САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УЯЗВИМОСТИ ГИПЕРВИЗОРОВ И СИСТЕМ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

конференция
РусКрипто'2013

http://www.ruscrypto.ru/conference/

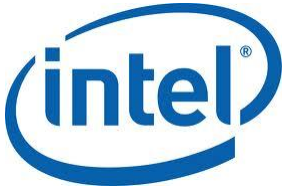
Д. т. н., профессор Зегжда Дмитрий Петрович
Никольский Алексей Валерьевич

Облачные вычисления

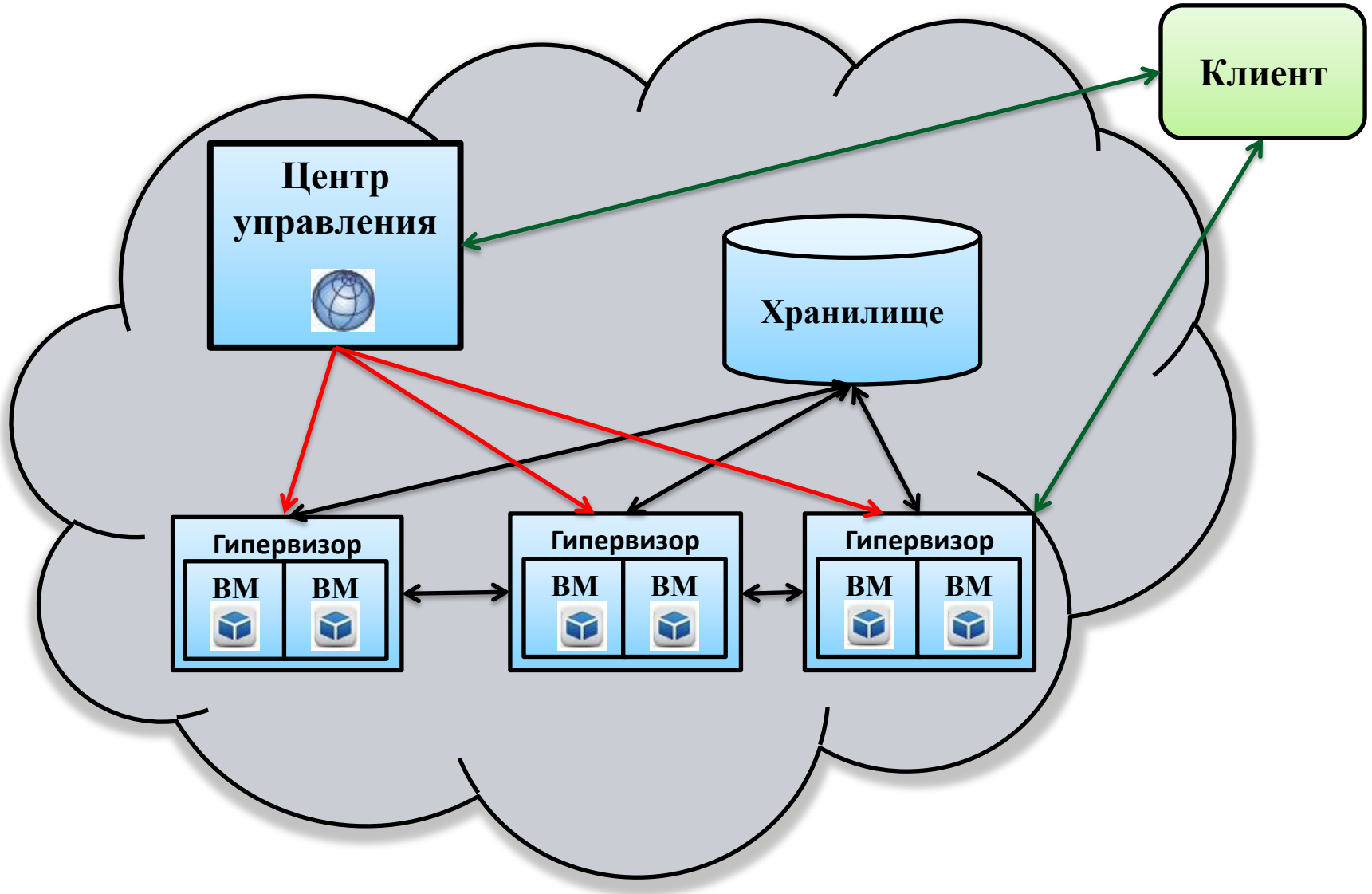
- **Платформы**

- **Гипервизоры**

- **Аппаратура**



Типовая архитектура облака



Облачные сервисы

SaaS (программное обеспечение как сервис)	Пользователи работают с конкретными приложениями, запущенными одновременно во многих виртуальных машинах в облаке
PaaS (платформа как сервис)	Пользователи имеют возможность создавать собственные приложения и программы, которые затем работают во многих виртуальных машинах одновременно
IaaS (инфраструктура как сервис)	Пользователи работают с виртуальными машинами в облаке, с возможностями изменения их конфигурации и установке в них любого программного обеспечения

