

# CSO Summit 2010

Москва, Конгресс-центр МТУСИ, 23 МАРТА 2010



Код безопасности  
ГК «Информзащита»

## ВИРТУАЛИЗАЦИЯ: ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**АЛЕКСАНДР ШИРМАНОВ**

Генеральный директор ООО "Код Безопасности"



# ГК «Информзащита»

Информзащита  
Группа компаний

- **«Код Безопасности»** – разработчик ПО и аппаратных средств ИБ, входит в ГК «Информзащита»
- **ГК «Информзащита»** - крупнейший российский специализированный холдинг ИБ, входящий в CNews 100
- **Более 10 лет на рынке ИБ**
- Компании группы и продукты собственного производства имеют **все необходимые лицензии и сертификаты:**

□ ФСТЭК России

□ ФСБ России

□ Минобороны

□ СВР России



# Информационная безопасность виртуальных серверов

- “40% виртуальных машин устанавливаются без участия специалистов по информационной безопасности”<sup>1</sup>
- “К концу 2012 года 60% виртуальных серверов окажутся менее защищенными, чем физические сервера”<sup>1</sup>
- На виртуальную среду распространяются требования законодательства РФ в области защиты информации

1. **Источник:** Gartner, Inc., Press Release “Addressing the Most Common Security Risks in Data Center Virtualization Projects” от 25.01.2010



# Виртуализация и требования законодательства РФ

- Требования применяются, если в виртуальной среде обрабатывается **информация ограниченного доступа**
  - Государственная тайна
  - Конфиденциальная информация
  - Банковская, коммерческая и др. тайны
  - Персональные данные

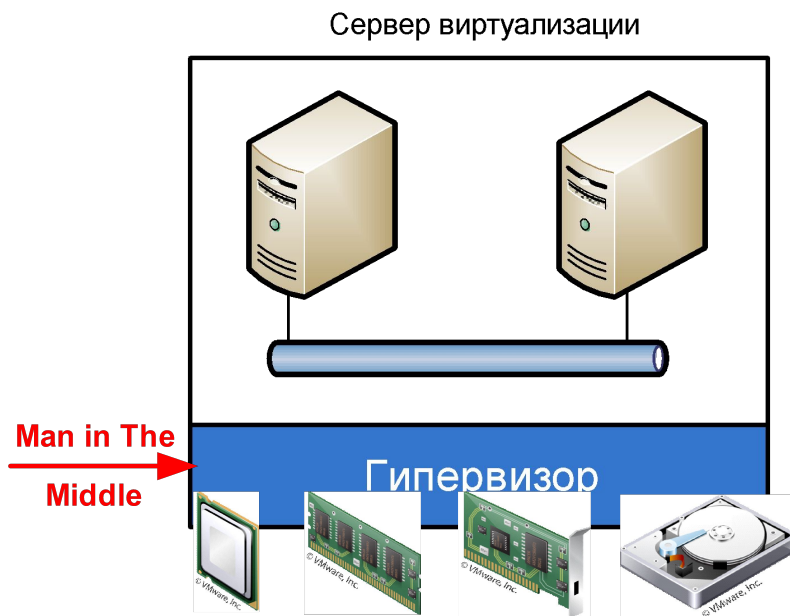


# Требования к средствам защиты информации (СЗИ) при обработке персональных данных

- **Постановление Правительства РФ №781:**
  - п. 5. “СЗИ, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия”
  - п.18: “Результаты оценки соответствия СЗИ... оцениваются в ходе экспертизы ФСТЭК/ФСБ”
  - п. 19: ”К СЗИ... прилагаются правила пользования, согласованные с ФСТЭК/ФСБ”
  - п. 20: “СЗИ подлежат учету в соответствии порядком, определенным ФСТЭК/ФСБ”
- **Приказ ФСТЭК №58 от 05.02.2010:**
  - п. 7: “Для ИСПДн 1 класса применяются СЗИ, соответствующее НДВ4”
- **Нормативные документы ФСТЭК и ФСБ**

