# Защита информации и информационная безопасность

Созиев Д.М.

Email:dsoziev@gmail.com

# Оглавление

# Что такое безопасность?

1. Отсутвие угроз или умение с ними справляться.
2. Стабильное развитие, рост предприятия.
3. Взаимовыгодное сотрудничество.

Как достигнуть?

# Классификация угроз

Экономические:

Новые технологии и рынки, цены на ресурсы, квалифицированный персонал

Финасовые:

Валютные колебания, Инфляция, Мошейничество

Информационные:

Утечки информации, отказ ИТ систем, кибершпионаж

# Экономические угрозы

Новые технологии и рынки сбыта:

Как защитить себя: инвестиции в инновации, создание новых потребностей, переход на рынки
с максимальной добавленной стоимостью

Ресурсные ограничения:

Как защитить себя: несколько поставщиков, экономия ресурсов

Квалифицированный персонал:

Как защитить себя: инвестиции в обучение сотрудников , создание привлекательных рабочих мест.

# Финасовые преступления в сфере ИТ

Мошейничество с кредитными картами.

Как защитить себя: осторожность, дополнительные с-ва аутентификации

Кража денежных средств через систему Банк-Клиент.

Как защитить себя: осторожность  и соблюдение правил

Финансовая отчетность.

Как защитить себя: Контроль утечек информации


# Утечки информации, отказ ИТ систем

Утечки информации о

- *Сотрудниках*
- *Клиентах*
- *Интеллектуалной собственности*

Как защититься: классификация информации, шифрование, контроль утечек.

