«ЭЛЬДОРАДО» — крупнейшая российская сеть магазинов бытовой техники и электроники

Актуальные проблемы ИБ в ритейле и опыт их решения

Курносов Федор

Сеть «Эльдорадо» включает:

*данные на 31.07.2016

ПРИСУТСТВИЕ:
БОЛЕЕ 200 ГОРОДОВ ПО ВСЕЙ СТРАНЕ

413
розничные гипермаркеты

каждый магазин работает как пункт самовывоза

583 150
м² торговой площади

750 485
м² общей площади

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" ЗП-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.

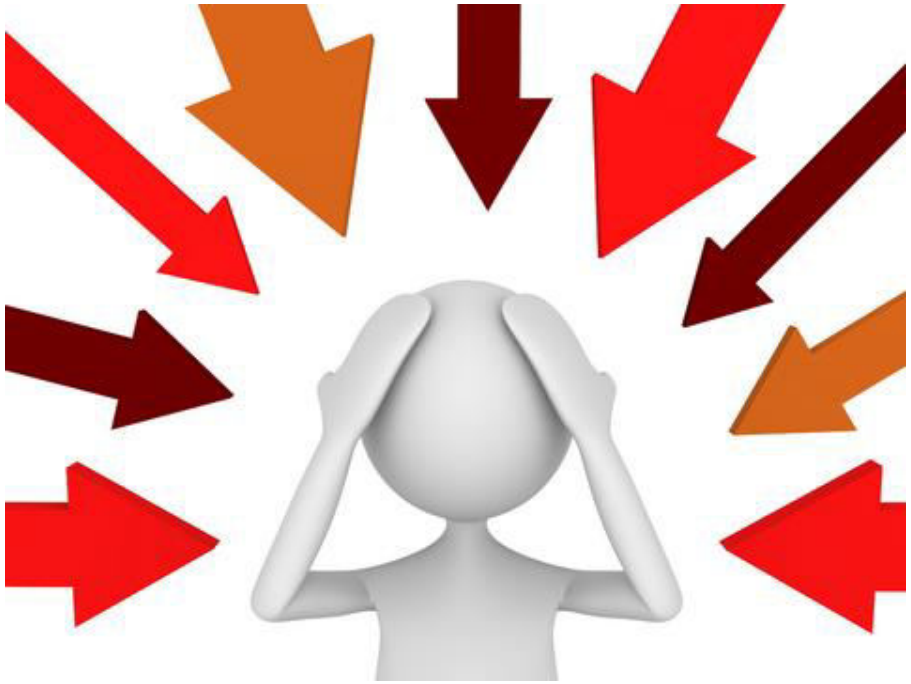
Цель ИБ: помощь бизнесу

- ✓ 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

