ИНФОСИСТЕМЫ ДЖЕТ

Jet infosystems

ЛЕТ

ФОРМИРУЕМ ТРЕНДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кроссканальное мошенничество. Вчера. Сегодня. Завтра

Алексей Сизов,
руководитель направления
противодействия мошенничеству
Центра информационной безопасности

Объемы мошенничества

- ✓ GIB – 2,65 млрд. рублей
- ✓ JET – 8,96 млрд. рублей

По мнению ведущих экспертов эти цифры недооценены в 5-10 раз!

Подробнее о цифрах

62% Атаки в рамках одного канала

30% Атаки, локализованные в разных каналах

8% Не определено

Системная проблема №1

Обеспечить защищенность на стороне клиента практически невозможно

- ✓ **Незащищённость среды**
- ✓ **Глобальная уязвимость софта**
- ✓ **Человеческий фактор или «русский авось»**

Социальная инженерия

- На корпоративный почтовый ящик приходит письмо с темой «Перед офисом на машину упало дерево»
- Внутри письма вместо фотографии находится вредонос

Эффективность схемы атаки

83%

Открыли письмо

Из них:

35% Не имеют собственного автомобиля

23% В этот день либо не были на авто либо стояли на крытом паркинге

Системная проблема №2

Начать заниматься мошенничеством крайне просто

- ✓ **Доступность информации и софта**
- ✓ **Низкие цены**
- ✓ **Прибыль перекрывает невысокий риск**

Цена вируса и цена последствий

350$

Стоит рабочий вирус, не регистрируемый базовым антивирусным софтом

Статистика по реальным срокам преследования

1-3 года

Системная проблема №3

Технологии защиты и контроля отстают от атакующей стороны

- ✓ **Как часто вы слышите от вендора:**
  - ✓ **«Решение этой задачи лежит вне скоупа внедренного решения»**
  - ✓ **Данный функционал будет реализован в Qx**

Подробнее о цифрах

Эффективность защиты:

90% Атаки на ДБО юр.лиц

35% Атаки на ДБО физ.лиц

5% Внутреннее мошенничество

Кроссканал или «невыявленные» риски

- ✓ Может быть кто-то пытается несанкционированно перевести через систему ДБО деньги со счета клиента на свой?
- ✓ Выпускает пластиковую карту для клиента или подключается к ДБО без его ведома?
- ✓ Может быть в банковской системе есть ошибка в расчетах, в результате которой банк недополучает комиссионные доходы от клиентских операций?