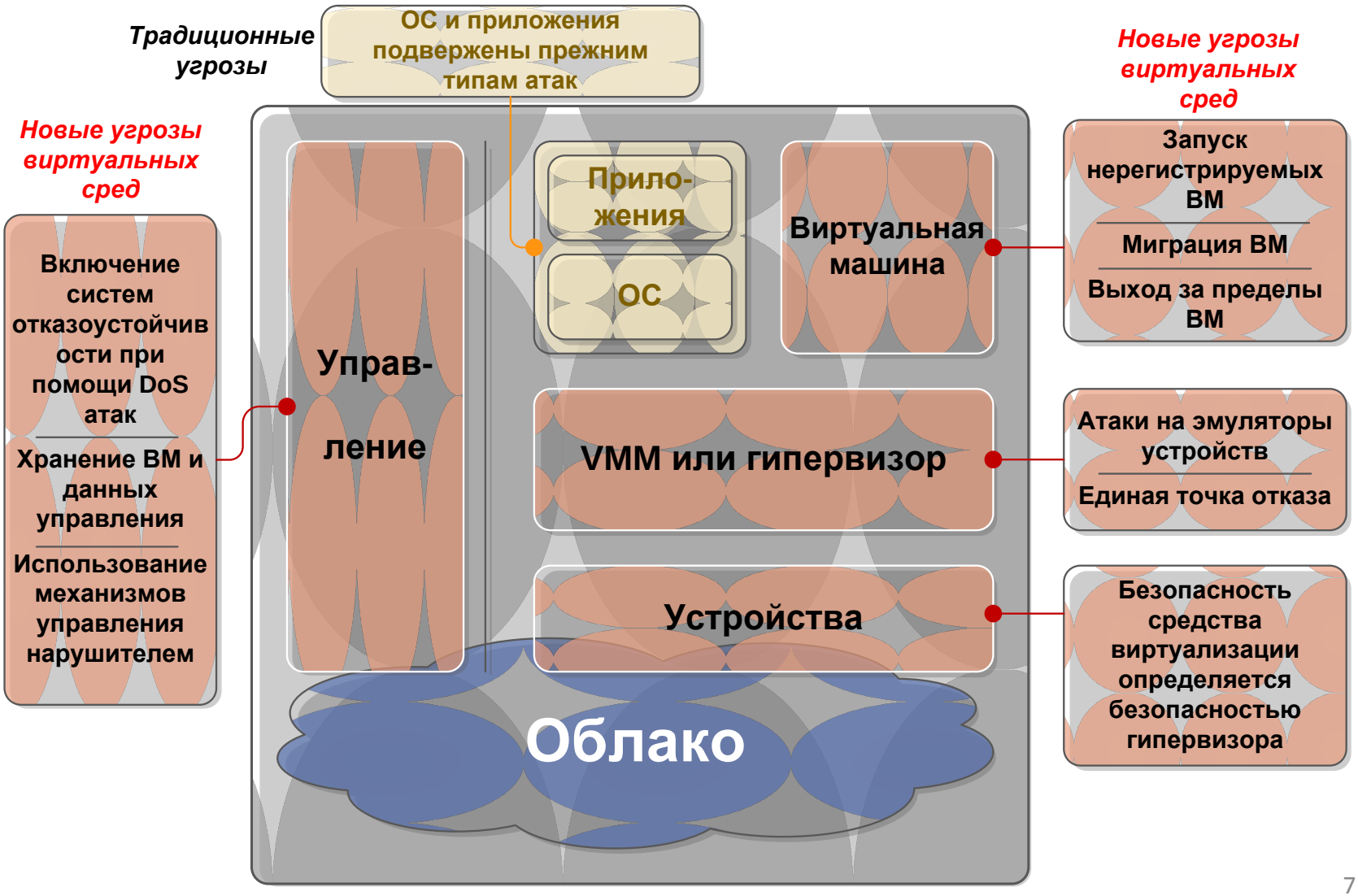
Исследование безопасности облаков

- Публичные облака подвержены атакам со стороны легальных пользователей IaaS
- Используя виртуальные машины можно влиять на работу средств виртуализации и осуществлять атаки на облако
- Некоторые облака требуют сетевой доступ пользователей к гипервизорам