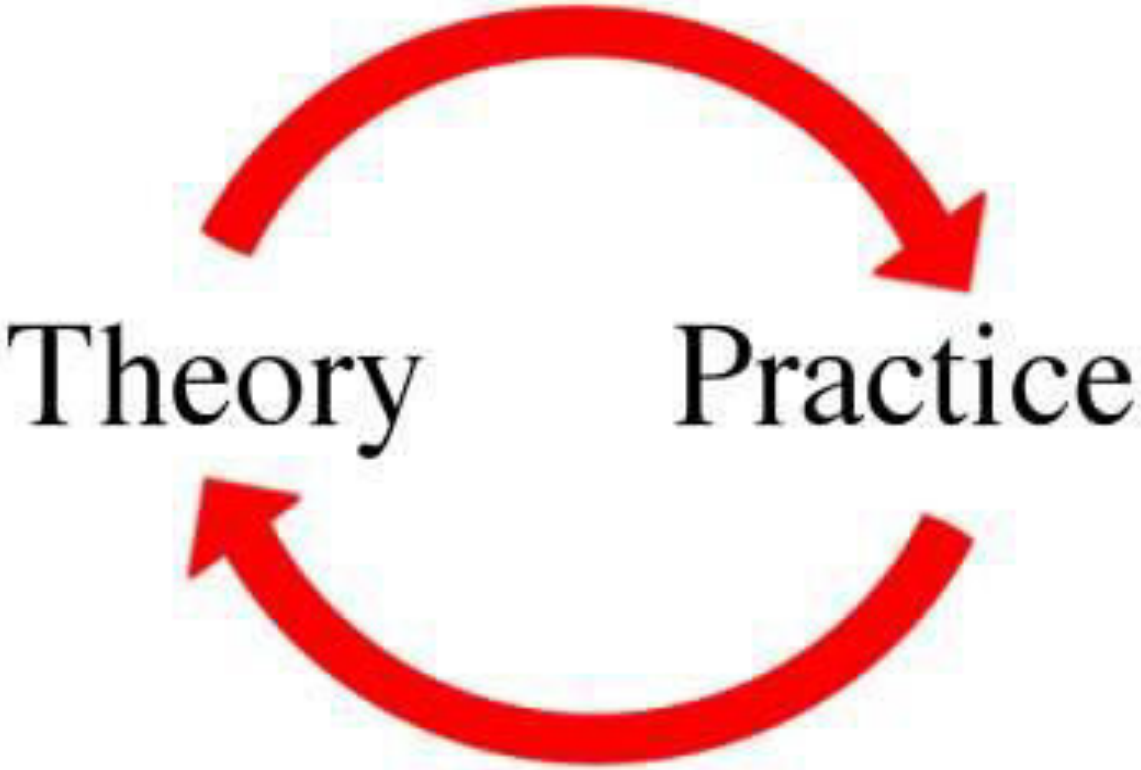
Вызовы ИБ

- 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

От теории к практике



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**

От чего ушли, к чему пришли

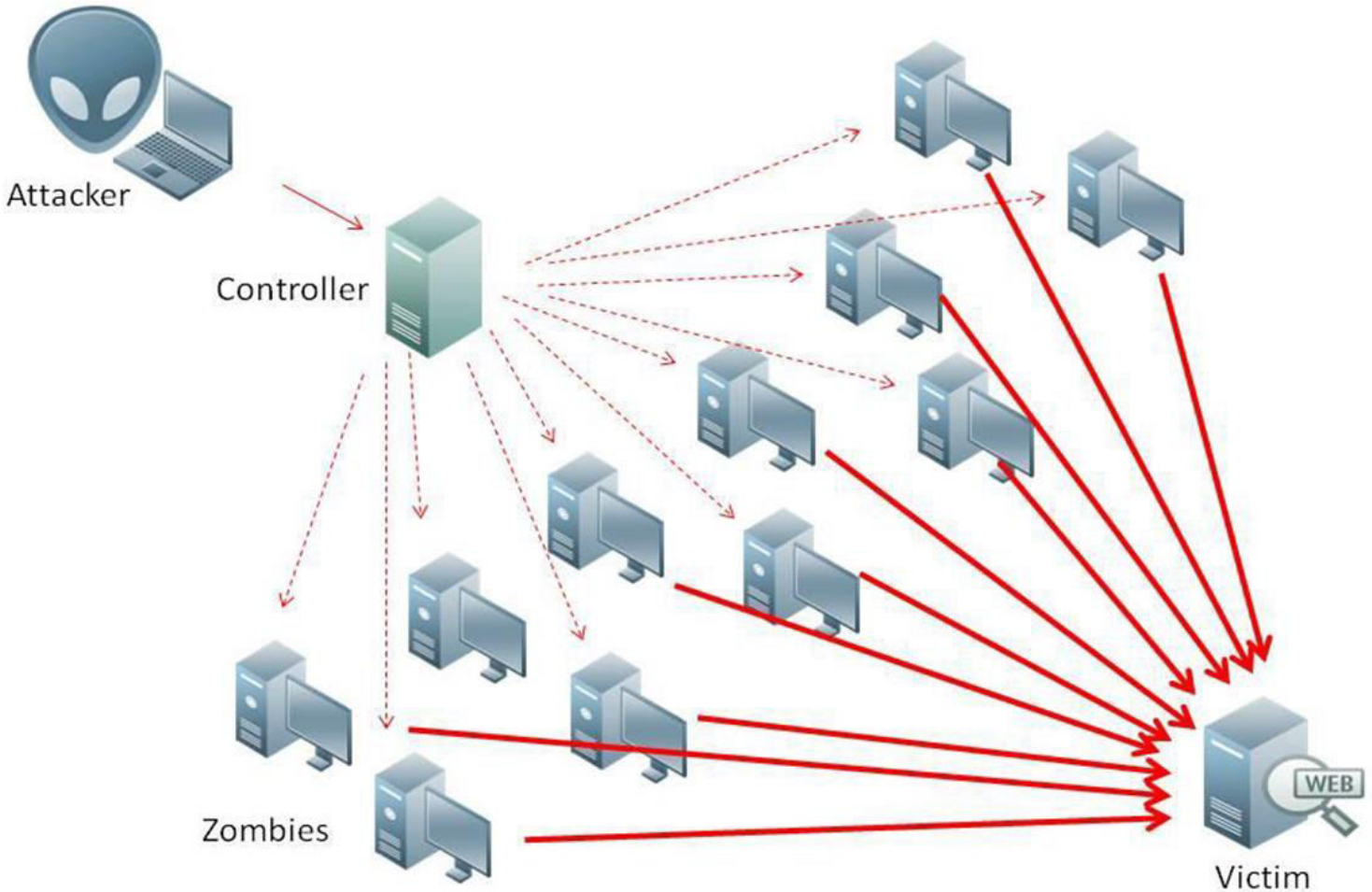
Основа обеспечения ИБ

- ✓Конфиденциальность
- ✓Целостность
- ✓Доступность

Наиболее значимые угрозы ИБ

- ✓ DDoS
- ✓ Атаки на web-приложение (в т.ч. подбор паролей клиентов)
- ✓ Мошенничество с ценами, промо, бонусами
- ✓ Утечка ПДн
- ✓ APT
- ✓ Санкции регуляторов

Защита от DDoS-атак



Защита от атак на web-приложение

ЭЛЬДОРАДО

WAF!

Защита на уровне web-приложения

- ✓ *Усиленная аутентификация*
- ✓ *Защита от подбора паролей*
- ✓ *Мониторинг*
- ✓ *Контроль заказов*

Регулярный анализ защищённости

- ✓ *Выявить имеющиеся уязвимости web-приложения, которые можно использовать для нарушения бизнес-логики и нанесения ущерба компании*
- ✓ *Спланировать мероприятия по закрытию уязвимостей*
- ✓ *Снизить риски для бизнеса*

«Сломайте свой ИМ раньше, чем его сломают другие!»

С чем мы столкнулись

- В марте на нас началась масштабная атака по подбору паролей от пользовательских аккаунтов
- В ходе атаки мы применяли различные средства противодействия вплоть до изменения логики входа пользователя на сайт