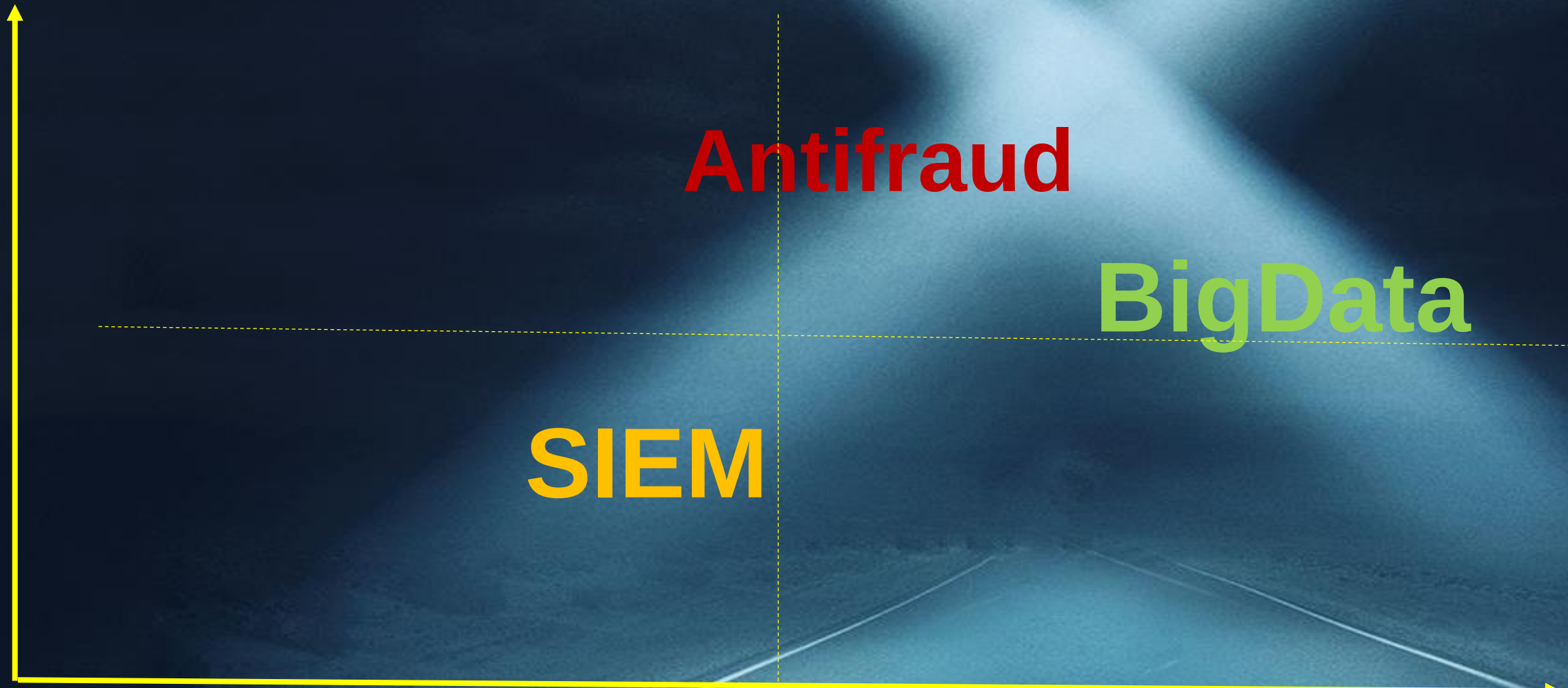
Примеры, как происходит воровство

- ✓ Более 25% банков (и вендоров!) считают внутренние переводы нерискованными
- ✓ Если злоумышленник откроет счет и карту с большим лимитом мошенничество пройдет
- ✓ Около 35% банков не контролируют неплатежные события
- ✓ Что произойдет, если 5 VIP-клиентов зайдут в пятницу вечером с одного IP?
- ✓ Более 65% банков не пересматривают белые списки
- ✓ Таргетированная атака на ДБО юр. лица с целью создания транзита уже реализовывалась неоднократно

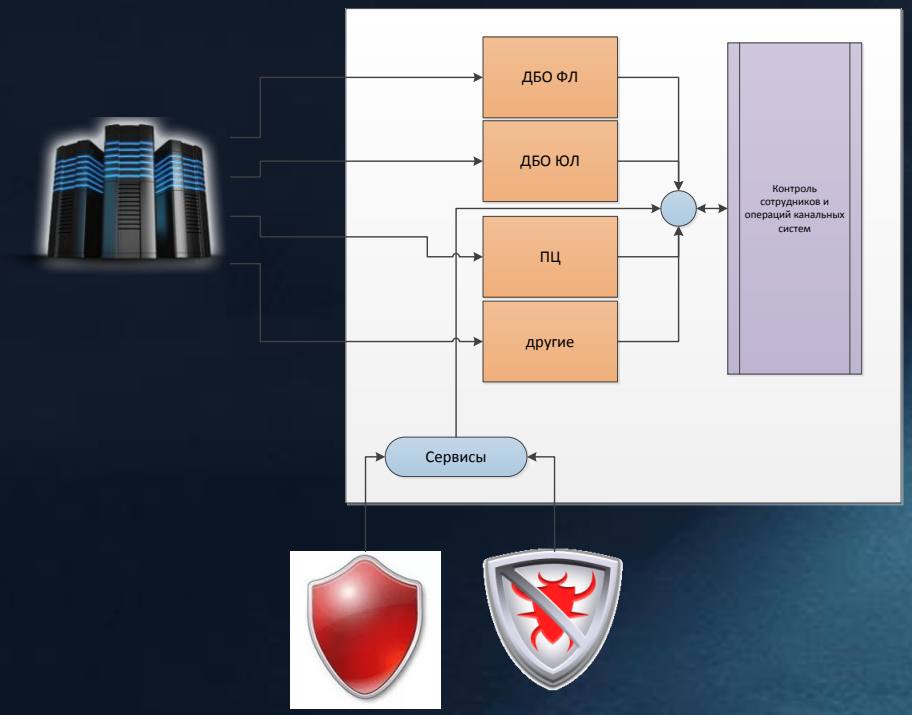
Что есть в рядовом банке для контроля рисков?

