# Обоснование затрат ИБ

Сергей Рысин

CNEWS Forum 2019

07.11.2019

# Диалог между бизнесом и CISO

- Политика открытости
- Язык денег

# Подготовка к диалогу с бизнесом

- Провести самостоятельный аудит ИТ-инфраструктуры
- Сформировать базу локальных нормативных актов:
  - Модель нарушителя
  - Модель угроз
  - Политика безопасности
  - Disaster recovery plan по различным видам ВАШИХ угроз
- Сформировать перечень бизнес-процессов, в которых участвует ИБ:
  - Какие БП обрабатываются в подразделении
  - Ресурсы, необходимые в БП
  - Входные данные в БП в подразделении
  - Результат БП, отправляемый заказчику данного БП
- Сформировать стратегию развития ИБ на горизонт 5 лет

# Новое оборудование – необходимость или прихоть?

- Для чего?
- Какие риски?
- В чем экономия?
- Соотношение стоимости и итоговой выгоды?

# Внедрение NGFW

- Для чего?

  Организация одного из элементов непрерывности бизнеса, минимизация рисков простоя

- Какие риски перекроет?

  Защита от угроз 0-day

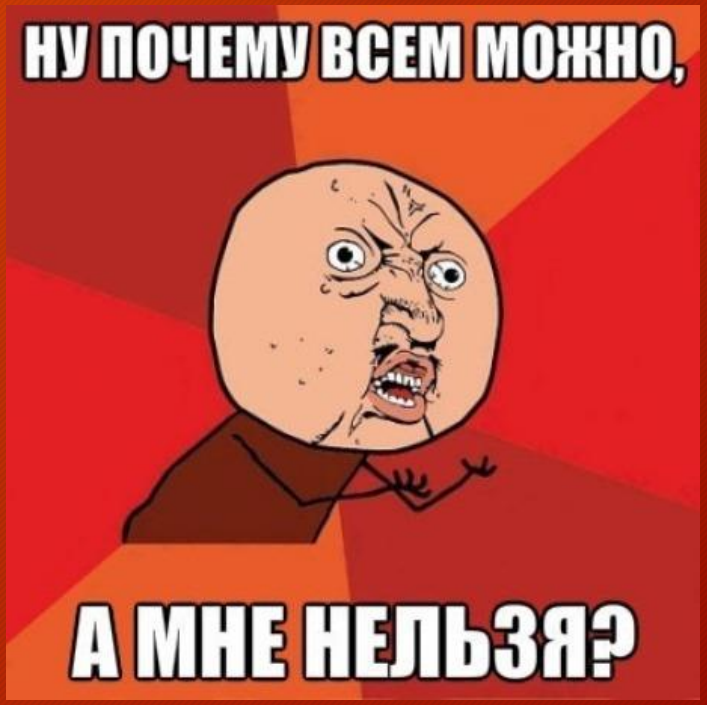
- В чем экономия?

  Отсутствие простоя организации в случае инцидента, потери рассчитываются на основе личного опыта компании или других игроков на рынке

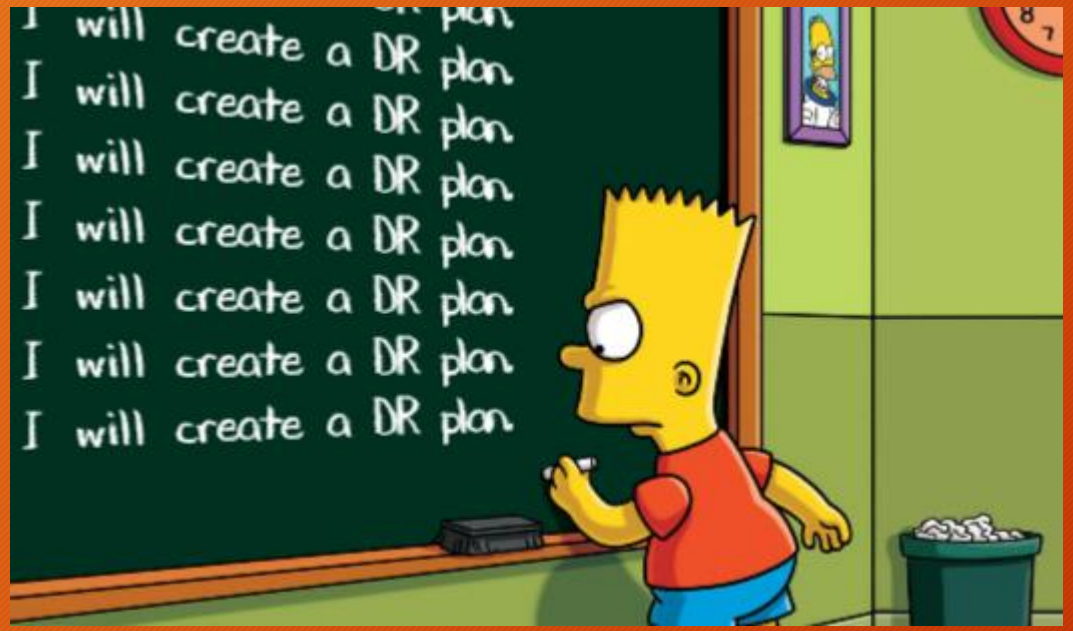
  В случае каждой компании необходимо считать стоимость простоя в час, в сутки

- Соотношение стоимости и итоговой выгоды?

  Разница между затратами на ИБ и возможными потерями с учетом их вероятности



# Аренда резервного ЦОДа


- Подготовлен Disaster recovery plan
- Стоимость оборудования = 100 ед.
- Риск потери данных:
  - Оценка потерь = 1 000 000 ед.
  - Вероятность потерь = 20%
- Выгода от аренды резервного ЦОДа = 199900 ед.

# Аутсорсинг на языке бизнеса

Сформировать перечень новых бизнес-процессов ИБ:

- Описать решаемые бизнес-задачи
- Описать трудозатраты
- Описать результат бизнес-процесса

Подсчитать стоимость:

- Содержания собственного штата специалистов
- Стоимость аутсорсинга

# Аутсорсинг – всегда ли благо?

- Плюсы:
  - Нет роста ФОТ
  - Нет необходимости формировать премиальный фонд
  - Для небольших компаний – качественный специалист за небольшие деньги
  - Решение рутинных задач
  - Нет необходимости прокачивать Soft Skills у аутсорсинга
  - Масштабируемость
  - Безболезненный отказ от услуги
- Минусы:
  - Отсутствует прозрачный контроль за работниками сервиса
  - Возможно воздействие на сервис компанию третьих сторон

# Личный опыт сервисов

Внешние сервисы

- SOC
- Security Awareness
- Анализ СМИ

# SOC – собственный VS как сервис

- Минимальный штат :
  - 6 работников первой линии
  - 6 работников второй линии
  - 1 аналитик третей линии
- Минимальный ФОТ в месяц: ~1,9 млн. руб.
- Ежегодные затраты на информационные базы: ~10 млн. руб.
- Приблизительные единовременные затраты на оборудование: ~15 млн.

Ежемесячный сервис в рамках договора: ~ 670 тыс. руб.

# Спасибо! Вопросы? ;)

Сергей Рысин

sergey@rysin.su