирование профиля группы типовых клиентов
3. Разработка системы расчета уровня риска проводимой операции
4. Разработка сценариев реагирования на различные уровни риска
5. Создание специального подразделение реагирования и специальной группы анализа и обучения системы
6. Встраивание полученной системы в связку ИБК - АБС

Банк Москвы

Что обещают вендоры

1. Выявление подавляющего числа попыток мошеннических транзакций
2. Реализация возможности проводить расследования и отстаивать интересы Банка и его клиентов
3. Снижение общего числа попыток мошеннических транзакций
4. Сокращение расходов на поддержание безопасности систем ДБО
5. Повышение конкурентоспособности Банка

Поднятие статуса СБ до бизнес-подразделения?

Банк Москвы

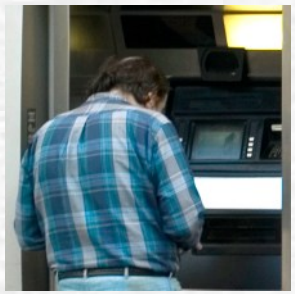
Просто пример
(на базе ArcSight FraudView)

Информационная безопасность банков

Хранилище

Оператор

Клиент



Подозрительная транзакция

Мошенническая транзакция

Легальная транзакция

Credit Cards

Online

Retail

Wholesale

В партнерстве с ВТБ

Банк Москвы

Что не так

1. Большинство систем спроектировано для банков от 1 млн. клиентов (технические, идеологические, лицензионные трудности)
2. Внедрение любой антифродовой платформы требует внесения изменений в существующие системы ДБО и АБС
3. Внедрение любой системы в «боевом» режиме требует создания новой инфраструктуры и нового подразделения
4. Сложности в интеграции уже имеющихся «своих» механизмов первичного фрод-анализа

Банк Москвы

Это мы можем сами

Информационная безопасность банков

1. Контролировать IP-адреса и изменения параметров компьютеров клиента
2. Контролировать «черные» и «белые» списки по номерам счетов корреспондентов
3. Контролировать пороговые значения сумм платежа
4. Контролировать значимые параметры (ИНН, КПП, назначение, сумму и т.д.)
5. Контролировать «новизну» параметров платежа

ЭТО ДАЕТ 80%-ВЕРОЯТНОСТЬ ВЫЯВЛЕНИЯ ФРОДА

Банк Москвы

Тогда зачем?

1. При большом числе (более 10 тыс платежей в день) очень велико число платежей, попадающих под дополнительный «ручной» контроль
2. Велика доля «человеческого фактора» (ошибки) при ручном исполнении большого объема контрольных функций
3. При полуручной обработке невозможно быстро и эффективно применять «тонкую» аналитику по «профилю клиента»
4. В ручном режиме сложно проводить корреляционные оценки в он-лайн режимах контроля

Банк Москвы

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ

Какие будут вопросы?

Контакты:

Окулесский Василий Андреевич, к.т.н.

Тел. (495) 925-8000 доб. 114-58
E-mail: Okulessky_VA@mmbank.ru