denovo

Вдохновляясь Будущим

# Безопасность в виртуальных и облачных средах:

## новые подходы к решению старой задачи

Тарас Мандрик
Системный архитектор

# Трансформация IT-инфраструктуры

# Мотивация

denovo
Вдохновляясь Будущим

**Чего мы хотим (ИТ)?**

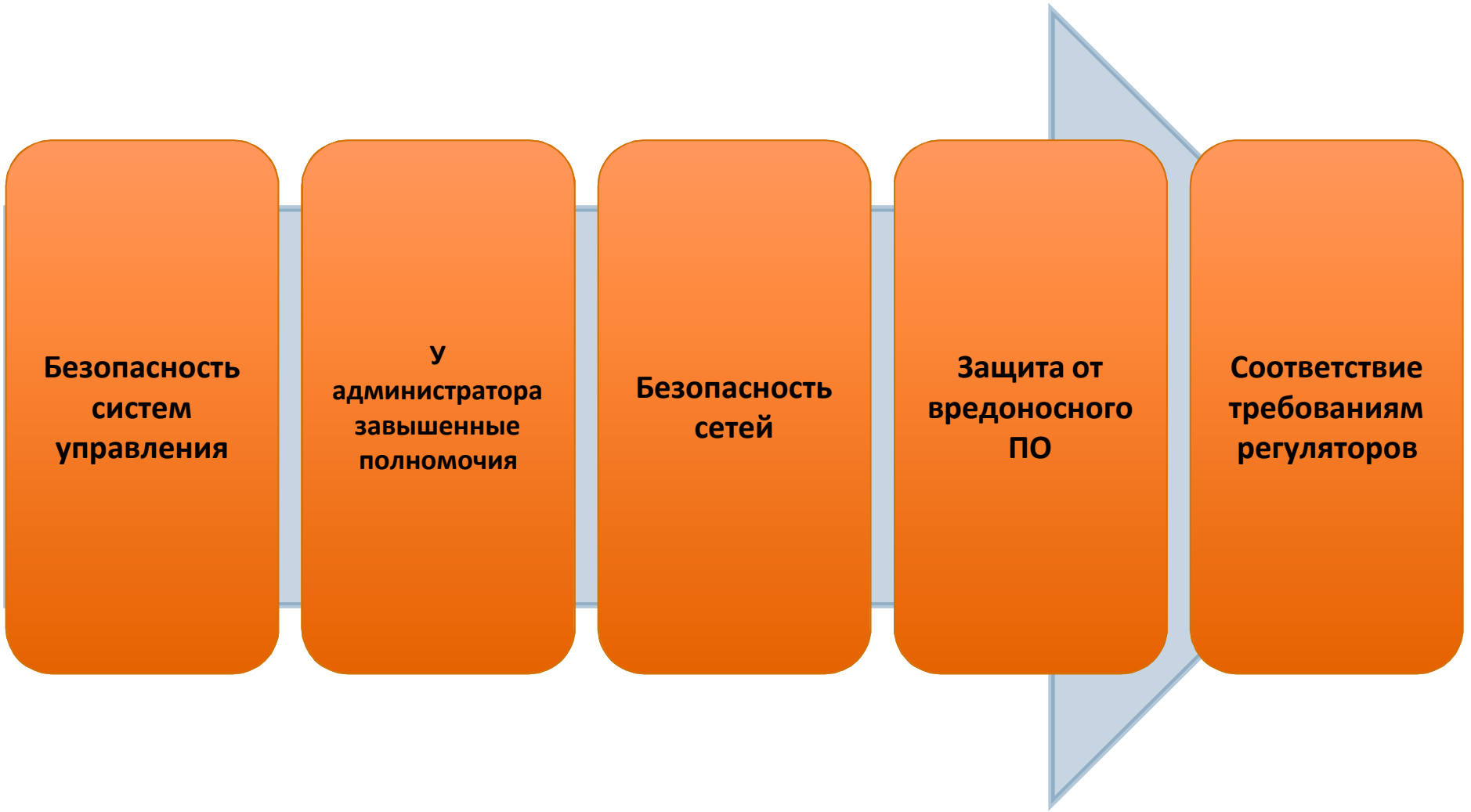
- Сервисы должны быть доступными
- Инфраструктура должна отнимать минимум внимания
- Создавать ВМ без сложных согласовательных процедур, регламентов
- Чтобы нам не мешали при внедрении и эксплуатации

**Чего хотят они (ИБ)?**

- ЦОД должен быть защищен
- Соблюдение корпоративных стандартов
- Выполнение требований регуляторов
- Спецсредства контроля
- Вовремя участвовать в проекте, понимать как это устроено

# Какие беспокойства у службы ИБ?

denovo
Вдохновляясь Будущим



# Безопасность гипервизора

denovo
Вдохновляясь Будущим

- **Безопасность систем управления**
- У администратора завышенные полномочия
- Безопасность сетей
- Защита от вредоносного ПО
- Соответствие требованиям регуляторов