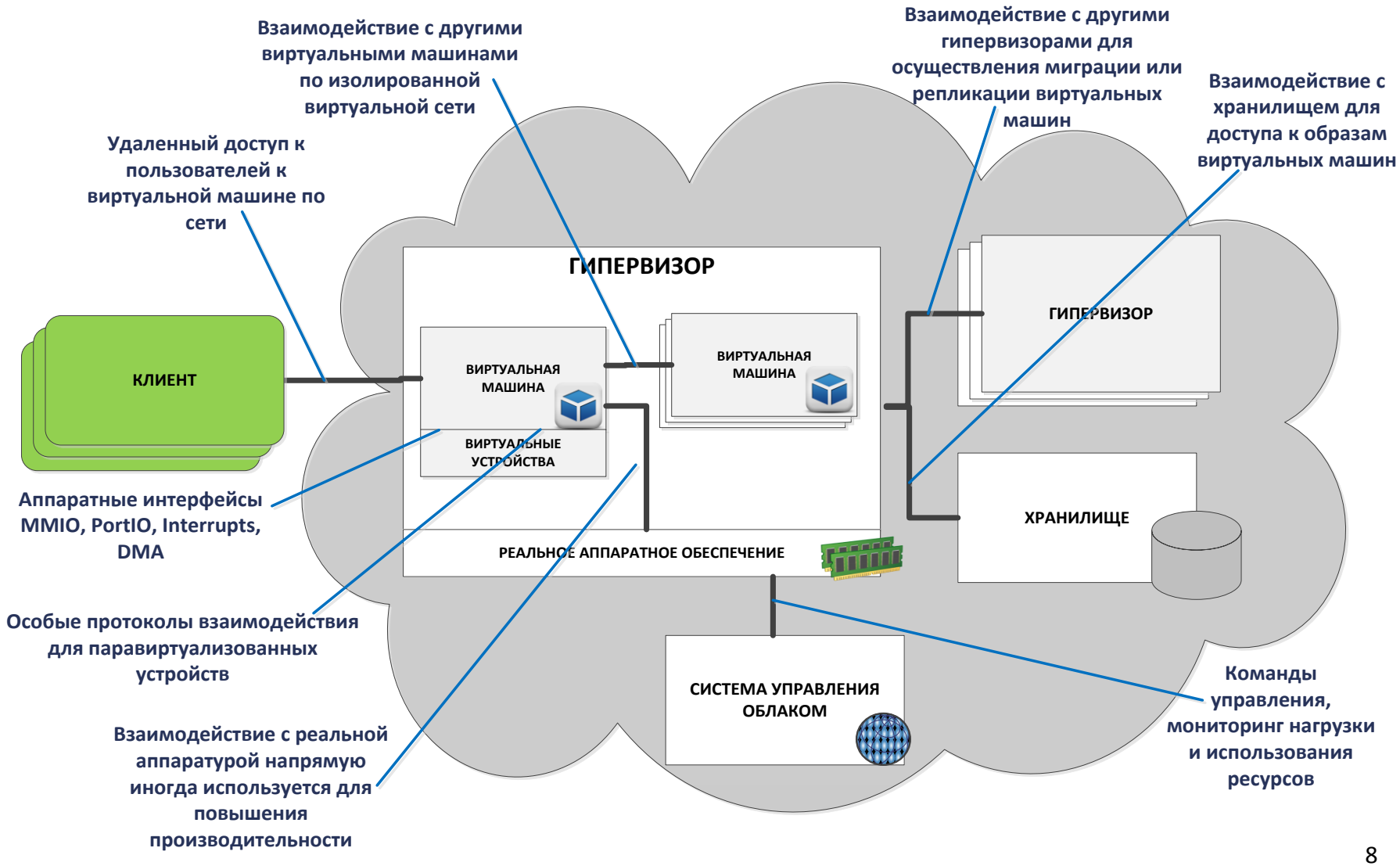
Методы исследования

- Проверка существующих уязвимостей
- Изучение исходного кода
- Анализ сетевого траффика

Анализ угроз гипервизора в облаке



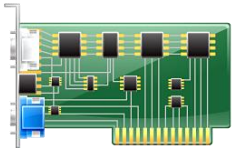
Роль гипервизора в облаке

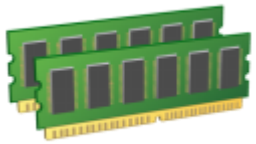


Как устроен гипервизор

- **Планировщик виртуальных машин**
  - *Средний размер 200 000 строк кода*

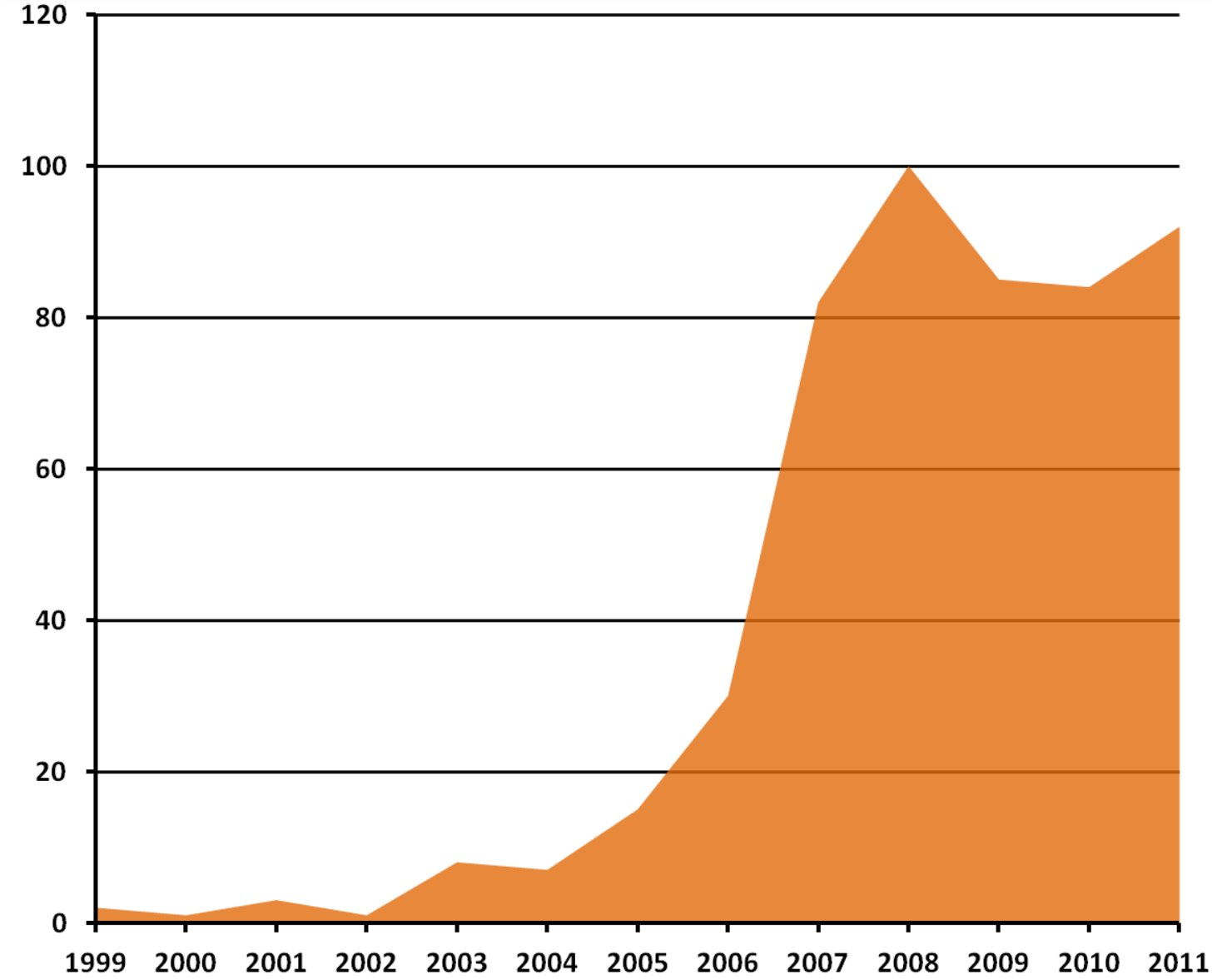
- **Эмуляторы устройств**
  - Оперативную память
  - Процессорное время
  - BIOS/EFI
  - Жесткий диск
  - Сетевые устройства
  - Системные устройства (таймеры, шины PCI, контроллеры прерываний, и др.)
  - Дополнительные устройства (видео карту, мышь, клавиатуру, и др.)