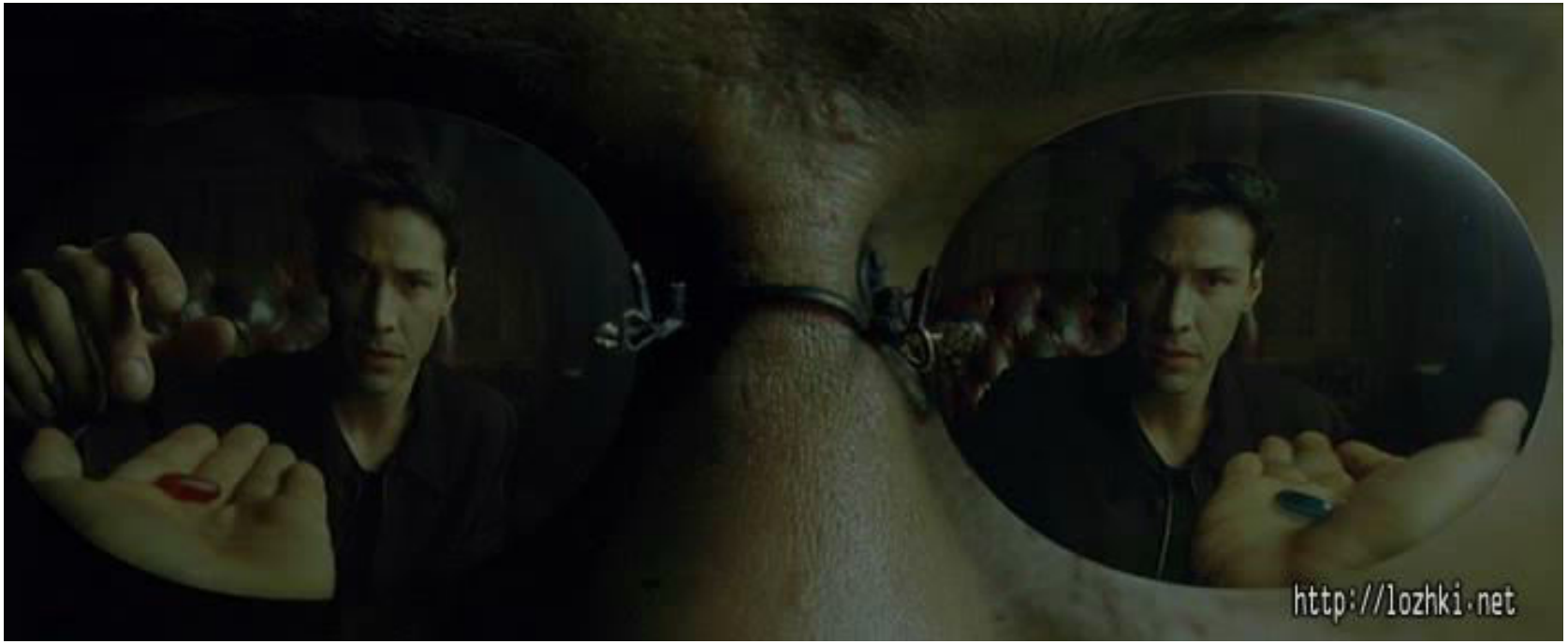
Как выяснилось впоследствии, подобная атака шла по всем онлайн- ритейлерам ru-зоны

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

Как защититься?