## **Гипервизор** ESXi

- Небольшой объем = меньше площадь для уязвимости
- Компоненты Vmware и сторонние компоненты можно обновлять независимо

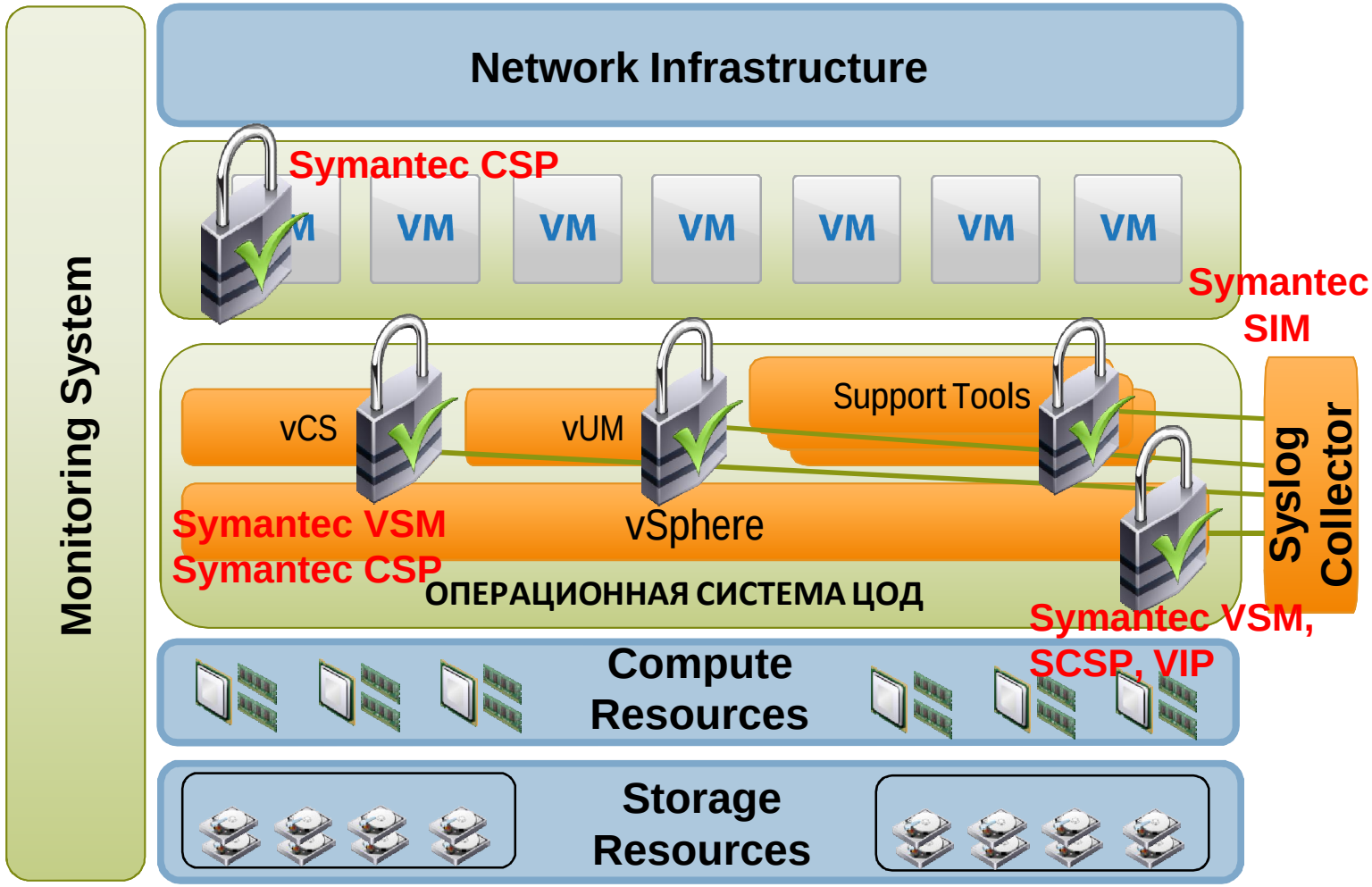
Пока не обнародовано ни одного случая взлома гипервизора или нарушения изолированности ВМ

Можно получить доступ к гипервизору через средства управления

# Безопасность системы управления виртуализацией

denovo
Вдохновляясь Будущим

- Безопасность систем управления
- У администратора завышенные полномочия
- Безопасность сетей
- Защита от вредоносного ПО
- Соответствие требованиям регуляторов



# Контроль действий администратора

denovo
Вдохновляясь Будущим


- Двойной контроль для критически важных операций (Symantec Virtualization Security Manager)
- Защита от бесконтрольного использования root-доступа (Symantec Virtualization Security Manager)
- Обнаружение инцидентов (Symantec VSM/CSP/SSIM)

