Актуальные проблемы ИБ в ритейле и опыт их решения

Федор Курносов

ЭЛЬДОРАДО

ГЕОГРАФИЯ «ЭЛЬДОРАДО»

Сеть «Эльдорадо» включает (данные на 28 февраля 2015):

- **374 розничных гипермаркета**
- **6 пунктов интернет-магазина**
- **5 интернет-гипермаркетов**

Торговая площадь: 542 992,75 кв. метров
Общая площадь: 700 447,96 кв. метров

Присутствие: более 200 городов по всей стране

«Эльдорадо» - крупнейшая российская сеть магазинов бытовой техники и электроники

Информационная безопасность в Эльдорадо

- ✓ Выделенное подразделение ИБ
- ✓ Поддержка топ-менеджмента
- ✓ Высокая зрелость процессов ИБ
- ✓ Регулярные тренинги по ИБ
- ✓ Использование лучших мировых практик (сертифицированная по ISO 27001:2013 СУИБ)
- ✓ Интеграция ИБ в бизнес-процессы

Сертификат Регистрации

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ - ISO/IEC 27001:2005

Настоящим удостоверяется, что:

JSC "ELDORADO"
14, Smolnaya Str.
Moscow
125493
Russian Fed.

Выдан Сертификат №: IS 574217

о соответствии действующей Системы Управления Информационной Безопасностью требованиям стандарта ISO/IEC 27001:2005 в отношении следующих видов деятельности:

Осуществление закупок цифровой и бытовой техники и электроники, поддержка "Программы лояльности" и проведение безналичных платежей в соответствии с "Положением о применимости контролей" ЭП-9 от 11.01.2011.

От имени и по поручению BSI:

Исполнительный Директор, BSI EMEA

Дата первоначальной регистрации: 11/05/2011 Дата последней выдачи: 11/05/2011 Действителен до: 11/05/2014

Стр.: 1 из 2

Настоящий сертификат был выпущен в электронной системе BSI и остаётся собственностью BSI, использование сертификата ограничивается условиями Договора.
Электронный сертификат может быть подтвержден online.
Назначенные копии могут быть подтверждены на www.bsi-global.com/ClientDirectory.

British Standards Institution (Британский Институт Стандартов) учрежден на основании Королевского Устава.
Головной офис BSI (EMEA): 389 Chiswick High Road, London, W4 4AL, United Kingdom.

Цель ИБ: Помощь бизнесу

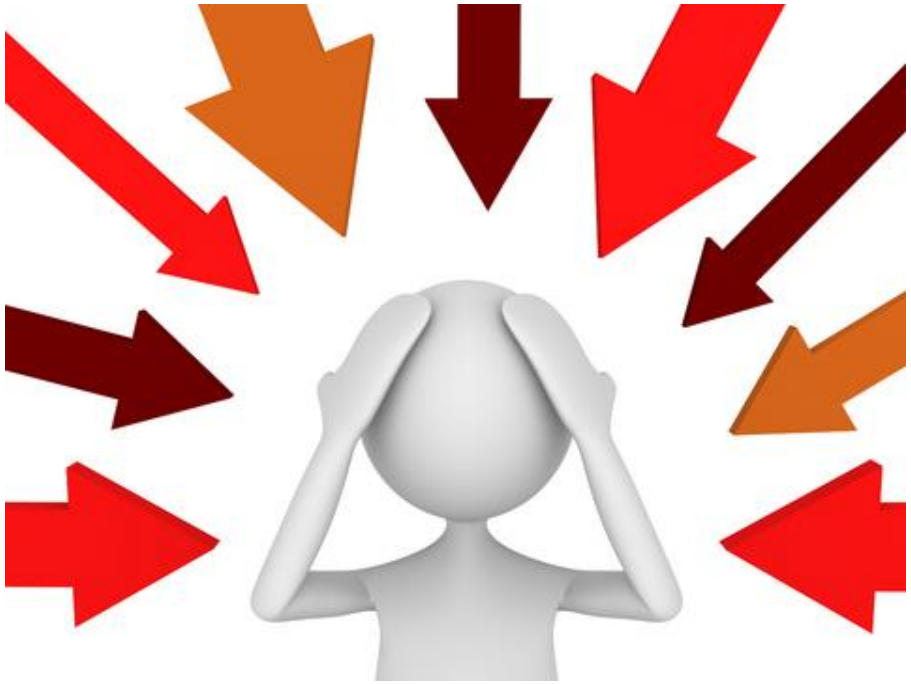
- ✓ Поддержка бизнеса:
  - ✓ Управление рисками ИБ
  - ✓ Обеспечение соответствия
  - ✓ Организация процессов ИБ
- ✓ Развитие ИБ:
  - ✓ Интеграция ИБ в корпоративную культуру
  - ✓ Минимизация затрат на ИБ
  - ✓ Повышение эффективности и прозрачности ИБ

