ИНФОСИСТЕМЫ ДЖЕТ

Облачный антифрод: почему весь канальный антифрод уйдет в облака

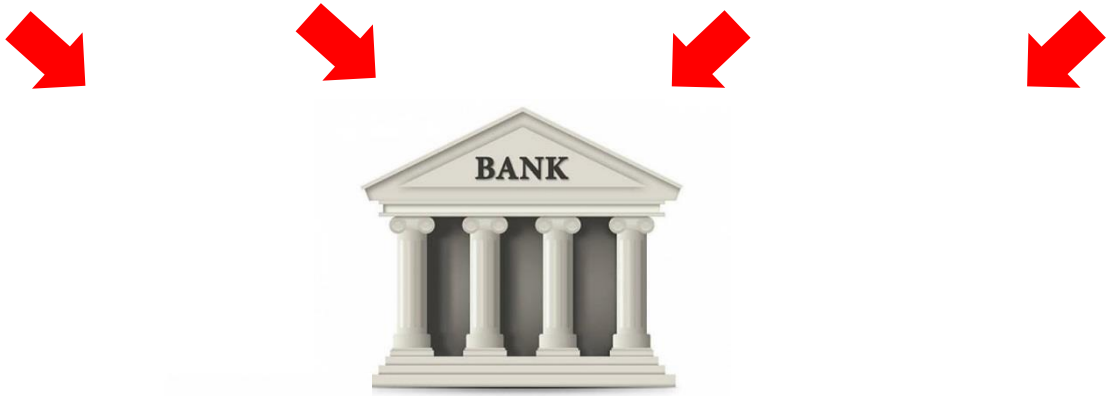
Алексей Сизов
Руководитель направления решений противодействия мошенничеству
Инфосистемы Джет

24 февраля 2016 г.