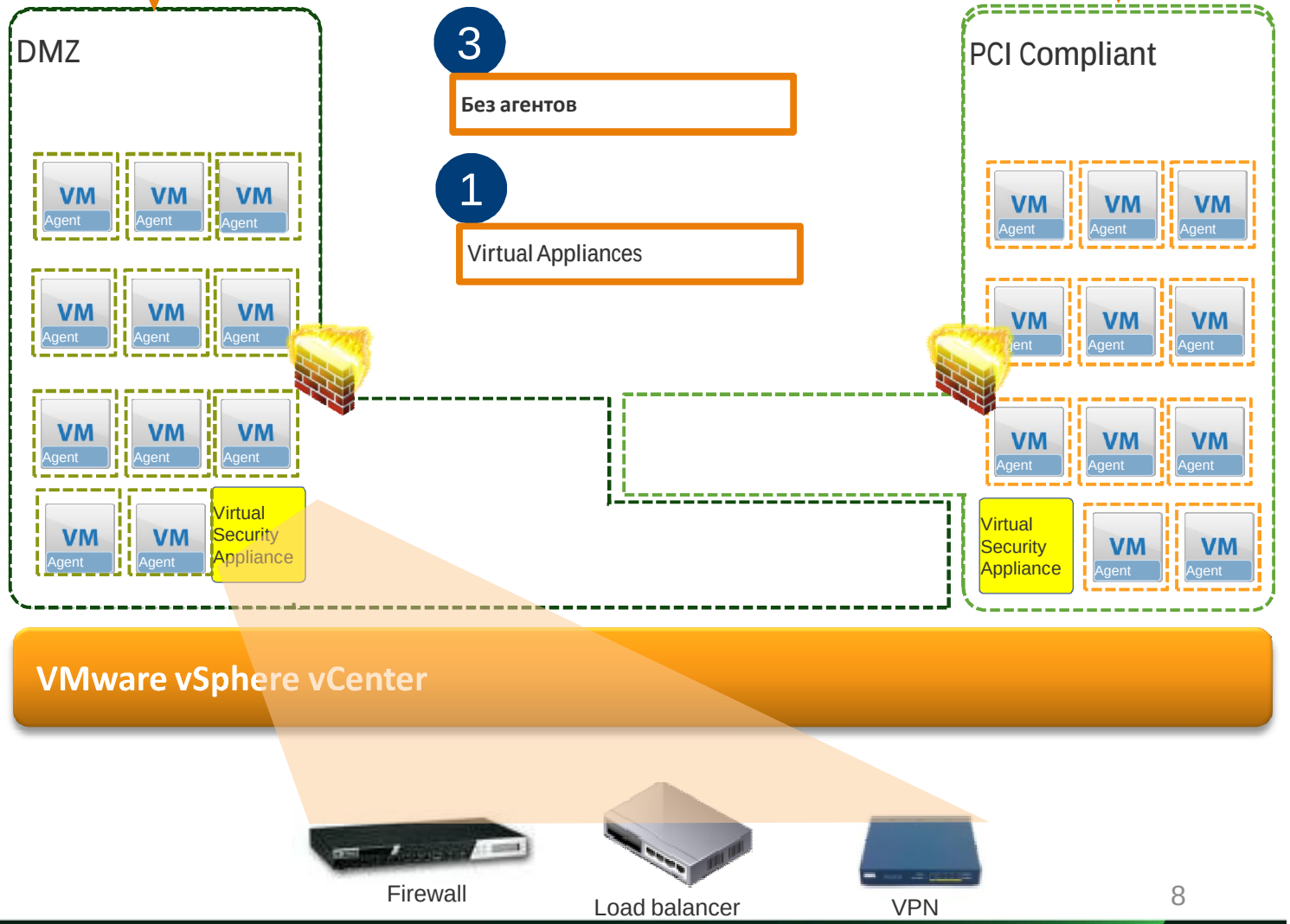
# Безопасность виртуальных сетей

denovo
Вдохновляясь Будущим

- Безопасность систем управления
- У администратора завышенные полномочия
- **Безопасность сетей**
- Защита от вредоносного ПО
- Соответствие требованиям регуляторов