  - *Средний размер 500 000 строк кода*

Уязвимости в средствах виртуализации



Всего

553

уязвимости

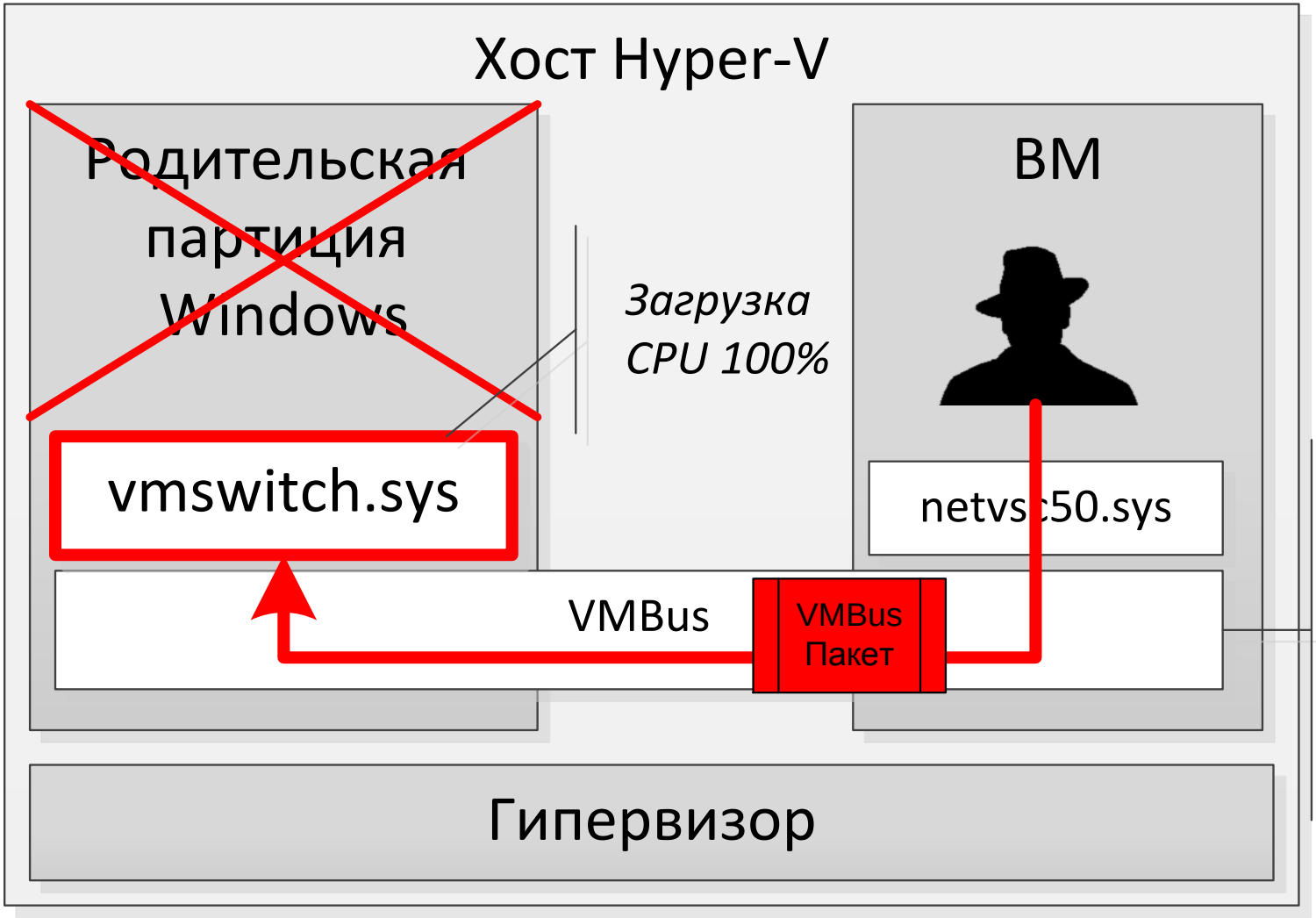
По данным
IBM XForce

Классификация уязвимостей средств виртуализации

Класс	Описание	Процент от общего числа уязвимостей
Воздействие на гипервизор	Нарушение работы гипервизора, нарушение работы ВМ	38%
Выход за пределы ВМ	Нарушение изоляции ВМ, внедрение кода в другие ВМ или гипервизор	35%
Воздействие на гостевую ОС	Нарушение работы гостевой ОС, внедрение кода в гостевую ОС	15%
Прочие	Нарушение работы средств управления средств виртуализации, нарушение работы вспомогательных программ	12%