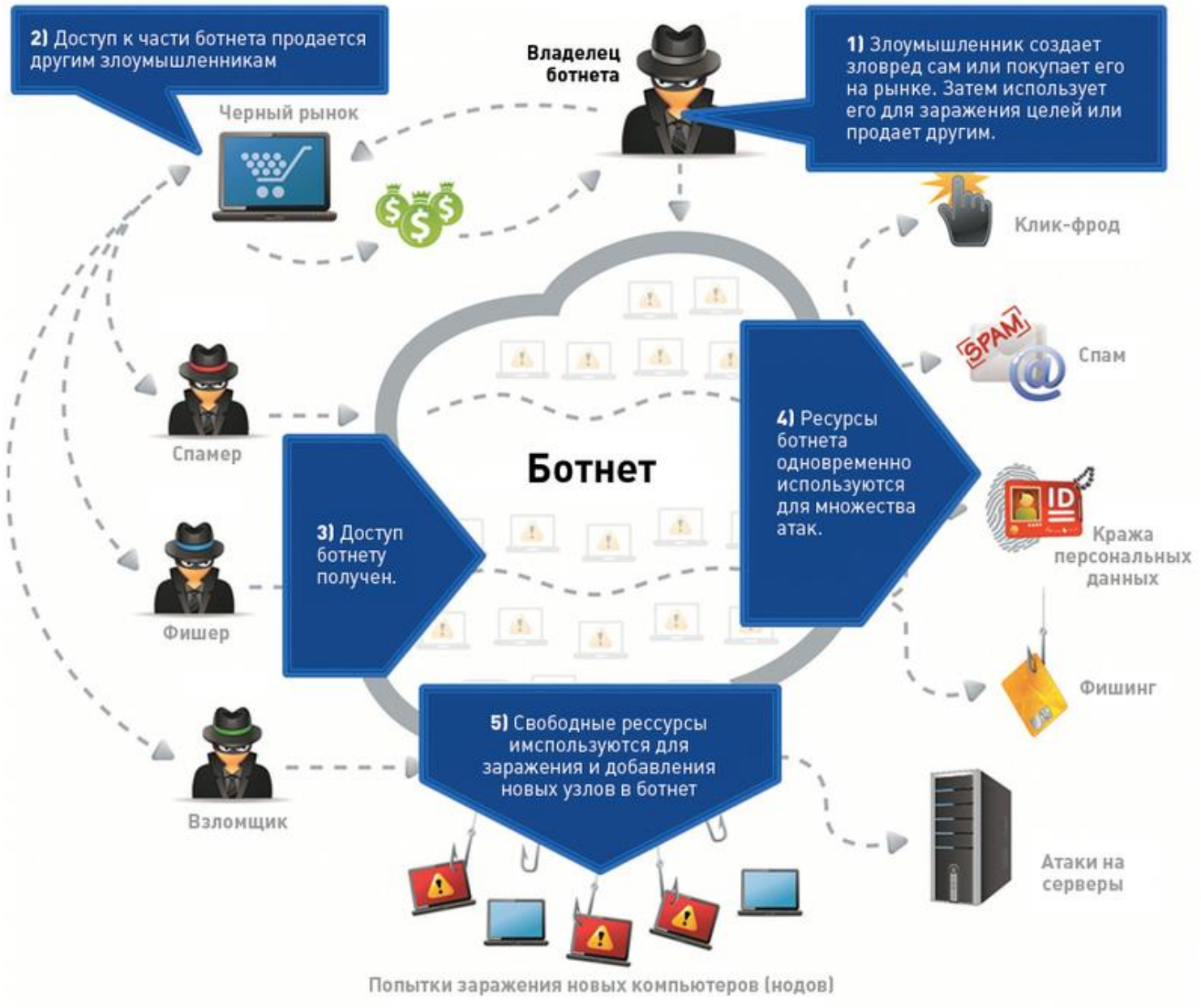
Вывод из строя ИТ инфраструктуры

- DDOS
- Блэк-аут

Как защититься: резервирование оборудования, каналов связи и источников питания.

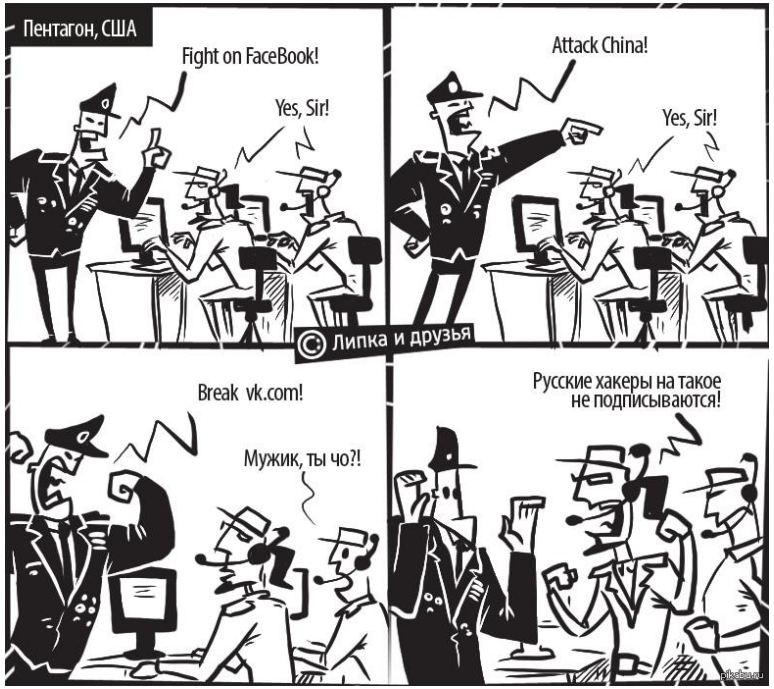
# Кибершпионаж

# Бот-нет


2) Доступ к части ботнета продается другим злоумышленникам
Черный рынок
Владелец ботнета
1) Злоумышленник создает зловред сам или покупает его на рынке. Затем использует его для заражения целей или продает другим.
Клик-фрод
Спам
Спамер
Ботнет
4) Ресурсы ботнета одновременно используются для множества атак.
3) Доступ ботнету получен.
Кража персональных данных
Фишер
Фишинг
5) Свободные рессурсы имспользуются для заражения и добавления новых узлов в ботнет
Взломщик
Атаки на серверы
Попытки заражения новых компьютеров (нодов)

# Составные этапы атаки

1. Сбор сведений
2. Определение уязвимостей и подбор инструментов для атаки
3. Получение доступа к ИТ системе
4. Нанесение ущерба жертве.