Пусть твои дела будут такими, какими ты хотел бы видеть их в старости.
Марк Аврелий

ЭЛЬДОРАДО

Вызовы ИБ

- ✓ Требования регулятора - сбор и уточнение ПДн на территории РФ 242-ФЗ
- ✓ Злоумышленные действия – APT и атаки на web-приложения
- ✓ Экономический кризис – необходимость экономии на СЗИ



Локализация процессов обработки ПДн на территории РФ

- ✓ Требование 242-ФЗ
- ✓ С 01.09.15 локализировать отдельные процессы обработки ПДн в РФ:

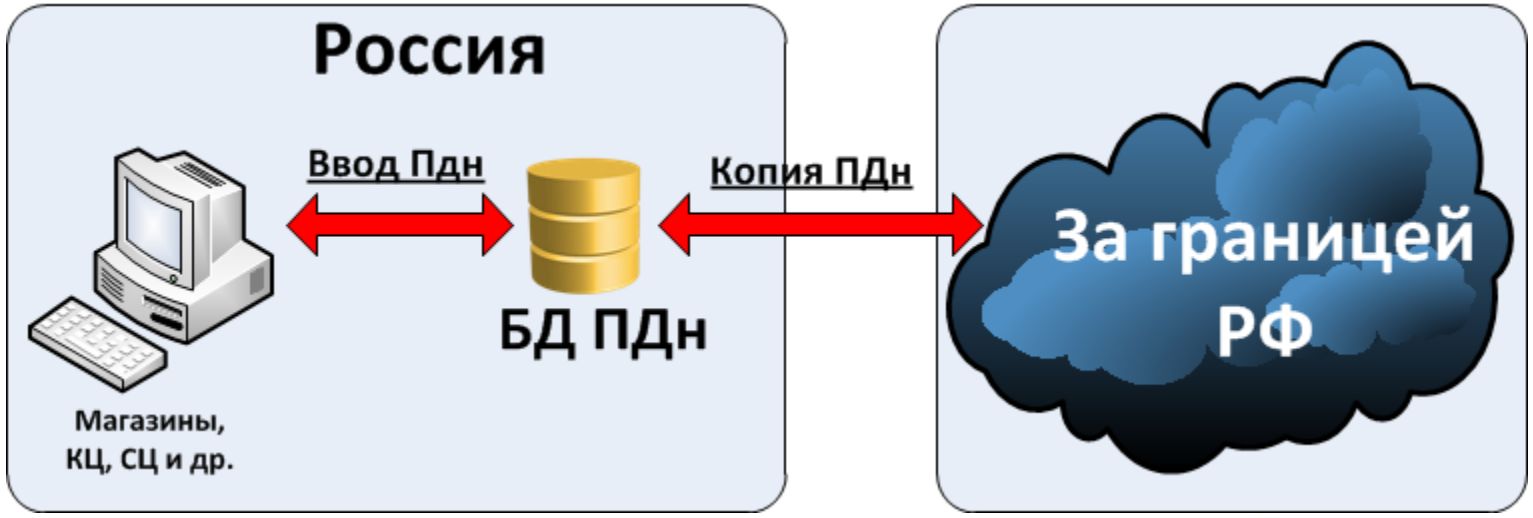
  При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ

- ✓ **Трансграничная передача ПДн при выполнении требований 152-ФЗ разрешена**

ЭЛЬДОРАДО

Решение: Сбор и уточнение ПДн в РФ

- ✓ Создаем БД в РФ
- ✓ Все операции, которые подпадают под понятие сбор ПДн проводим с использованием ее
- ✓ При необходимости передаем данные за границу РФ