2 Каждая ВМ защищается firewall, действующим на уровне гипервизора

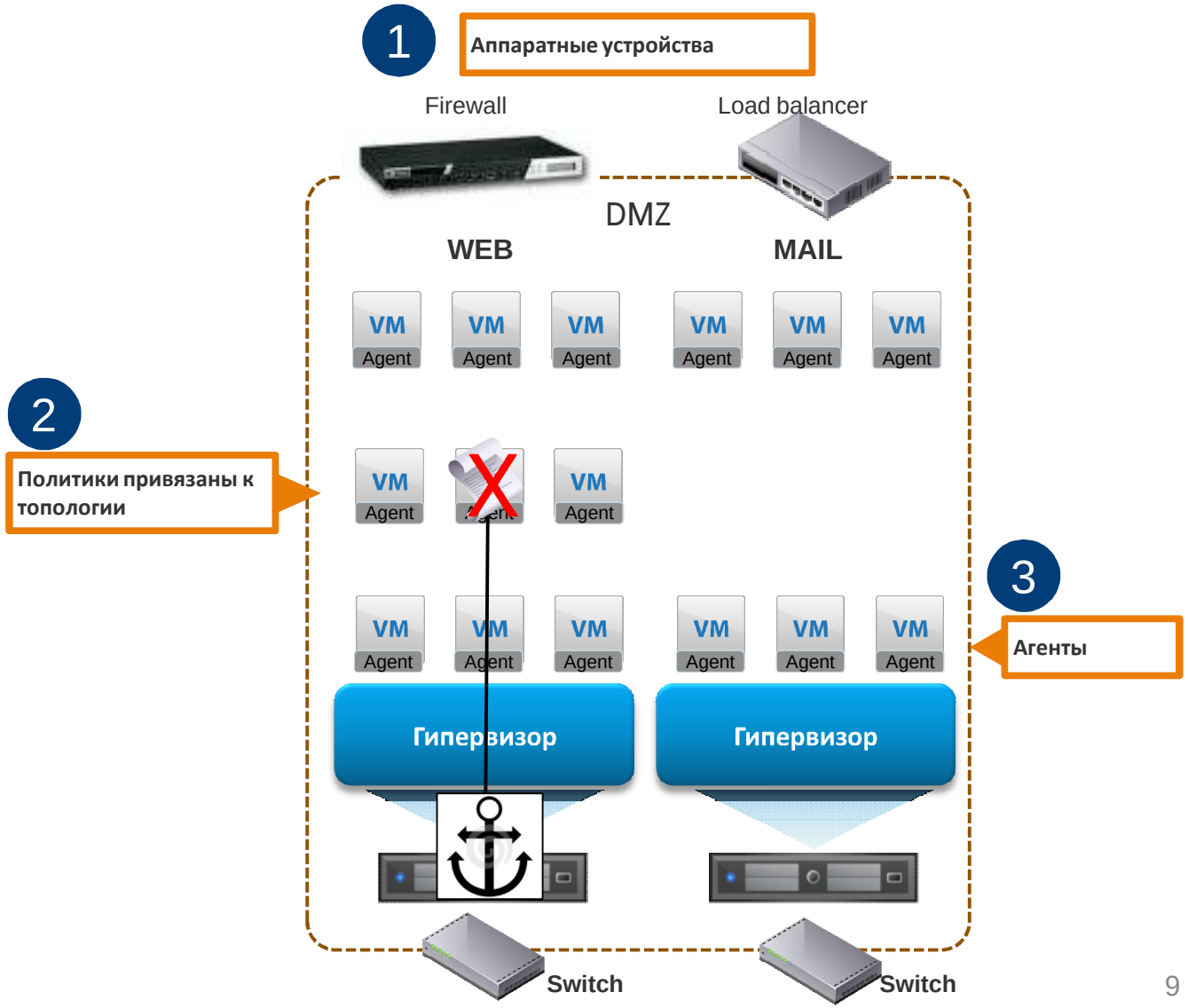
Политики основаны на логических зонах доверия



# При традиционном подходе

denovo
Вдохновляясь Будущим

- Безопасность систем управления
- У администратора завышенные полномочия
- **Безопасность сетей**
- Защита от вредоносного ПО
- Соответствие требованиям регуляторов