# Сбор сведений

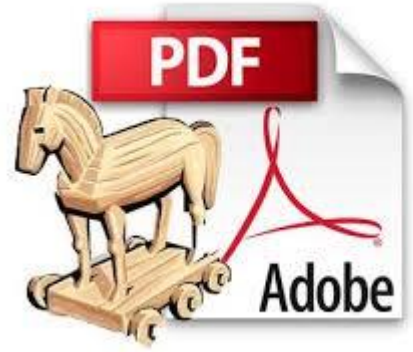
Источники информации

- Социальные сети: Facebook, VK, LinkedIn
- Вэб сайт
- Google/Yandex
- DNS, RIPE

Социальная инженерия

# Определение уязвимостей

1. Определение версии ПО
2. Подбор эксплоит`а
3. Написание Payload
4. Шифрование Payload+ эксплойт



# Получение доступа

1. Отправка эксплойт`а
2. Запуск на компьютере жертвы
3. Установление соединения с сервером злоумышленника
4. Очистка логов

# Нанесение ущерба

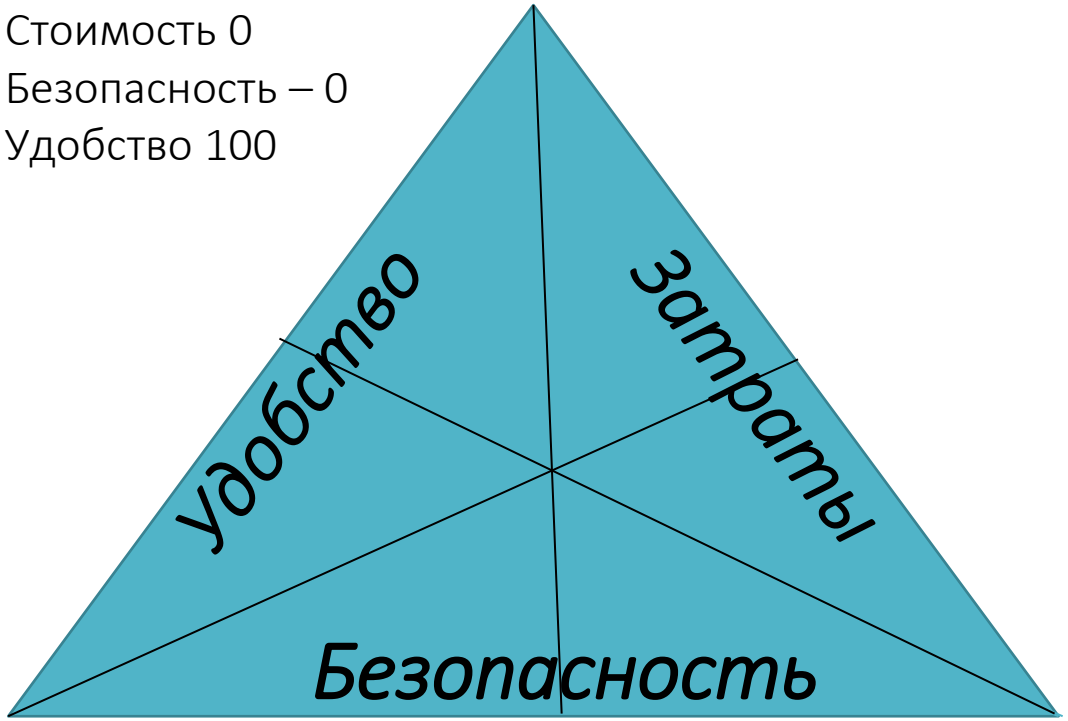
1.Кража информации