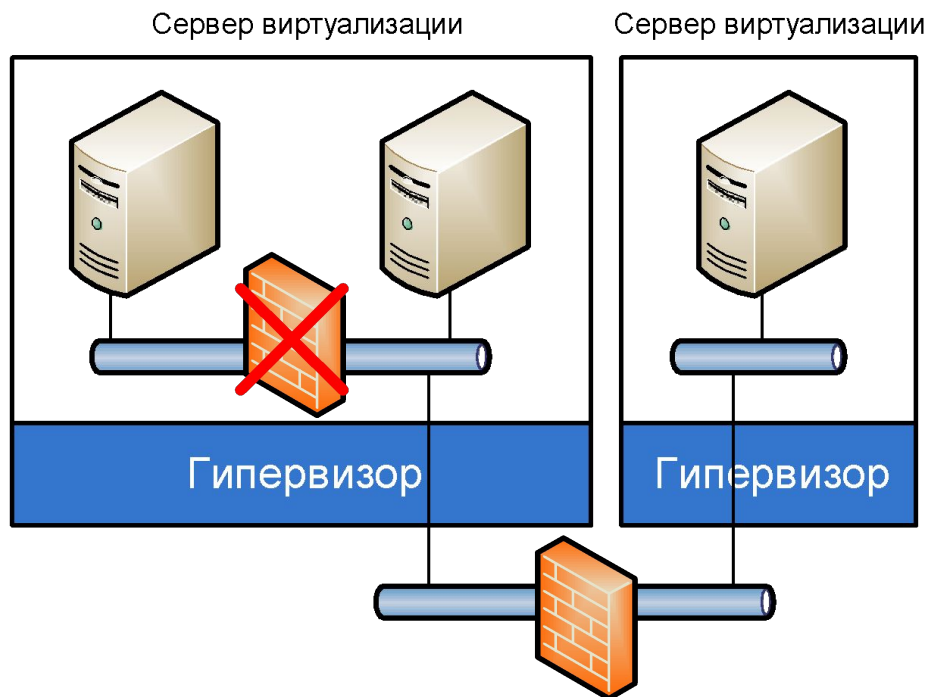


# Виртуализация: примеры угроз



- Гипервизор управляет основными ресурсами
- При компрометации, гипервизор = «человек в середине»