По данным IBM XForce

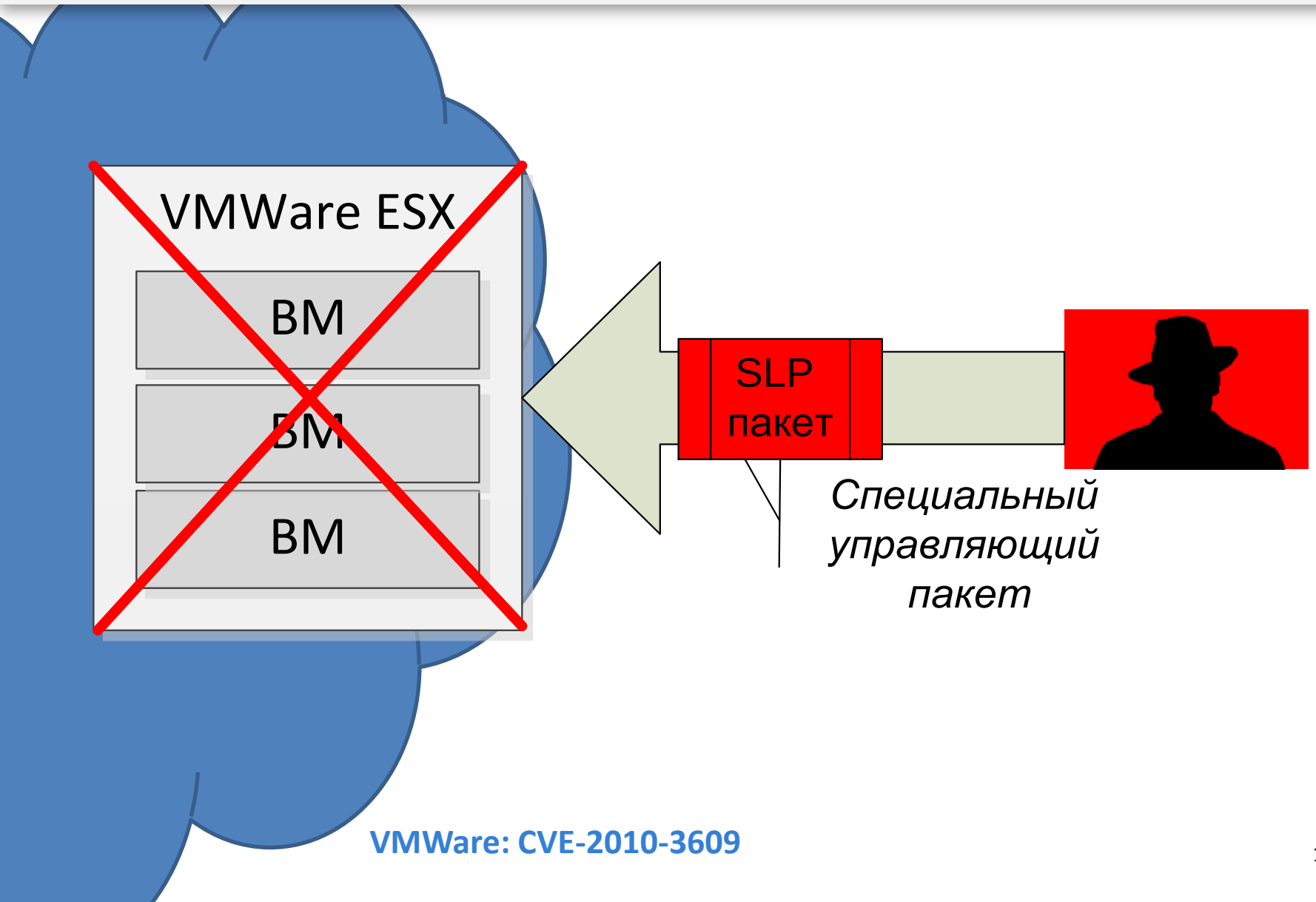
Воздействие на гипервизор: нарушение работы гипервизора Hyper-V