Злоумышленные действия – APT и атаки на web

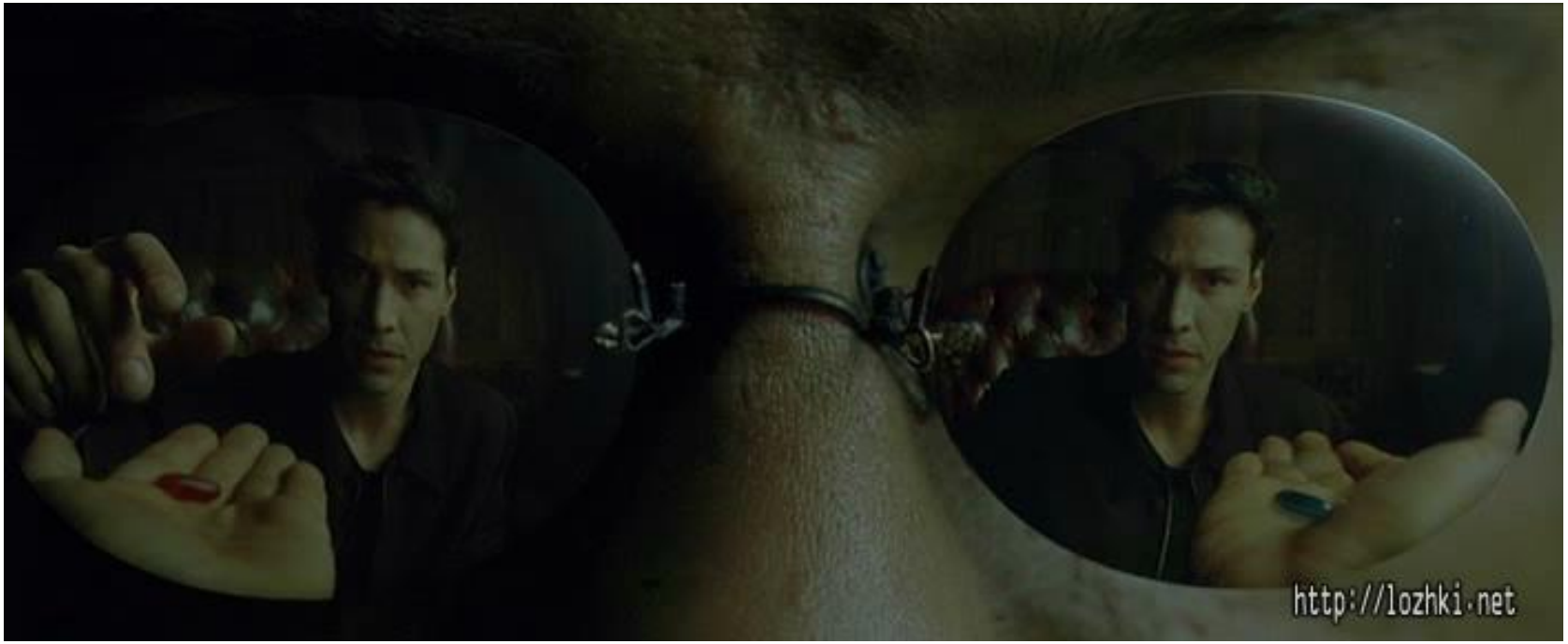
Отличительные особенности APT-атак

- ✓ Атака хорошо подготовлена
- ✓ Атака направлена именно на вашу компанию
- ✓ Атака включает в себя многие техники проведения атак, такие как вредоносное ПО, социальная инженерия

Злоумышленные действия – APT и атаки на web

Как защититься?

Во-первых, принять аксиому, что универсальной таблетки нет☺



Злоумышленные действия – APT и атаки на web

Как защититься?

Использовать комплексную систему защиты:

- ✓ Антивирусное ПО
- ✓ IDS и IPS
- ✓ SIEM
- ✓ Песочницы
- ✓ **Обучение персонала**