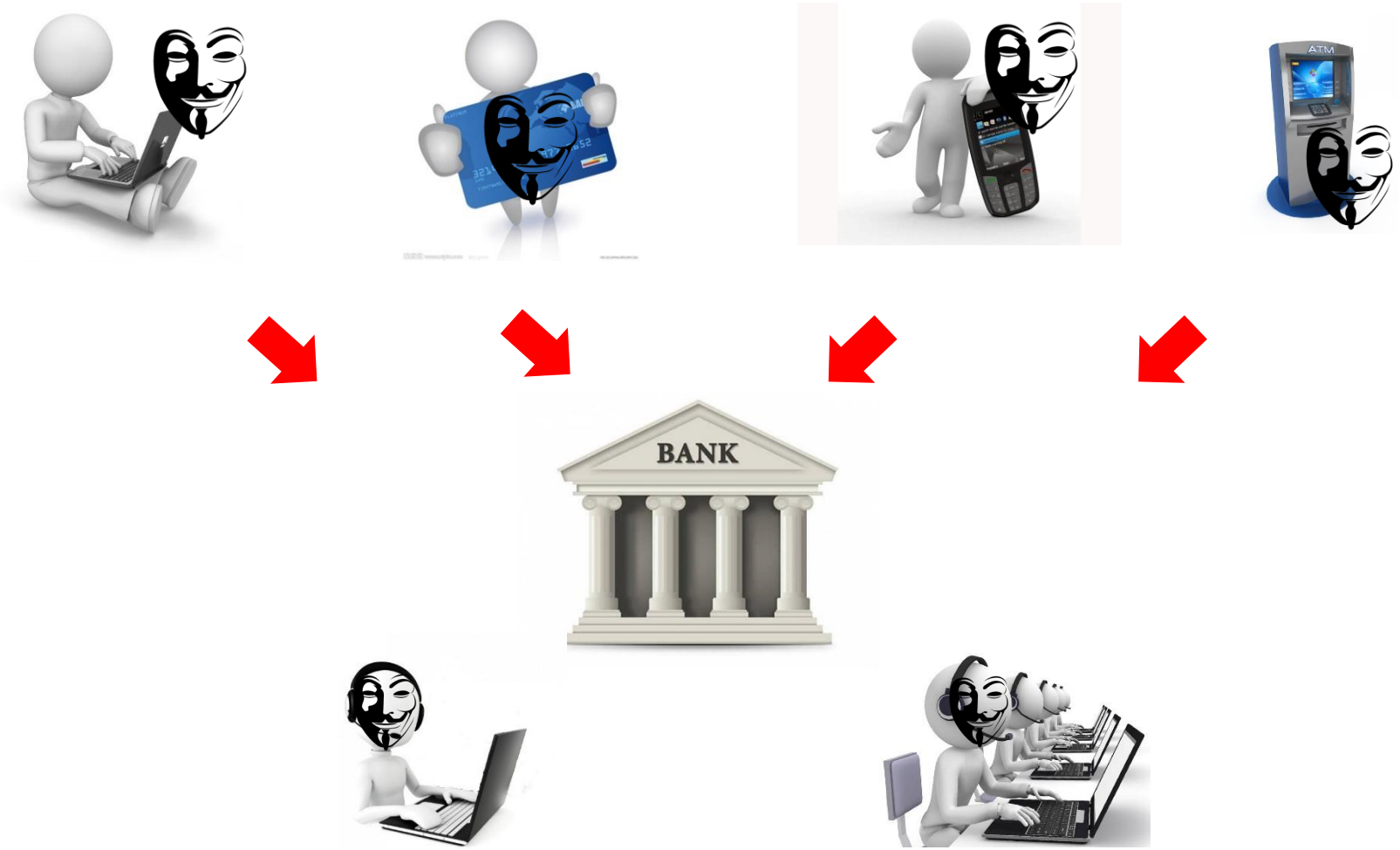
Облачные системы

Велико ли различие?

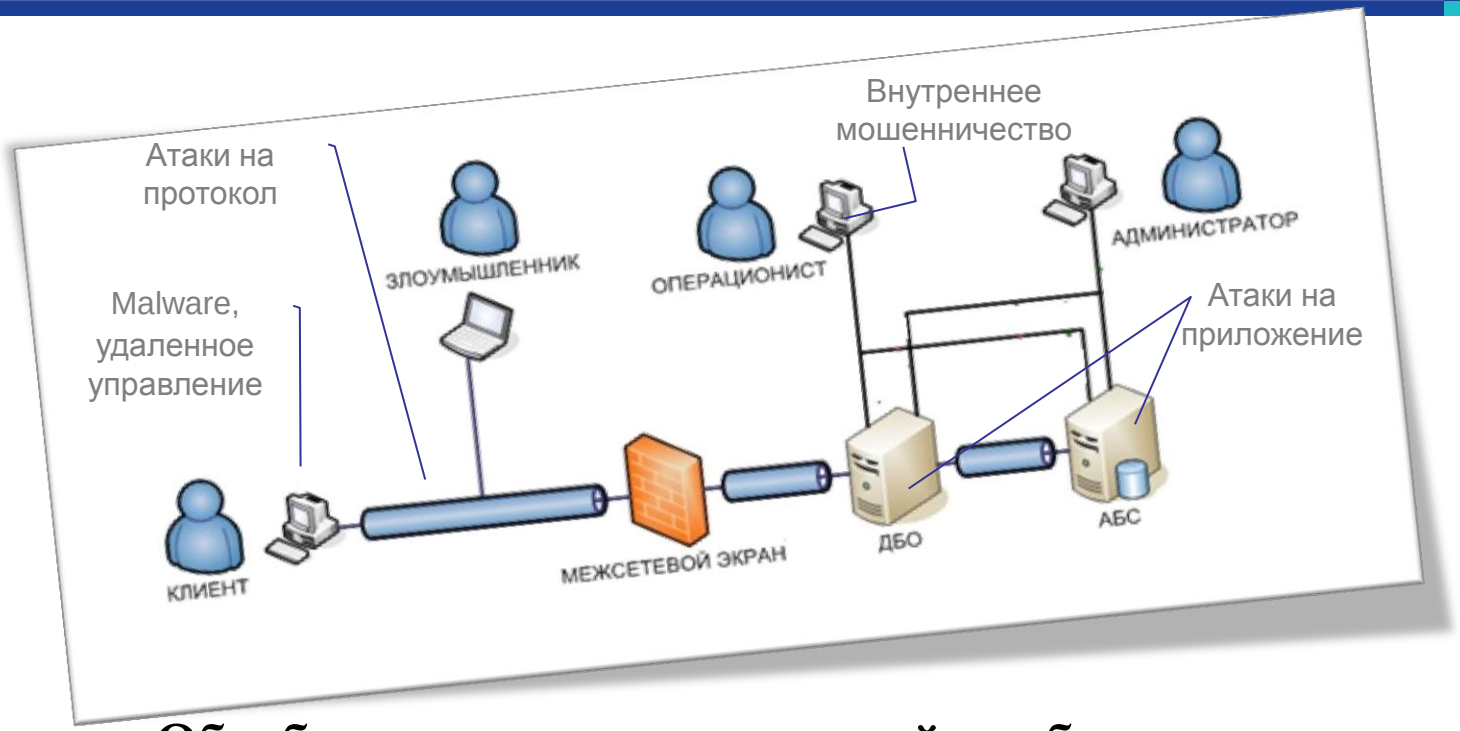
«Классические» риски



«Классические» риски



Общая схема



Обработка платежных операций для банка

- **Контроль среды совершения операции**
- **Контроль канала передачи данных и системных событий**
- **Контроль совершаемых операций**
- **Контроль внутренней обработки таких операций**

