

ИНФОСИСТЕМЫ ДЖЕТ

Больше чем безопасность



НПС: Куда? Бежать?

Евгений Акимов
Заместитель директора ЦИБ
ЗАО «Инфосистемы Джет»

18 февраля 2013 г.

- Путь Джедая
 - СТО БР
 - ЗПДн
 - PCI DSS
 - документы ЦБ
- ФЗ-161 «О НПС»
 - Положения ЦБ во исполнение...
 - «Пока гром не грянет...»
 - Перенос ст. 9 до декабря 2013
- Укрупнено, но более конкретно, чем:
 - Обследование / оценка соответствия
 - План мероприятий
 - Выполнение плана мероприятий



- Если есть compliance по предыдущим требованиям
 - Может по новому и так всё нормально?
- Это ж еще целый ГОД!!!
 - Посмотрим на других
 - Подождём, что будет
- Может отменят?
 - Или хотя бы ещё перенесут...



- Защита ПДн
 - Сертифицированные средства
 - Анализ защищенности
 - Мониторинг активности в БД
 - ОРД, юридические моменты
- PCI DSS
 - Мониторинг инцидентов
 - Контроль целостности
 - Защита БД, обнаружение вторжений
 - Внешние аудиты, pentest'ы, ОРД
- СТО БР
 - «Взамен» ЗПДн
 - Сертификация – под сомнение
 - Процессы, ОРД



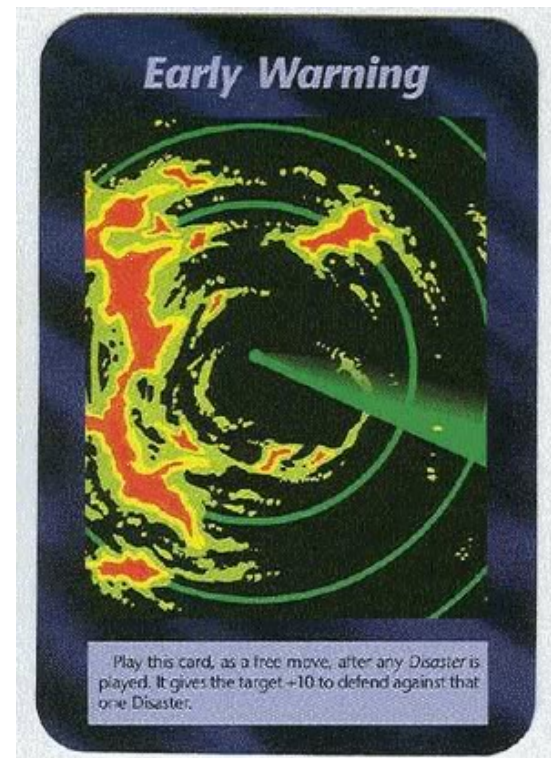
- Технические
 - Новые или модернизированные
 - «Сделал и забыл»
 - VPN, AV...
- Организационно-технические
 - Чаще новые
 - Постоянная активность
 - SIEM, V&C M-t...
- Организационные
 - Документация
 - Новые роли, процессы



- Технические
 - Очень близко СТО БР
- Организационно-технические
 - Предоставление сведений об инцидентах
- Организационные
 - Регулярная оценка соответствия
- Финансовая ответственность
 - Статья 9
 - Инциденты мошенничества



- Новая простая мошенническая схема
 - Потери около 5-10 Мруб. в мес.
- Традиционные механизмы
 - AV, VPN, HIPS
 - Шифрование, ЭЦП, строгая аутентификация...
- Контроль транзакций
 - Детектирование и предотвращение мошеннических операций