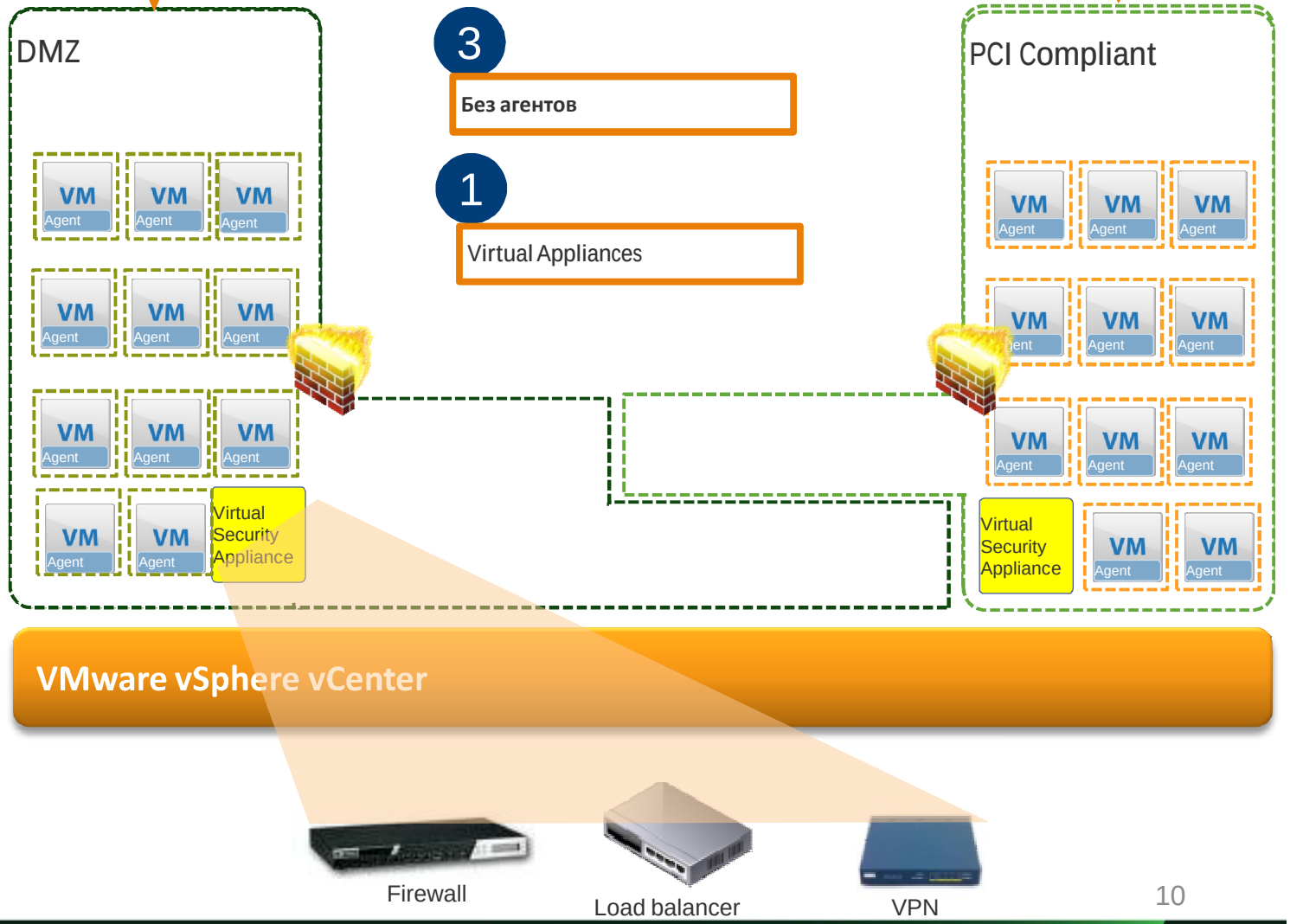
# Безопасность виртуальных сетей

denovo
Вдохновляясь Будущим

- Безопасность систем управления
- У администратора завышенные полномочия
- **Безопасность сетей**
- Защита от вредоносного ПО
- Соответствие требованиям регуляторов