ЭЛЬДОРАДО

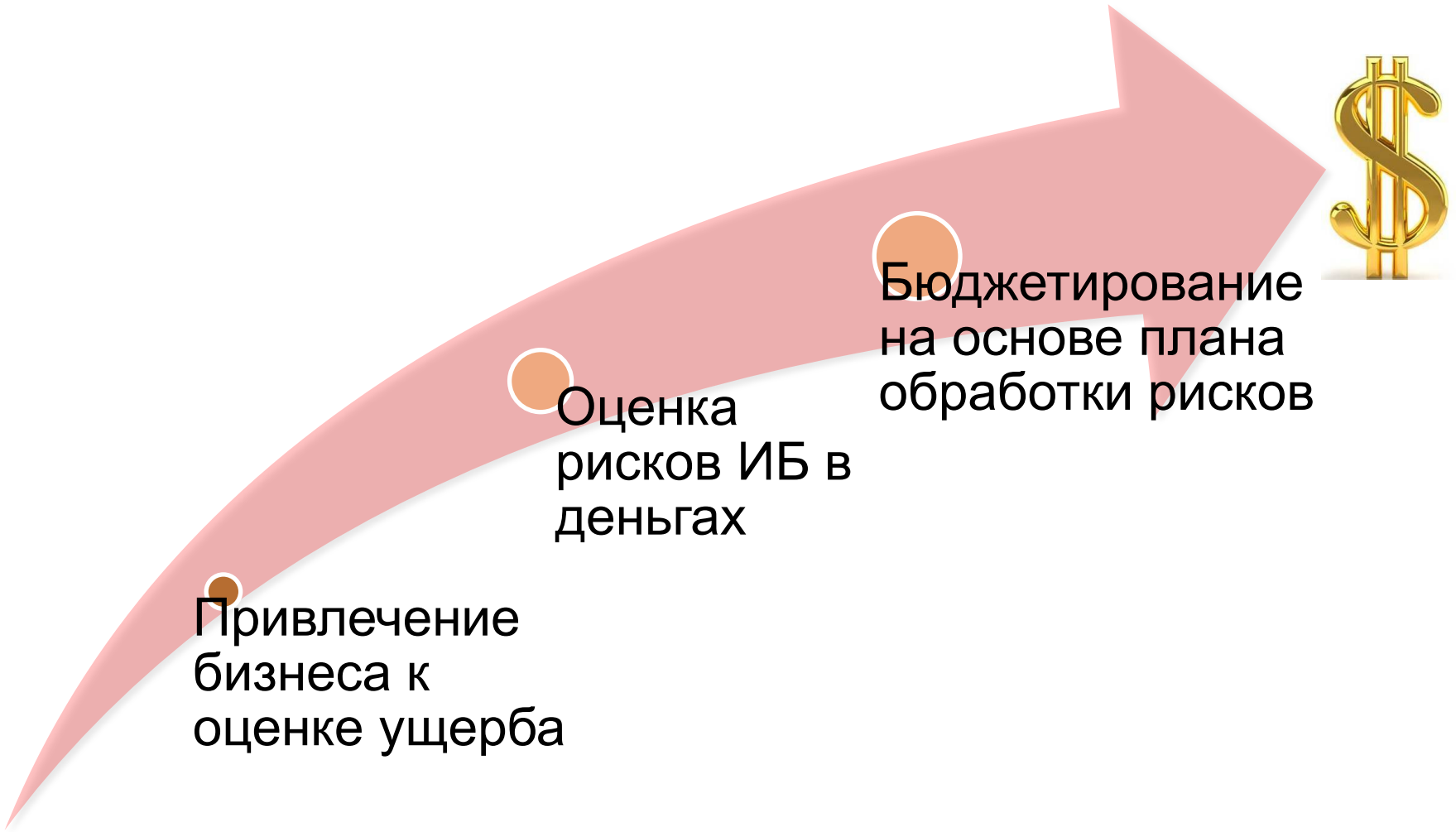
Злоумышленные действия – APT и атаки на web

- ✓ DDoS - атаки
- ✓ Атаки на web-приложение (в т.ч. подбор паролей клиентов)
- ✓ Перехват заказов

ЭЛЬДОРАДО

Кризис – необходимость экономии на СЗИ

Управление рисками ИБ



Риск = комбинация вероятности и ущерба

*

ЭЛЬДОРАДО

Риски влияют на бизнес через ИТ-активы

Бизнес: Определение ценности ИТ-активов

- Бизнес-подразделения определяют:
  - Маржу ($) от бизнес-процесса
  - Перечень поддерживающ их бизнес-процесс ИС
  - Степень (%) влияние каждой ИС на бизнес-процесс

ЭЛЬДОРАДО

ИТ: Декомпозиция ИТ-активов на компоненты

- ИТ определяет:
  - Состав компонентов в каждой ИС
  - Степень (%) влияния каждого компонента на ИС

ИБ: Анализ рисков

- ИБ осуществляет:
  - Выявление уязвимостей
  - Анализ угроз и их вероятности
  - Идентификацию и анализ рисков

Разработка плана обработки рисков…

…И выбор только необходимых и экономически обоснованных СЗИ, которые позволяют снизить риски ИБ до приемлемого уровня.

Реализация плана обработки рисков

Совместная деятельность ИБ и бизнеса!

ЭЛЬДОРАДО

Вопросы?