2. Вывод из строя инфраструктуры

3. Наблюдение  за системой жертвы

# Треугольник ограничений

Стоимость 0
Безопасность – 0
Удобство 100

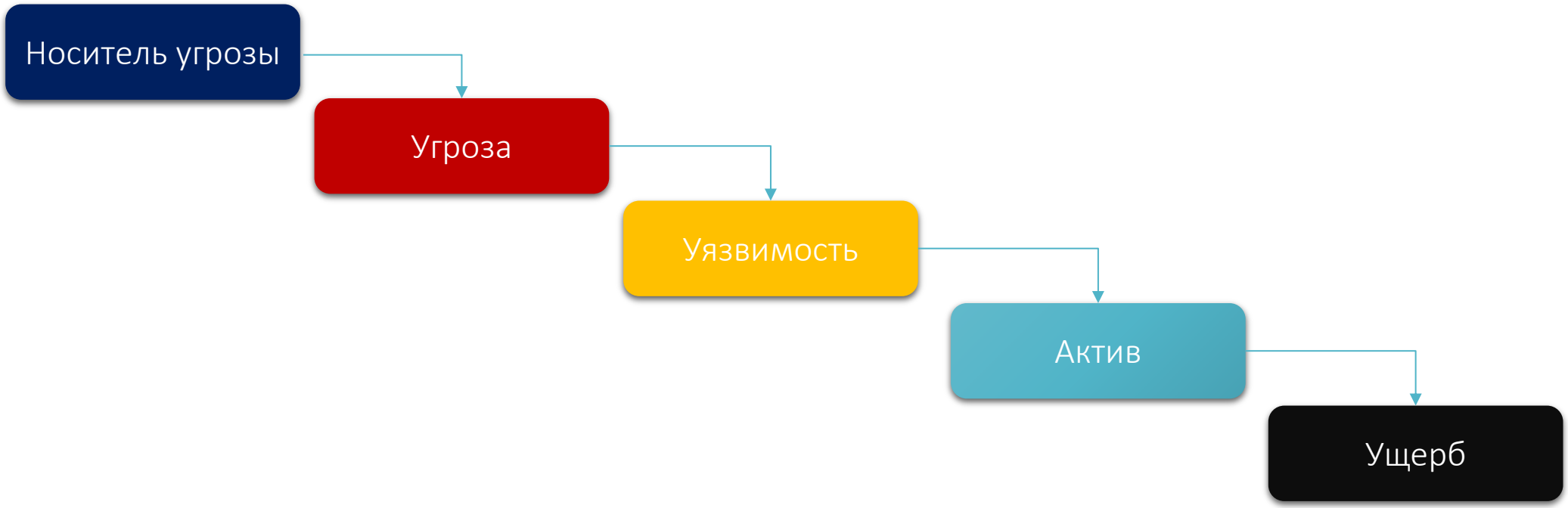



Стоимость 100
Безопасность – 100
Удобство 100

Стоимость 0
Безопасность – 100
Удобство 0

# Анализ рисков

РИСК = Вероятность X Ущерб



# Количественный подход

Вероятность осуществления угрозы
на основе статистики и исторических наблюдений.

Величина ущерба на основании  (Восстановительной, полной, остаточной) стоимости.

Что делать с нематериальными активами?