# Виртуализация: примеры угроз

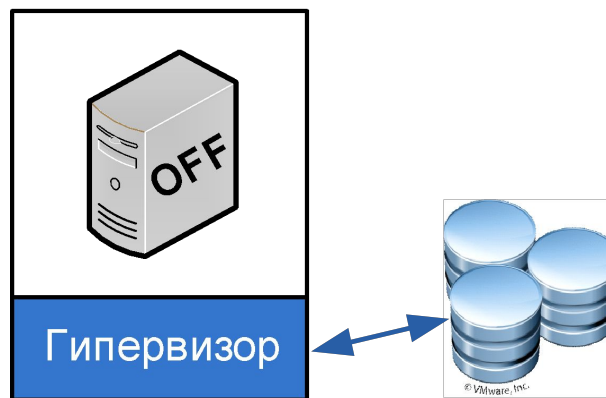


- Часть трафика “виртуализуется”
- Традиционные МЭ становятся не везде применимы



# Виртуализация: примеры угроз

Сервер виртуализации

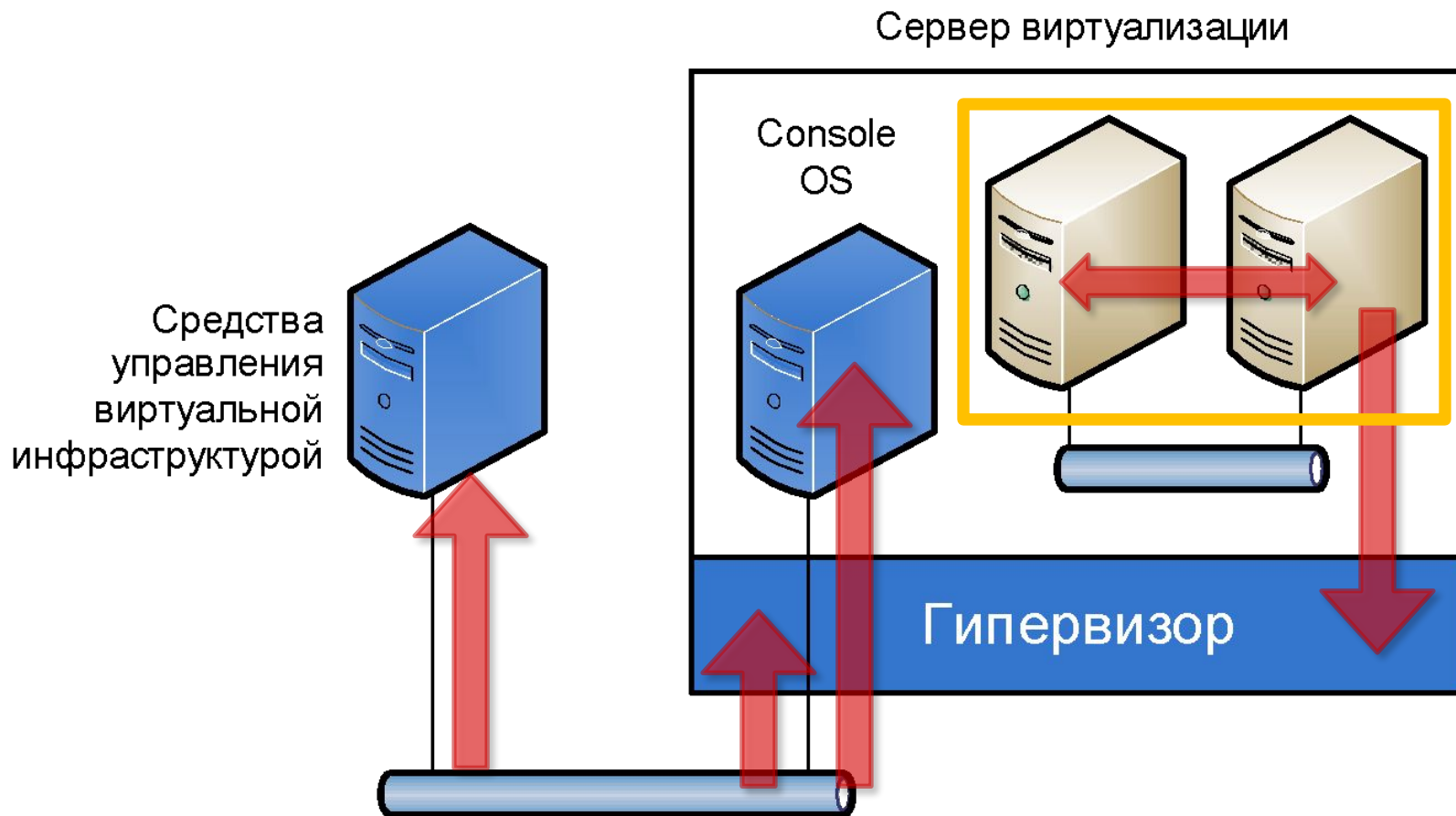


- Хранилище данных виртуальных машин физически отделено от места их обработки
- Гипервизор может читать и изменять данные виртуальных машин даже когда они не работают