VMBus передает пакет особого формата

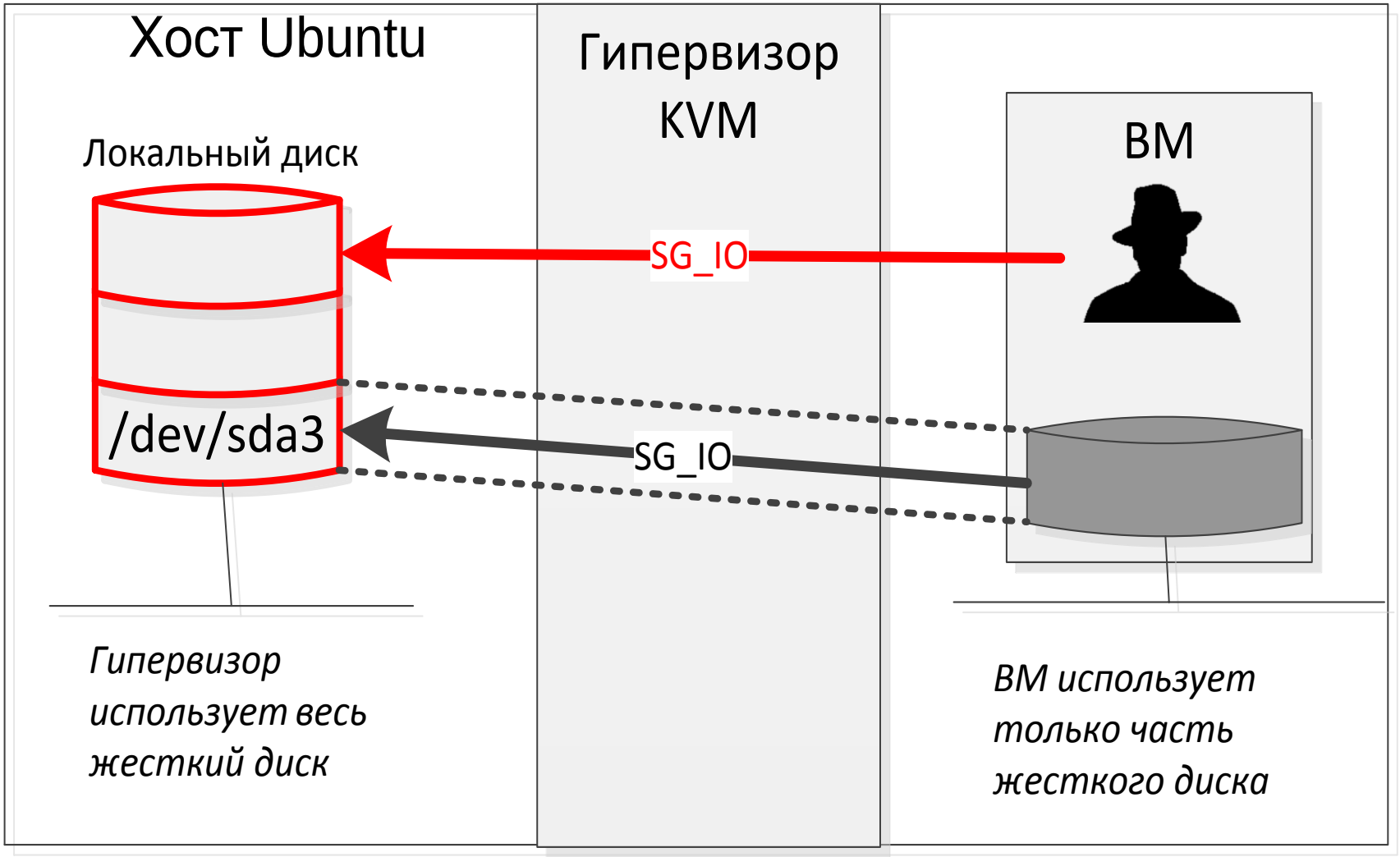
Hyper-V: CVE-2011-1872

Воздействие на гипервизор: удаленный DOS гипервизора ESX



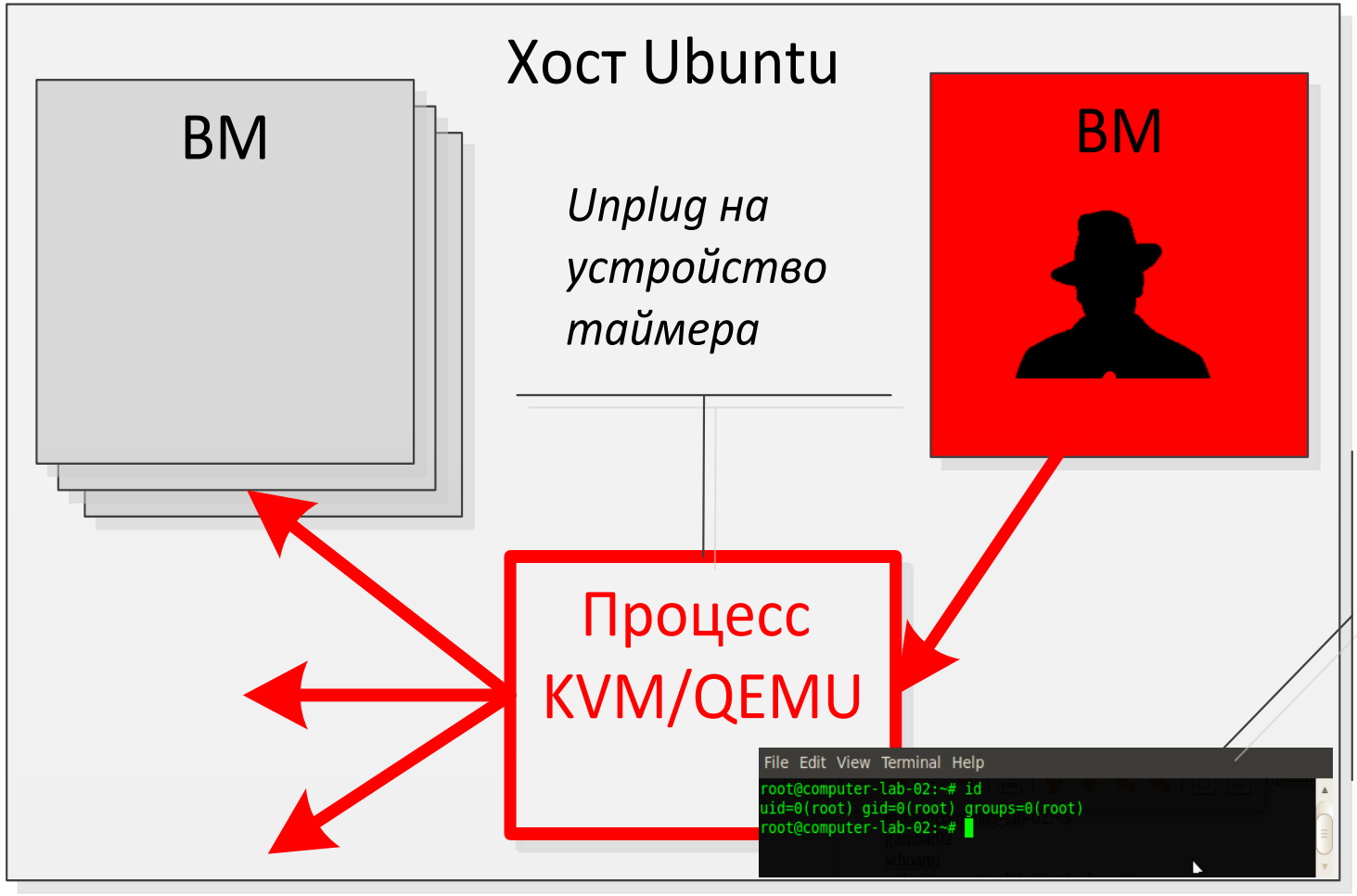
VMWare: CVE-2010-3609

Выход за пределы ВМ: запись и чтение данных с блочных устройств