2 Каждая ВМ защищается firewall, действующим на уровне гипервизора

Политики основаны на логических зонах доверия

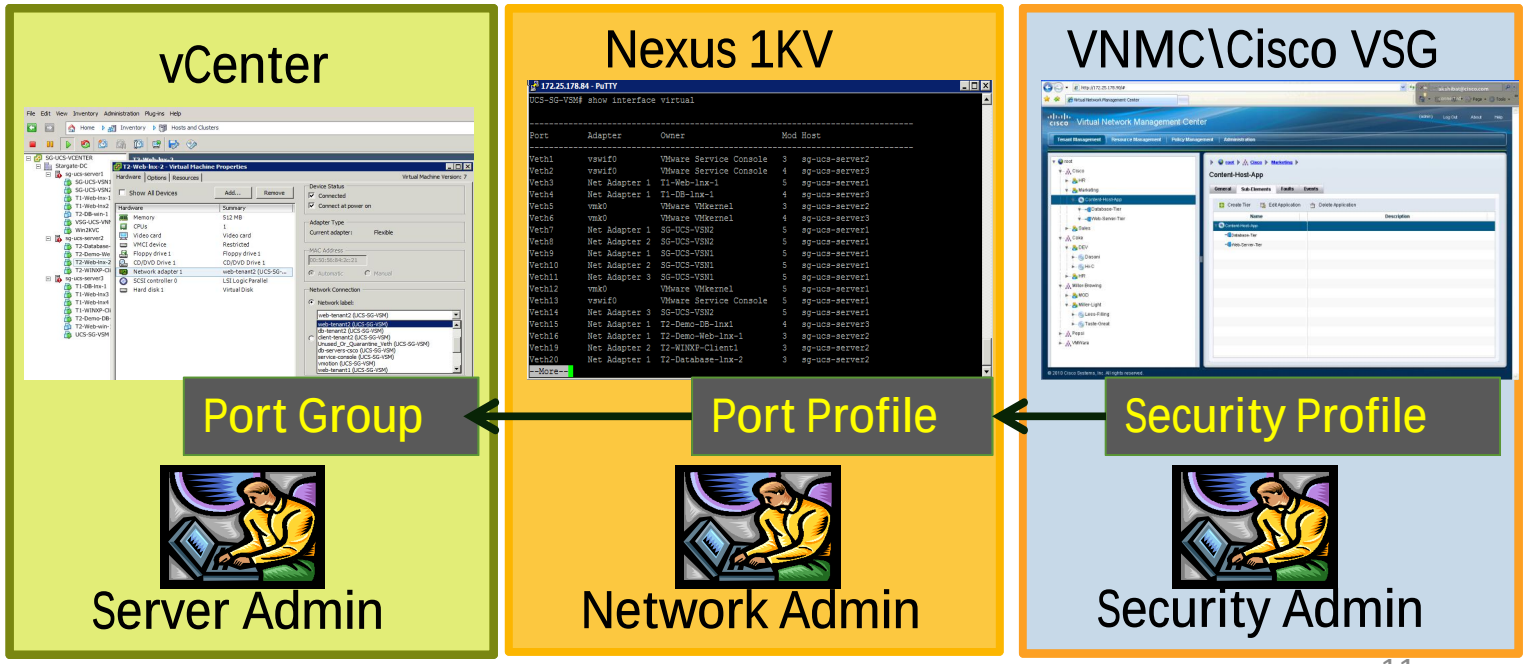


# Безопасность виртуальных сетей

denovo
Вдохновляясь Будущим

- Безопасность систем управления
- У администратора завышенные полномочия
- **Безопасность сетей**
- Защита от вредоносного ПО
- Соответствие требованиям регуляторов

- Подразделение информационной безопасности определяет политики
- Сетевые администраторы привязывают профили портов к политикам безопасности
- Администраторы серверов подключают ВМ к профилям портов на Nexus 1000V

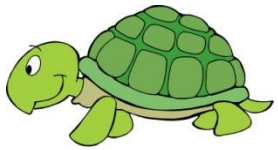


# Традиционный антивирус

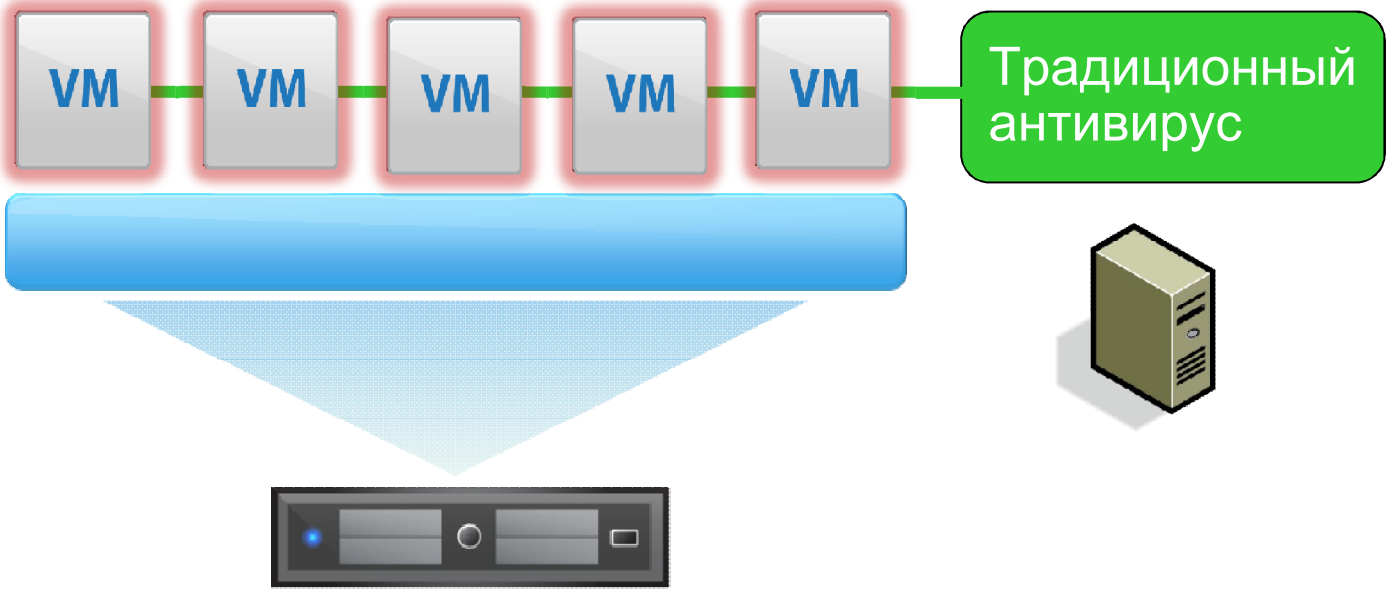
denovo
Вдохновляясь Будущим

- Безопасность систем управления
- У администратора завышенные полномочия
- Безопасность сетей
- **Защита от вредоносного ПО**
- Соответствие требованиям регуляторов