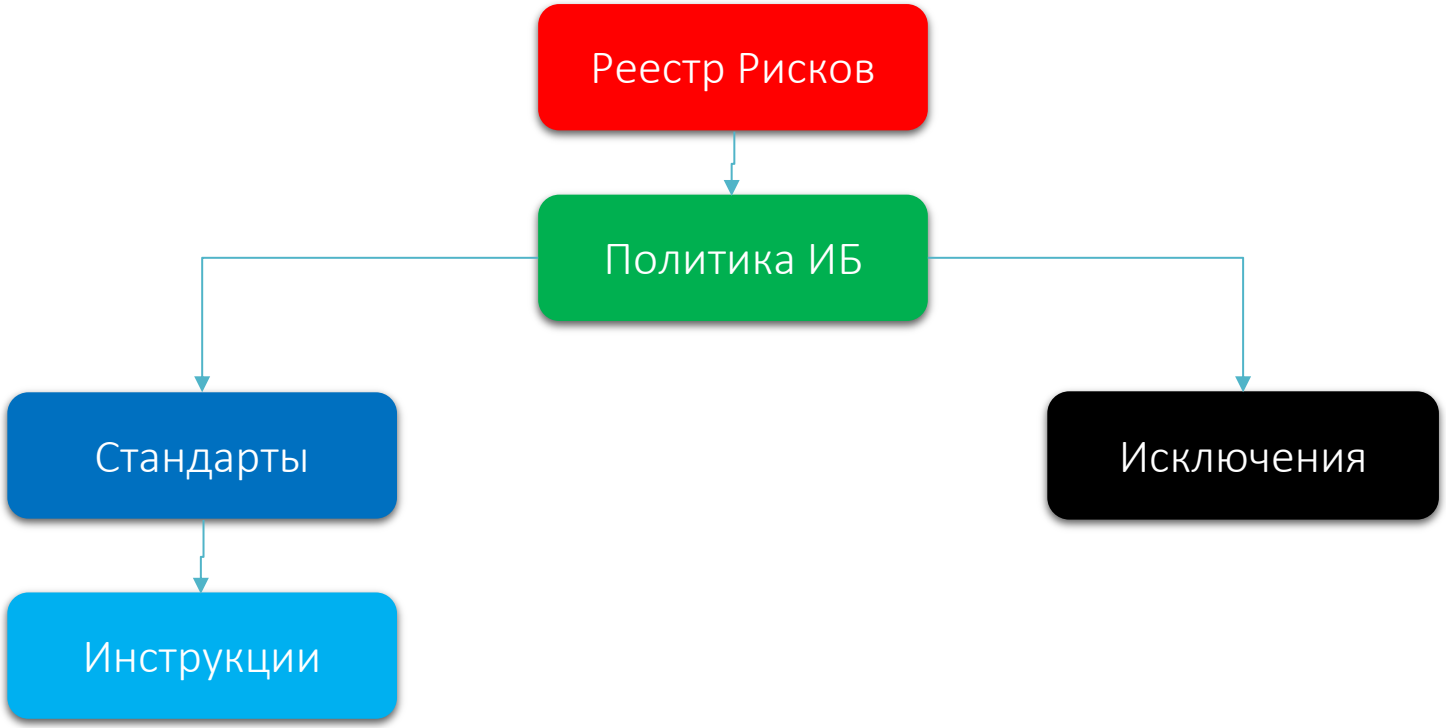
# Качественный подход

# Работа с риском

Что можно сделать?

- Уменьшить
- Передать
- Отказаться
- Принять

# Политика ИБ


Реестр Рисков
Политика ИБ
Стандарты
Исключения
Инструкции

# Обучение сотрудников

Тренинги  по применению политики ИБ

Средства защиты используемые в компании

Как защищать информацию

Что такое  социальная инженерия

Фишинговая кампания

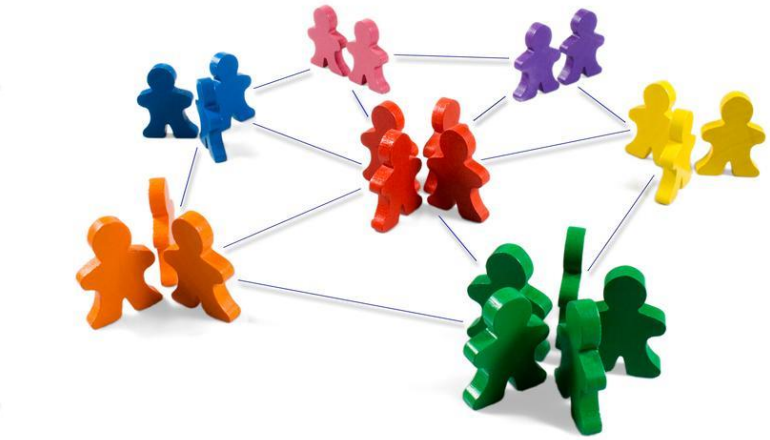
# Классификация информации

Публичная информация

Конфиденциальная информация

Конфиденциальная информация: персональные данные

Конфиденциальная информация: ограниченый доступ



# Защита от утечек информации

Системы защиты от утечек

- Хорошо описываемая информация или
- Цифровые отпечатки

- Проверка открытых каналов
- Поддержка клиентских устройств
- Поддержка зашифрованных каналов