Цели эксплуатации

- Скомпрометированные объекты
- Fingerprint
- Локальные угрозы
- Репутация

Антифрод

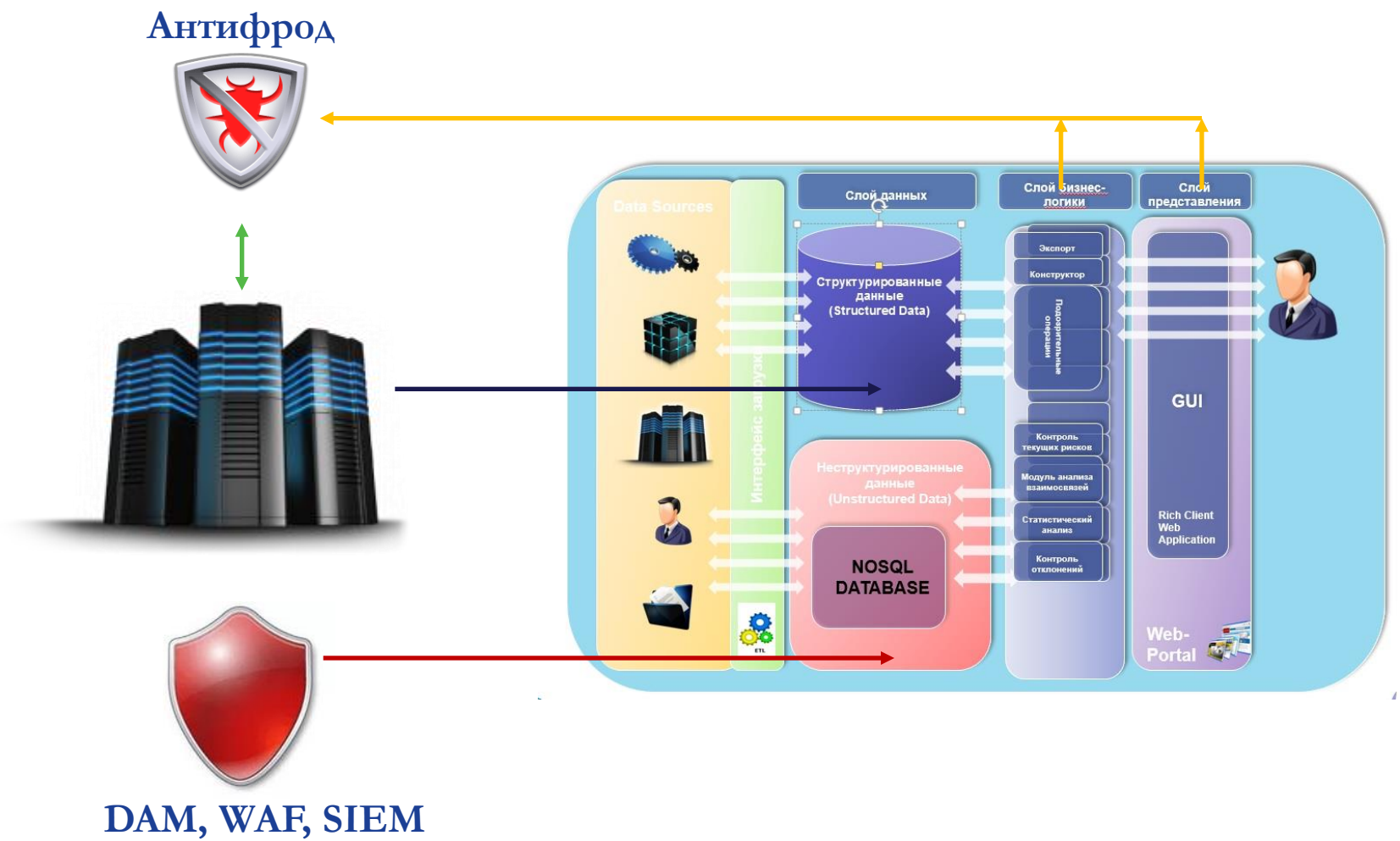
- Репутация+
- Данные получателя
- Жизненный цикл продукта

Восприятие результата

- **Зафиксированная компрометация**
- **Вредоносный объект**
- **Удаленное управление**

- **Идентификация устройства**
- **Косвенные риски**
- **Снятие плохой репутации или факту компрометации**

Концептуальная архитектура



Методология

Методы детектирования угроз:

1. **Контроль известных случаев мошенничества**
2. **Контроль отклонений от статистических показателей в разрезе (клиента, продукта, группы, сотрудника, филиала …)**
3. **Профилирование действий**
4. **Репутация**

Будущее?

Тенденции:

1. **Централизованные сервисы уведомления об угрозах и компрометации**
2. **Расширение объема данных, которые «отдают» для сторонней обработки**
3. **Интеграция облаков в процесс противодействия мошенничеству**

ИНФОСИСТЕМЫ ДЖЕТ

Контакты:

Алексей Сизов

Руководитель направления решений противодействия мошенничеству

Инфосистемы Джет

asizov@jet.su

+7 926 575 53 80