**Анализ, выявление схем
мошенничества**

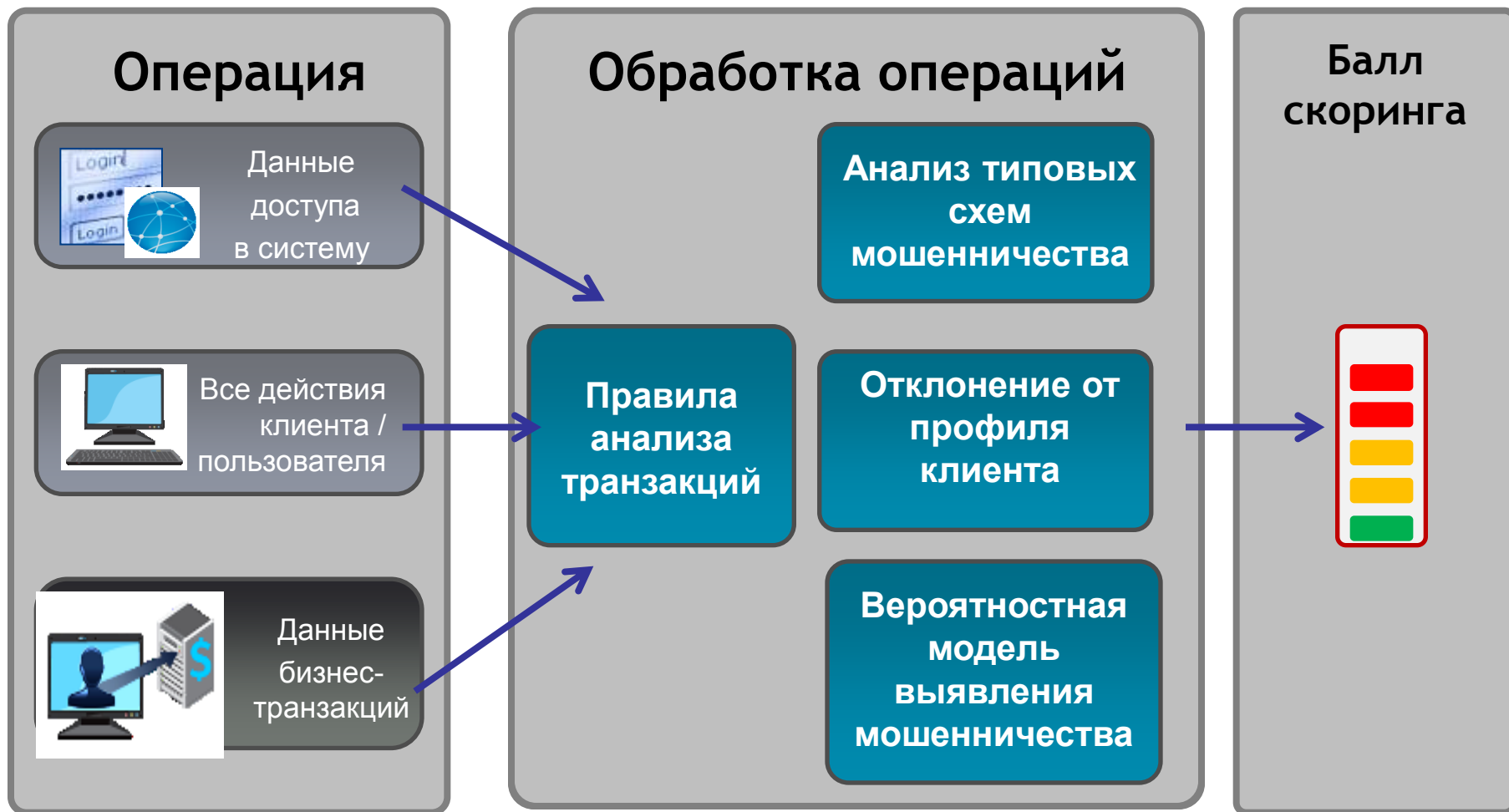
**Интеграция с системами
банка, автоматизация
процедур реагирования**

AntiFraud система

**Политика управления
рисками, политика
реагирования на случаи
хищения**

**Техническая и
консалтинговая
поддержка системы**

Схема работы



- AntiFraud-система
эффективна
 - 14/12/2013
- Создание AntiFraud-системы
 - около полугода
 - 14/06/2013
- Выбор поставщика
 - 1-2 месяца
 - 01/05/2013
- Формирование требований,
обоснование проекта (через пилот)
 - 2 месяца
 - 01/03/2013