KVM: CVE-2011-4127

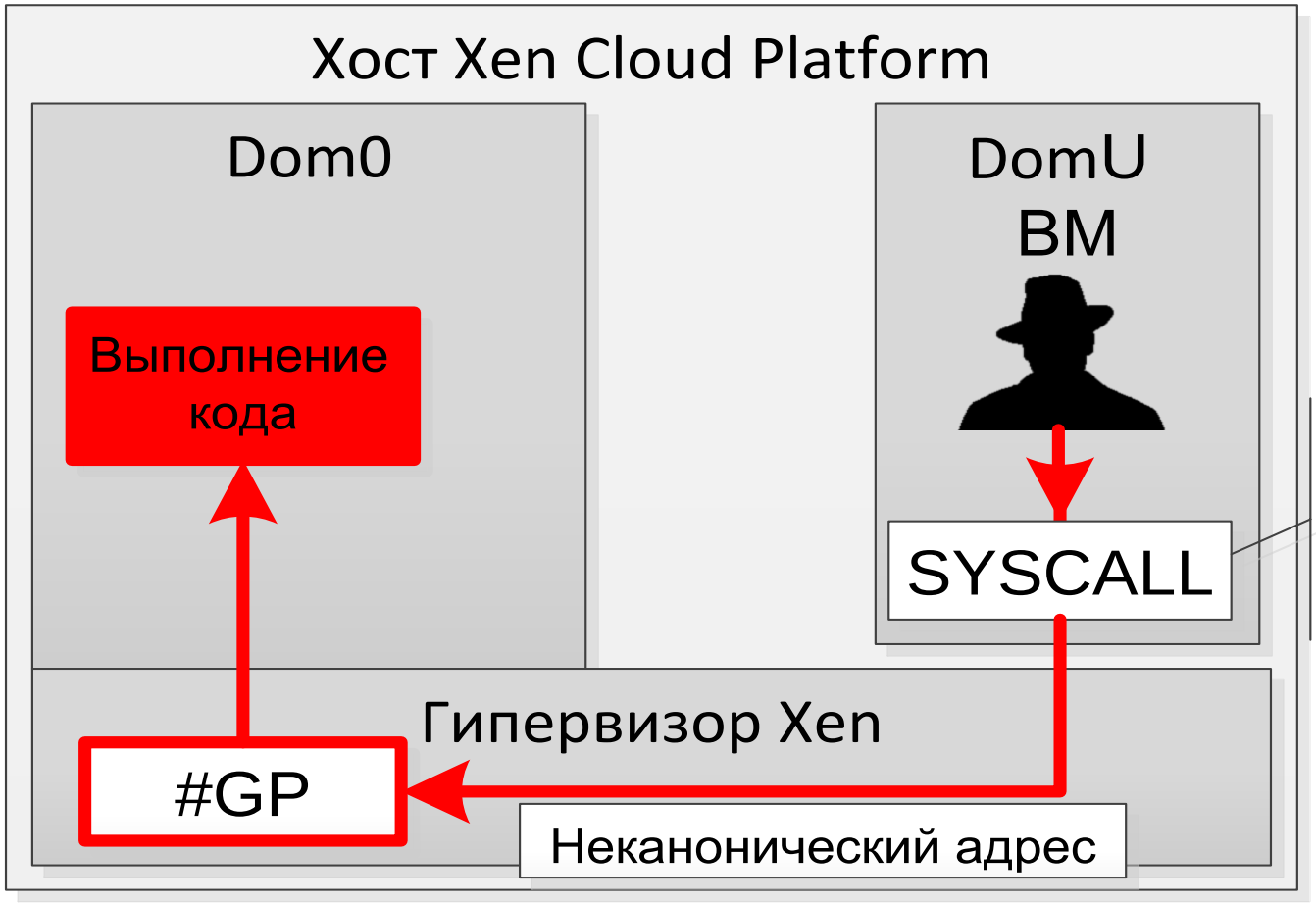
Выход за пределы ВМ: внедрение кода в гипервизор KVM



Нарушитель получает контроль над всем хостом

KVM: CVE-2011-1751

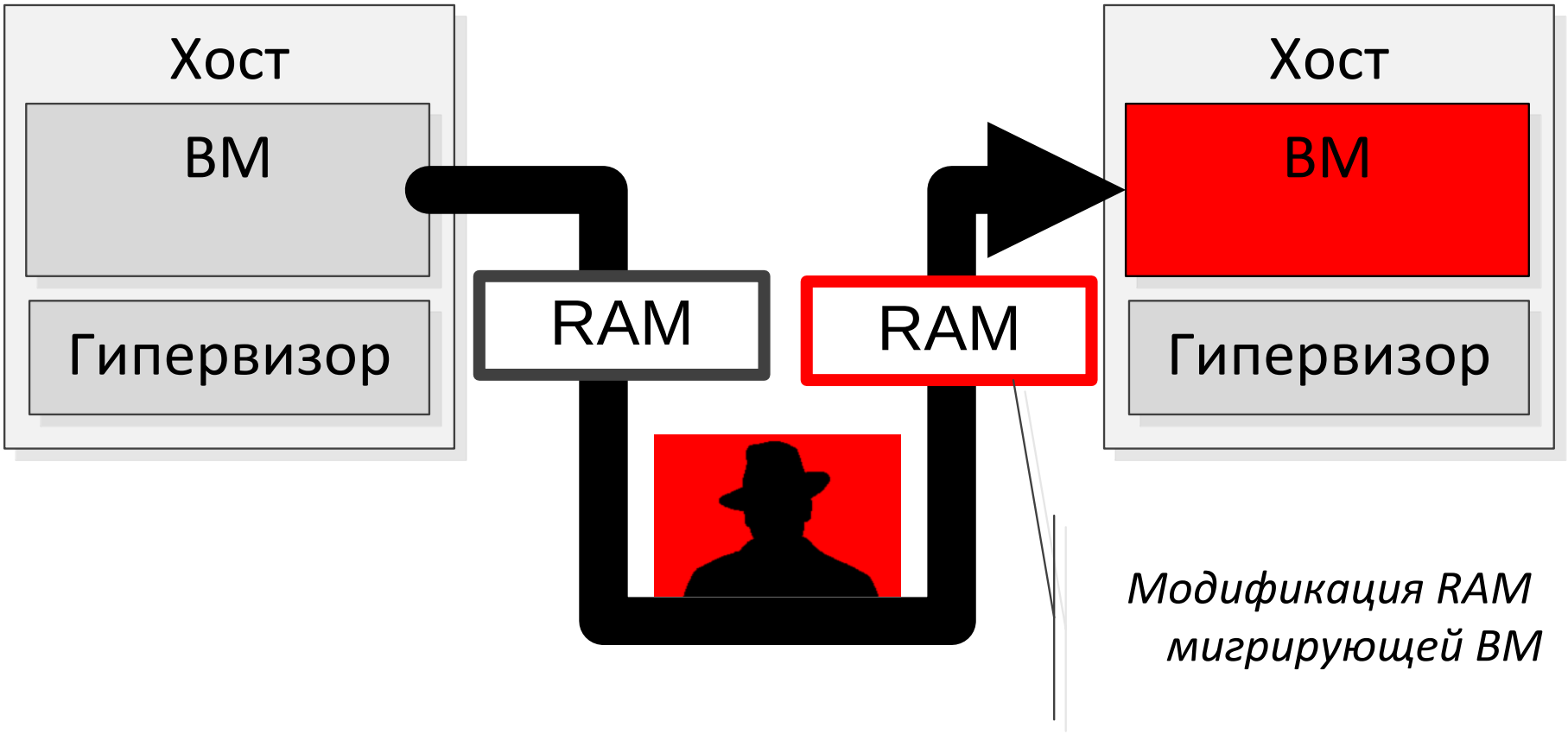
Выход за пределы BM: внедрение кода в гипервизор Xen