- ✓ Контроль операций процессингового центра (требование VIOR)
- ✓ Контроль движения денежных средств по ПОД/ФТ (соответствие 115-ФЗ)
- ✓ Контроль операций ДБО на уровне АБС или наложенными средствами/собственной разработкой (защита от массовых атак на юр. лица)

Технологии

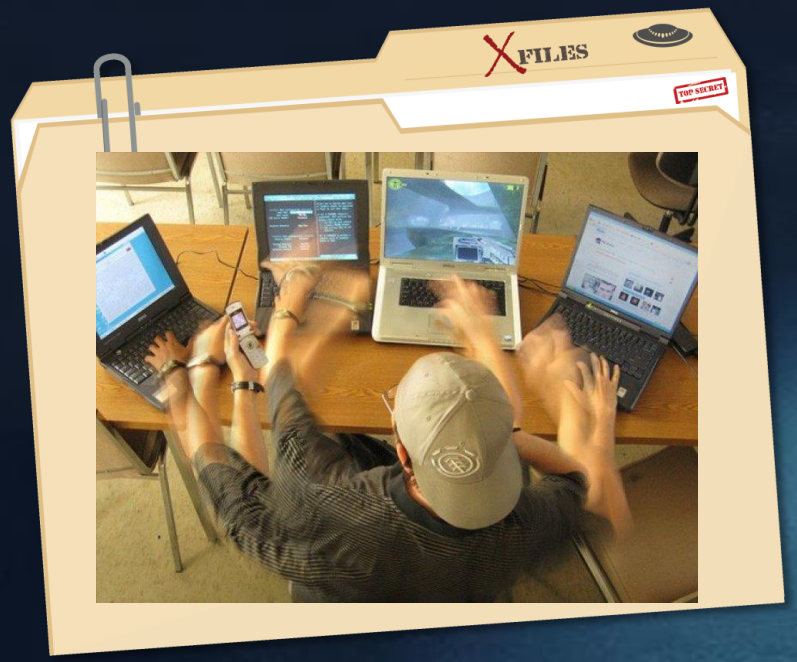


Источники данных



- ✓ ДБО юридических лиц
- ✓ ДБО физических лиц
- ✓ Процессинговый центр (front- и back-системы)
- ✓ АБС (одна или несколько)
- ✓ CRM юридических лиц
- ✓ CRM физических лиц
- ✓ CRM
- ✓ DAM
- ✓ WAF
- ✓ Log-manager или SIEM

Ключевые задачи интеграции



- ✓ Обеспечить механизмы ETL для основных банковских систем
- ✓ Создать подмножество MDM-систем для связывания данных из разных систем ДБО юридических лиц
- ✓ Обеспечить связанную обработку 3-х и более каналов

Серебряная пуля аналитики

- ✓ Общие схемы, уникальные правила
- ✓ Очень сложно настроить обучаемую модель с заданными показателями ошибок первого и второго рода
- ✓ Эффективность может быть выше, чем у канального ДБО, но требуется на порядок больше аналитической работы
- ✓ Решается множество сопутствующих задач