§ Конкуренция за ресурсы



Сканирование в 15:00 дня

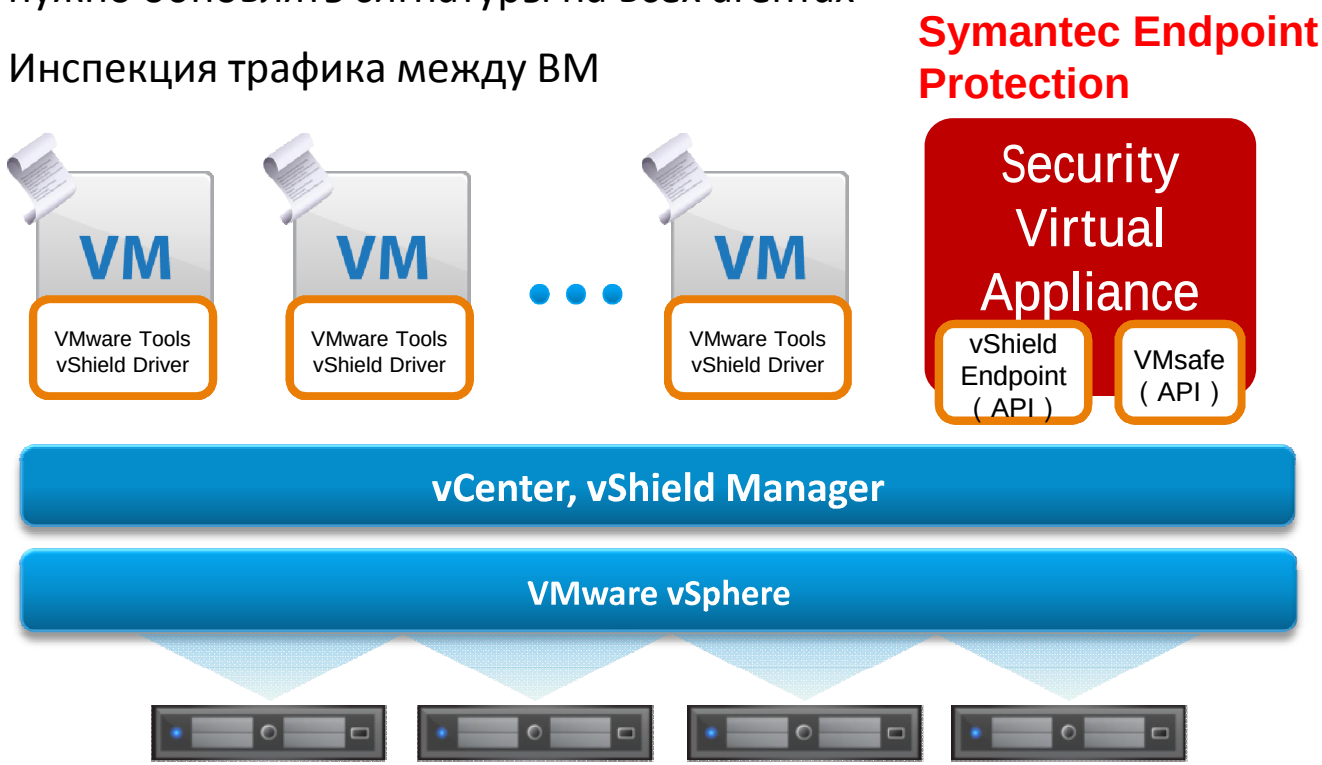


# Антивирус для виртуальных сред

denovo
Вдохновляясь Будущим

- Безопасность систем управления
- У администратора завышенные полномочия
- Безопасность сетей
- **Защита от вредоносного ПО**
- Соответствие требованиям регуляторов

- Проще управление: не нужно устанавливать агенты, обновлять их
- Надежнее защита: защита при включении ВМ, невозможно отключить защиту
- Лучше производительность: нет одновременных проверок, не нужно обновлять сигнатуры на всех агентах
- Инспекция трафика между ВМ



# Автоматическая проверка на соответствие

denovo
Вдохновляясь Будущим

Безопасность систем управления

У администратора завышенные полномочия

Безопасность сетей

Защита от вредоносного ПО

**Соответствие требованиям регуляторов**

1

Предопределенные шаблоны

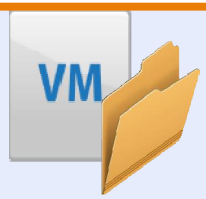
SOX | HIPAA | PCI DSS | ... | NIST | PCI DSS | NERC/ FERC