- Требования похожи, но отличаются
 - ЗПДн, СТО БР, PCI DSS, НПС
 - Бизнес-требования
- Территориально-распределённая структура
 - Понять для себя
 - Оценить соответствие для регулятора
- Человеческий фактор
 - «На коленке» в Excel не получается



- Единая система контролей
 - «привязка» требований к их конкретной реализации
- Автоматизация work-flow процессов ИБ
- Документирование результатов
- Контроль выполнения задач



Как это выглядит?

RSA Archer eGRC Enterprise Governance, Risk and Compliance

Управление политиками | Управление соответствием | Управление рисками | Enterprise Management | Administration

Navigation Menu: Administration, Управление политиками, Управление соответствием, Управление рисками, Enterprise Management, Administration

Проекты по соответствию: 141346

Record 1 of 2

Dashboard: Контроли

Welcome, System Administrator

Контроли по степени соответствия

Контроли по типу оценки

Контроли

3.77%

96.23%

29 9 22

Степень документированности 29

Степень документированности и выполнения 9

Степень выполнения 22

51 Ф3-152 2 Ф3-161

Действительно бежать и вот куда

- Готовность формально не плохая, но надо:
 - Доработать документацию
 - Оценить соответствие
 - Следовать плану
- Чтоб не потерять деньги
 - Идти по пути внедрения AntiFraud систем
- Чтоб самим не потеряться
 - Автоматизировать процессы ИБ



БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ



Спасибо

Евгений Акимов
зам. директора ЦИБ
ЗАО «Инфосистемы Джет»
eakimov@jet.su

Объем проектов 1 225 млн.
руб.

Заказчиков 247

Контрактов 482

Комплексных проектов 165

- 17 ЭКИБ и СУИБ
- 39 ЗПД и СТО БР
- 24 PCI DSS
- 44 DLP
- 21 SOC/DAM
- 8 IdM
- 7 FM/RA и Business Assurance
- 5 Защита приложений, порталов и пр.



Проекты по отраслям

- 49 банки
- 33 телеком операторы
- 17 страховые и пр. финансовые
- 9 государственные организации
- 24 нефтегазовый сектор
- 13 промышленность
- 18 retail и остальные

ИБ нового ИТ-ландшафта

- Virtual&Cloud Security
Банки, телекоммуникации
- Mobile Security
Телекоммуникации

Эффективность и прозрачность ИБ

- IS Performance Management
Промышленность, нефтегаз
и госсектор

Безопасность бизнеса

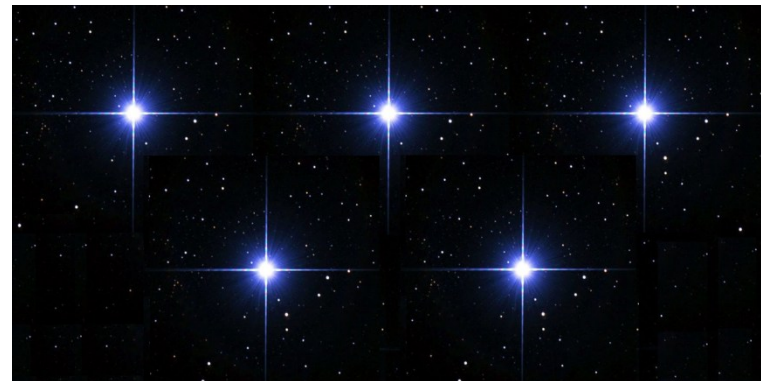
- AntiFraud
Retail
Банки



Скоро

- GRC
- CIRC
- BYOD
- Global SOC
- ИБ из облака

- Объем DLP проектов в Джете
 - 24,2% от общего объема проектов по ИБ
- Объем DLP проектов в России
 - 25,3% от общего объема рынка DLP*



$$1/4 + 1/4 = 5.0$$

* по данным antimalware.ru