Теперь это доступно оператору

Готовые инструменты работы с данными для анализа

- ✓ Datamining
- ✓ Machine Learning
- ✓ и многое другое

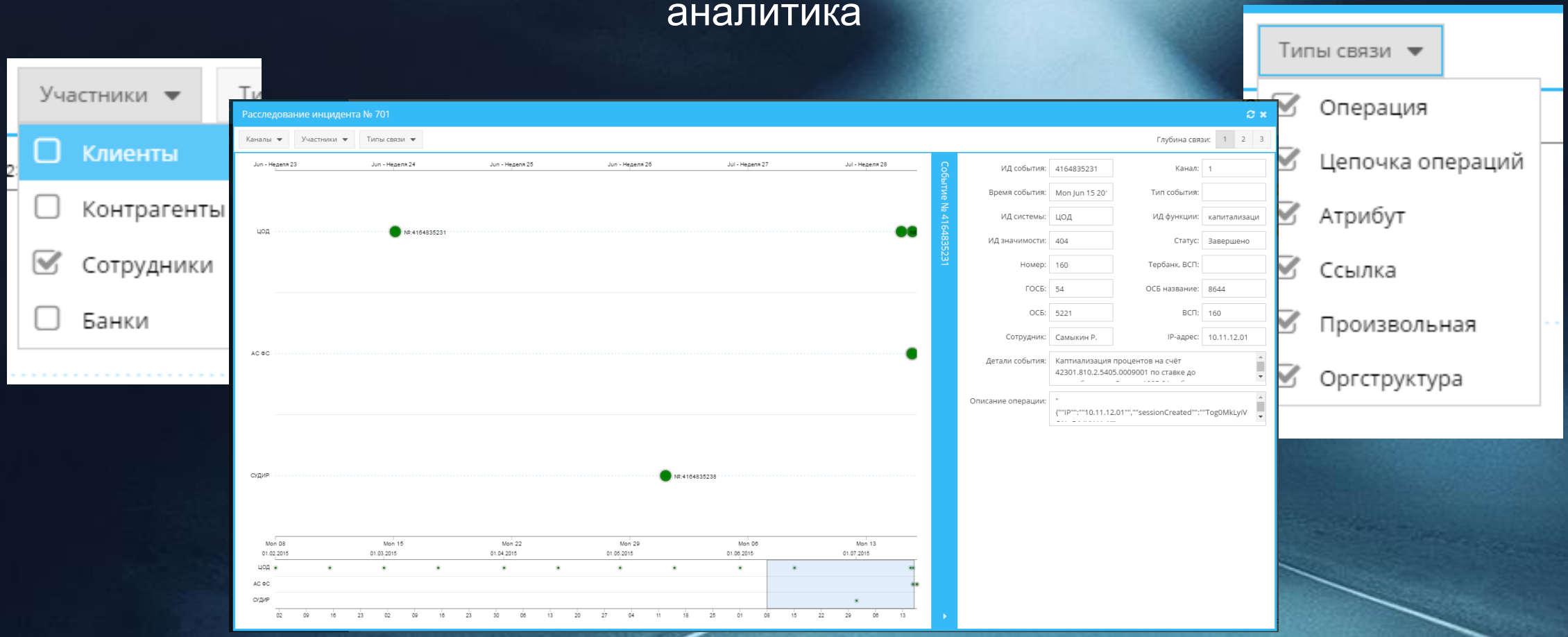
Сегменты контроля

Готовые инструменты работы с данными для анализа

- ✓ Операции РКО/АБС
- ✓ Операции по кредитным продуктам
- ✓ Операции бэк-офиса дистанционных каналов
- ✓ Поиски связей по десяткам метрик
- ✓ Контроль нефинансовых операций
- ✓ Контроль доступов в приложения
- ✓ Контроль казначейства
- ✓ и др.

Требования к верхушке айсберга

Представление данных доступных для оператора и аналитика



Системная проблема №4: коллективная работа

ИНФОСИСТЕМЫ ДЖЕТ

Л Е Т

ФОРМИРУЕМ ТРЕНДЫ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Спасибо за внимание!