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



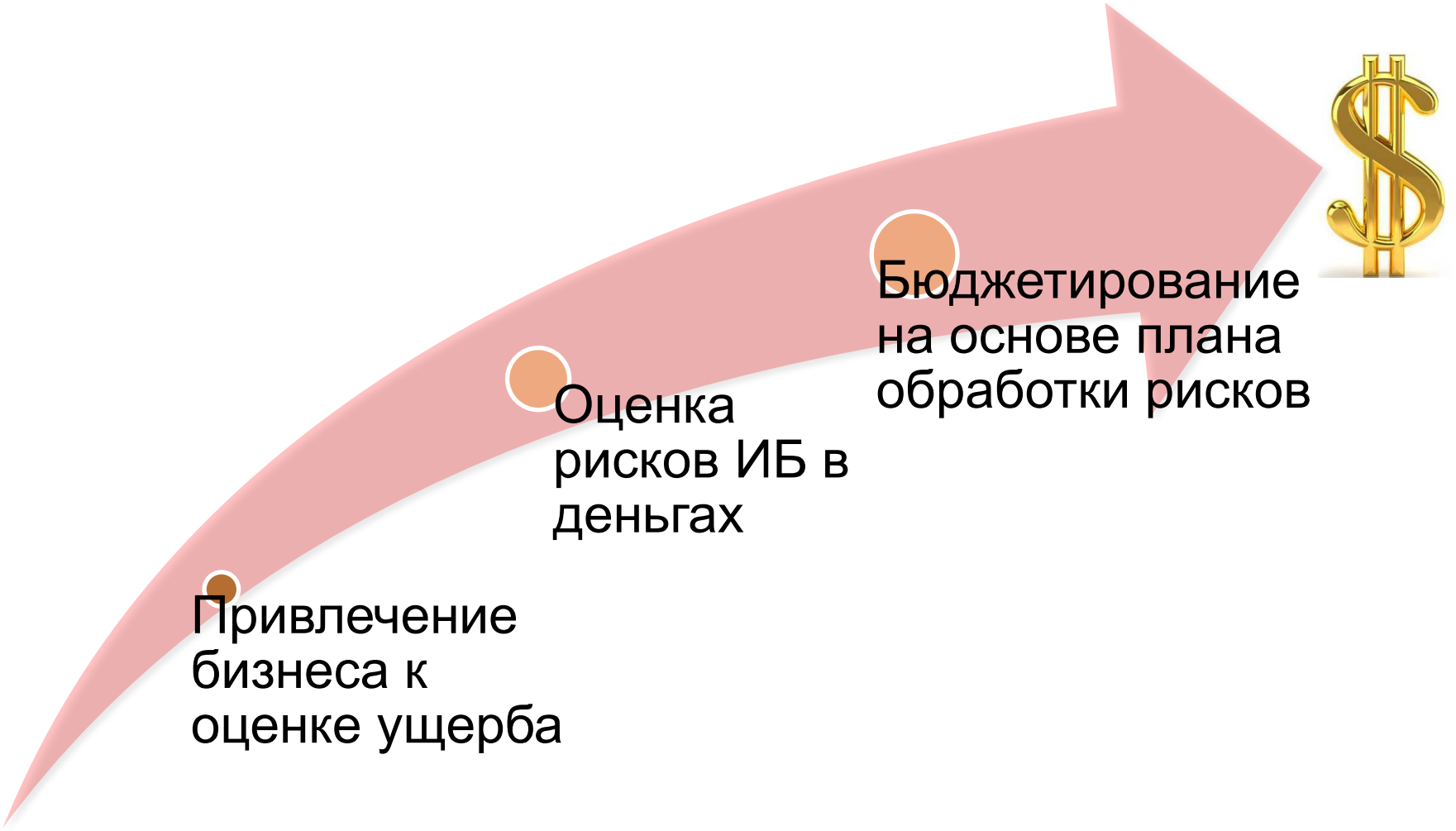
APT

Как защититься?
Использовать комплексную систему защиты:

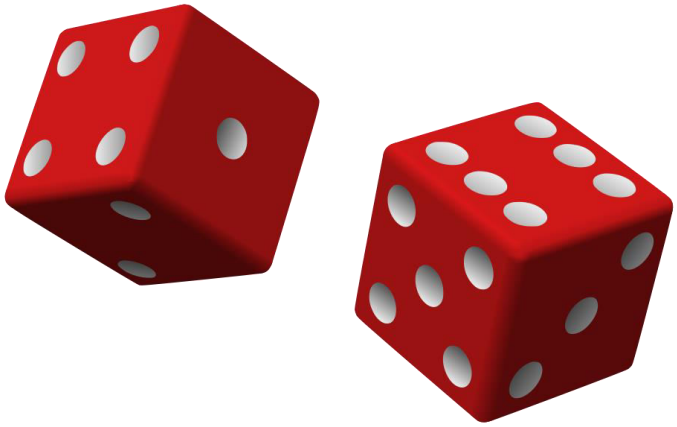
- ✓ Антивирусное ПО
- ✓ IDS и IPS
- ✓ SIEM
- ✓ Песочницы
- ✓ **Обучение персонала**

Кризис – необходимость экономии

Управление рисками ИБ



Риск = комбинация вероятности и ущерба



Риски влияют на бизнес через ИТ-активы

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!

Вопросы?