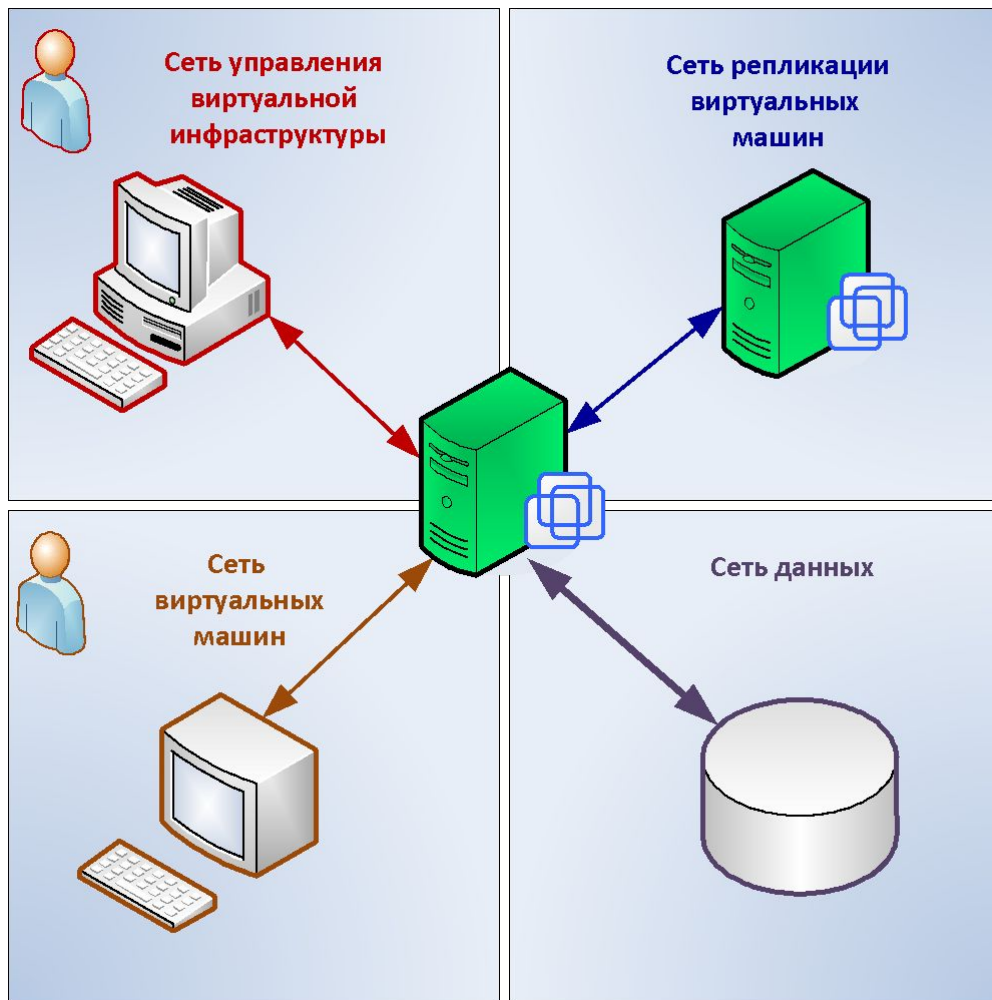




# Виртуализация: примеры атак

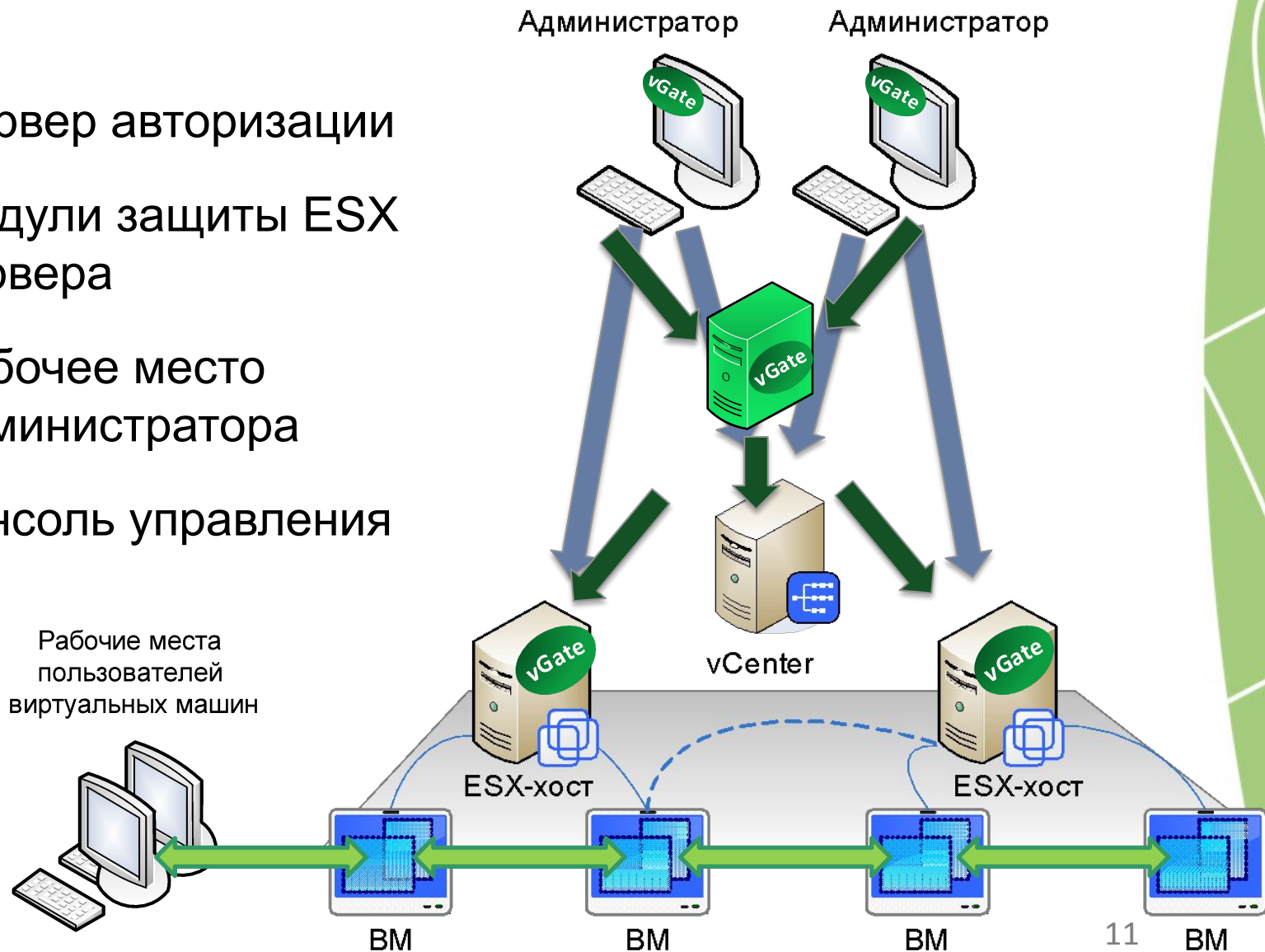


# Развертывание серверов виртуализации с точки зрения ИБ

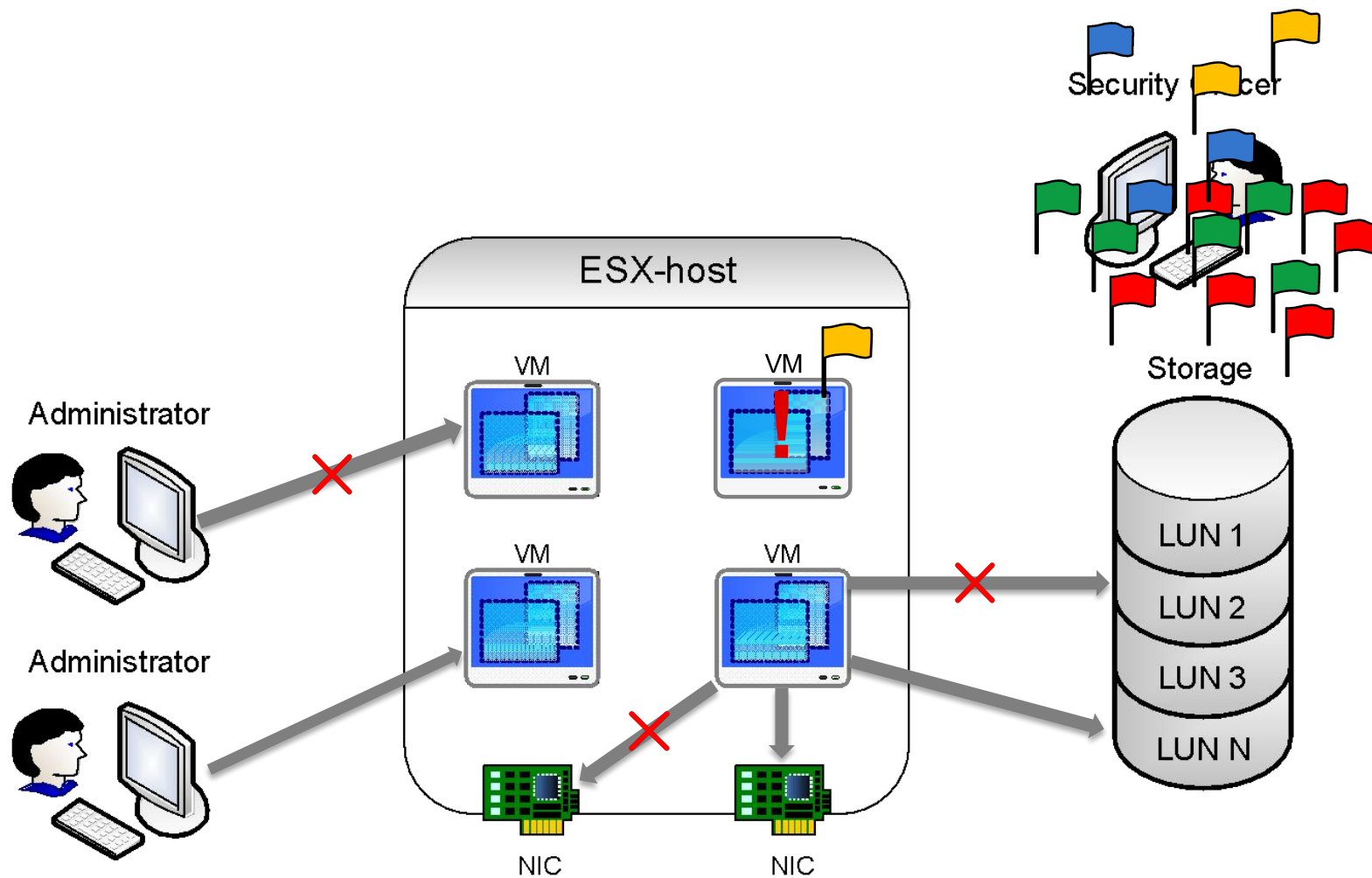


# vGate: КОНТРОЛЬ ДОСТУПА К ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ

- Сервер авторизации
- Модули защиты ESX сервера
- Рабочее место администратора
- Консоль управления



# vGate 2.0: SOD и RBAC



# vGate: сертификация

- **vGate 1.0: СВТ 5 и НДВ4 (сертификат ФСТЭК №2061)**
  - **позволяет использовать продукт для защиты АС до класса 1Г включительно (конфиденциальная информация) и в информационных системах персональных данных до 1 класса включительно**
- **vGate 2.0: СВТ 3 и НДВ 2**  
(выпуск и сертификация во втором полугодии 2010)
  - **позволит применять в АС до 1Б включительно и обрабатывать государственную тайну до “СС” включительно**



# Нам доверяют защиту своей информации

Центральный Банк  
ГАС «Выборы»  
Министерство финансов  
Федеральное казначейство  
ОАО «Вымпелком»  
ОАО «Внешторгбанк»  
Региональные управления  
Банка России и Сбербанка  
Росэнергоатом  
ГМК «Норильский никель»  
и т.д.





# CSO Summit 2010

Москва, Конгресс-центр МТУСИ, 23 МАРТА 2010

**СПАСИБО ЗА ВНИМАНИЕ!  
ВОПРОСЫ?**

**АЛЕКСАНДР ШИРМАНОВ**

Генеральный директор

- +7 (495) 980-2345 (многоканальный)
- [a.shirmanov@securitycode.ru](mailto:a.shirmanov@securitycode.ru)
- [www.securitycode.ru](http://www.securitycode.ru)