# Шифрование информации

Шифрование  носителей

Шифрование устройств

Шифрование файлов

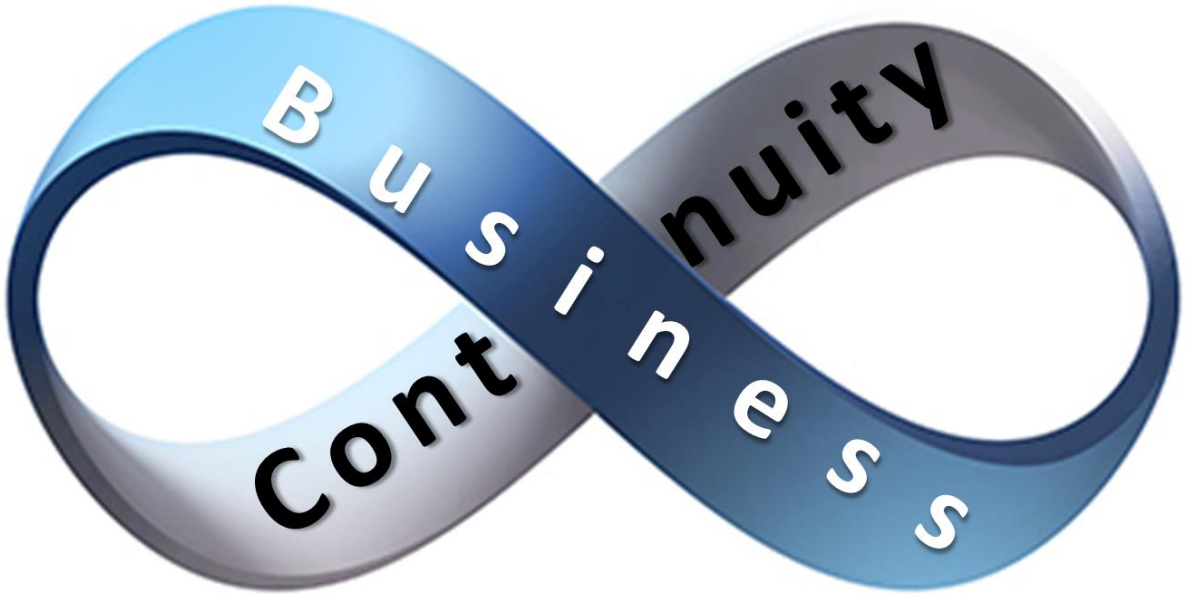
Шифрование  объектов

# Непрерывность бизнеса


Факторы для планирования:

- Оборудование
- Помещения
- Люди
- Контрагенты- поставщики

- Схемы резервирования
- Горячая
- Теплая
- Холодная



# План по востановлению

Оповещение руководства и сотрудников

Эвакуация сотрудников и минимизация потерь

Востановление работы  по одной из схем резервирования

Запуск востановительных работ
основной площадки (бизнес- процесса)

**NB: План необходимо тестировать не реже 1 раза**

# Аудит  Э и И Безопасности

Внешний и Внутренний аудит

Соответвие Политике ИБ, Стандартам ИБ

Тестирование на проникновение:

- Черный ящик
- Серый ящик
- Прозрачный ящик

# Стандарты ИБ

ISO 27000

PCI DSS 3.0

Common Criteria

ГОСТ


# Защита  Облачных сервисов  (SAAS)

Cloud Access Brokers

- Интеграция с API
- Использование прокси
- Использование шифрования при сохранение данных