2

Мониторинг данных и изменений

Непрерывное обследование

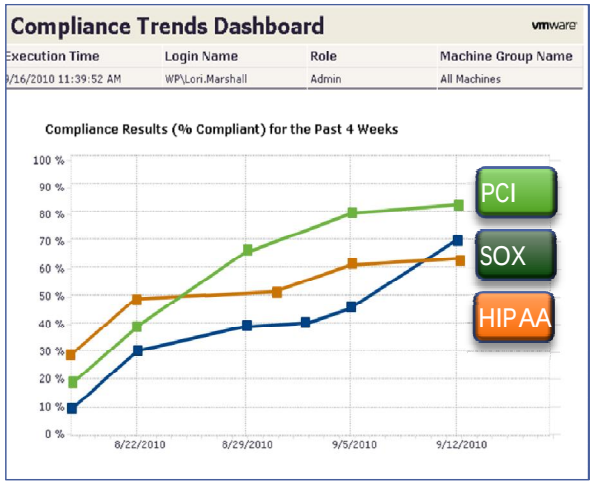
Автоматическое распространение

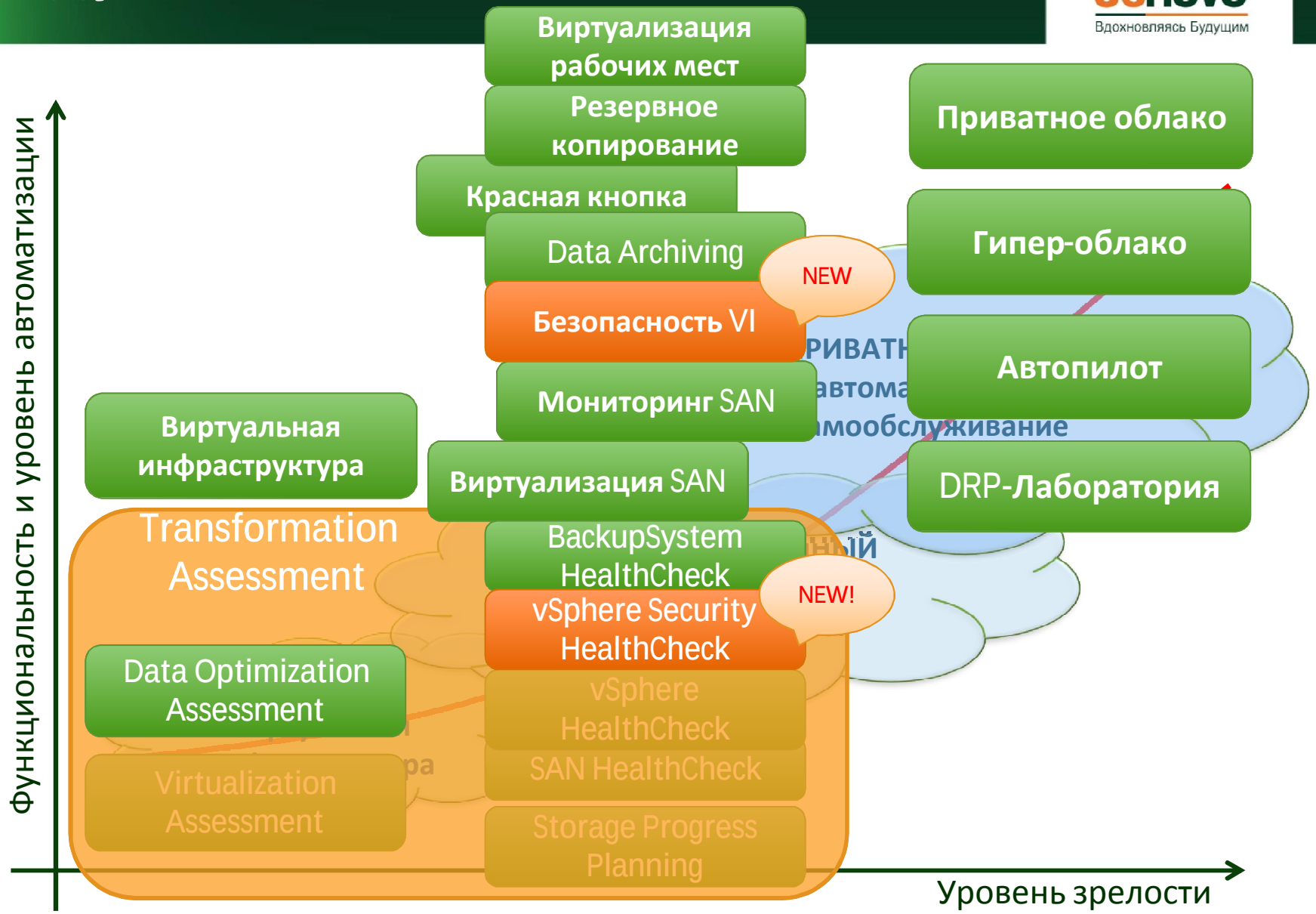



3

Автоматические отчеты



# Продукты De Novo 2013



# De Novo - Ваш помощник

denovo
Вдохновляясь Будущим

- **Мы построили Коммерческое Облако** промышленного класса. Вопросы безопасности нам не чужды.
- **Компетенции по широкому набору базовых технологий вендоров** позволяют использовать именно то, что максимально удовлетворяет требования каждого Заказчика
- **Проектный подход** компании и фирменная методология проектного производства гарантируют успех начинания

**Нужна помощь в эффективной защите виртуальной инфраструктуры?**
**Обратитесь к профессионалам!**