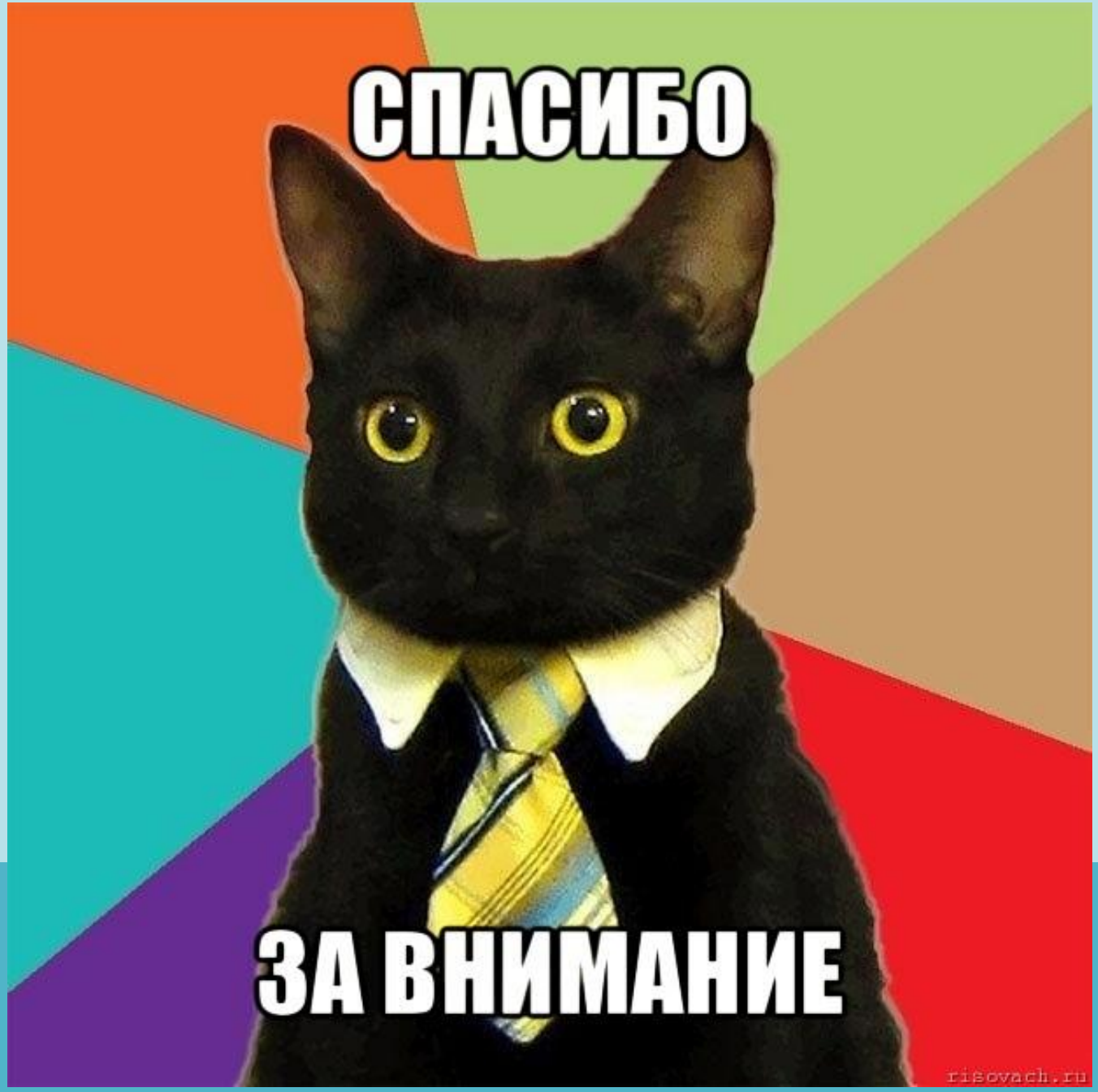
# Защита  мобильных устройств

Системы управления мобильными устройствами

Системы управления  мобильными приложениями

Системы управления  информацией на мобильных устройствах


Вопросы!


СПАСИБО
ЗА ВНИМАНИЕ
risovach.ru