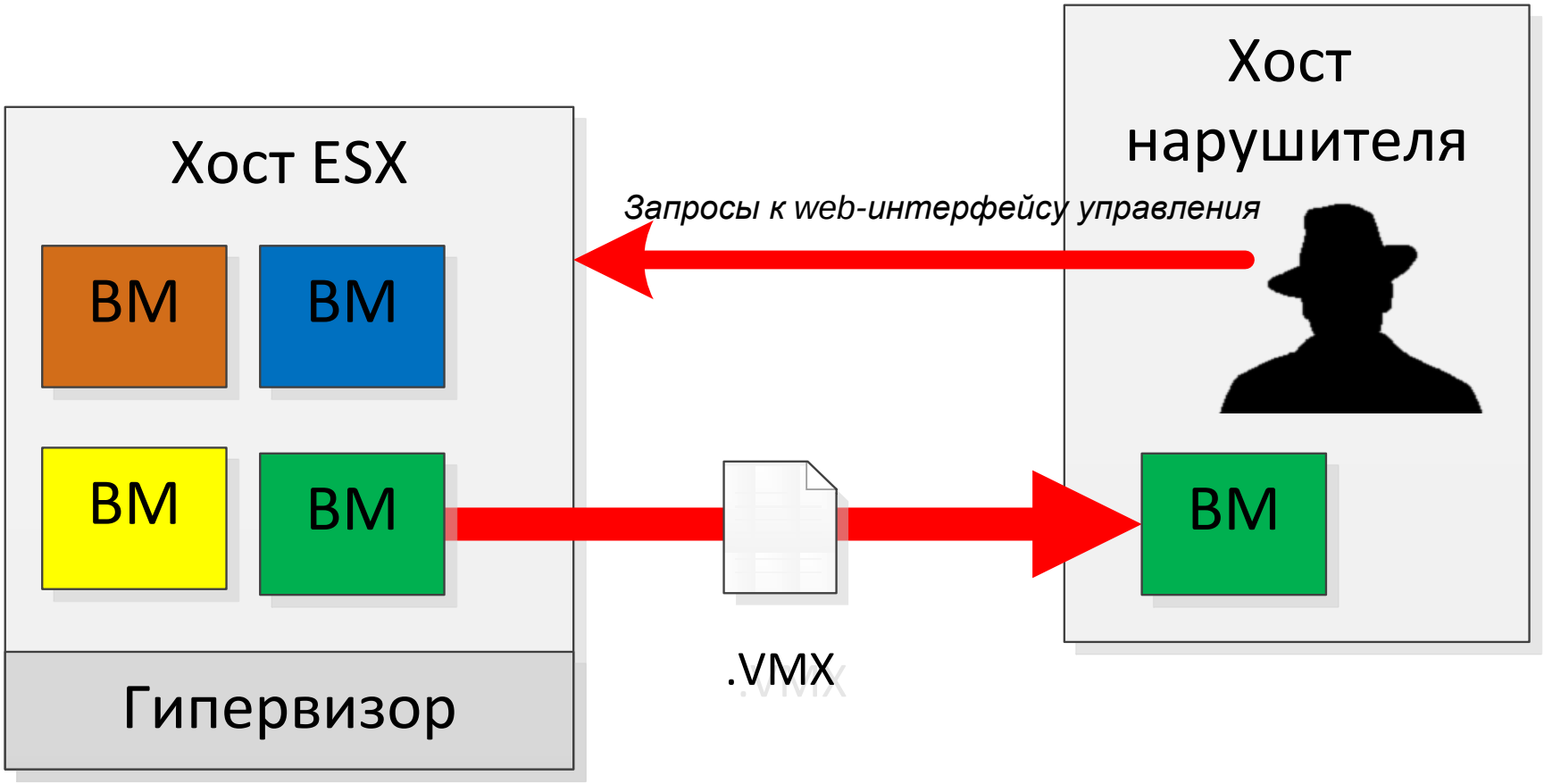
Нет проверки на канонический адрес при возврате SYSRET

XEN: CVE-2012-0217

Воздействие на гостевую ОС: модификация памяти ОС при миграции ВМ

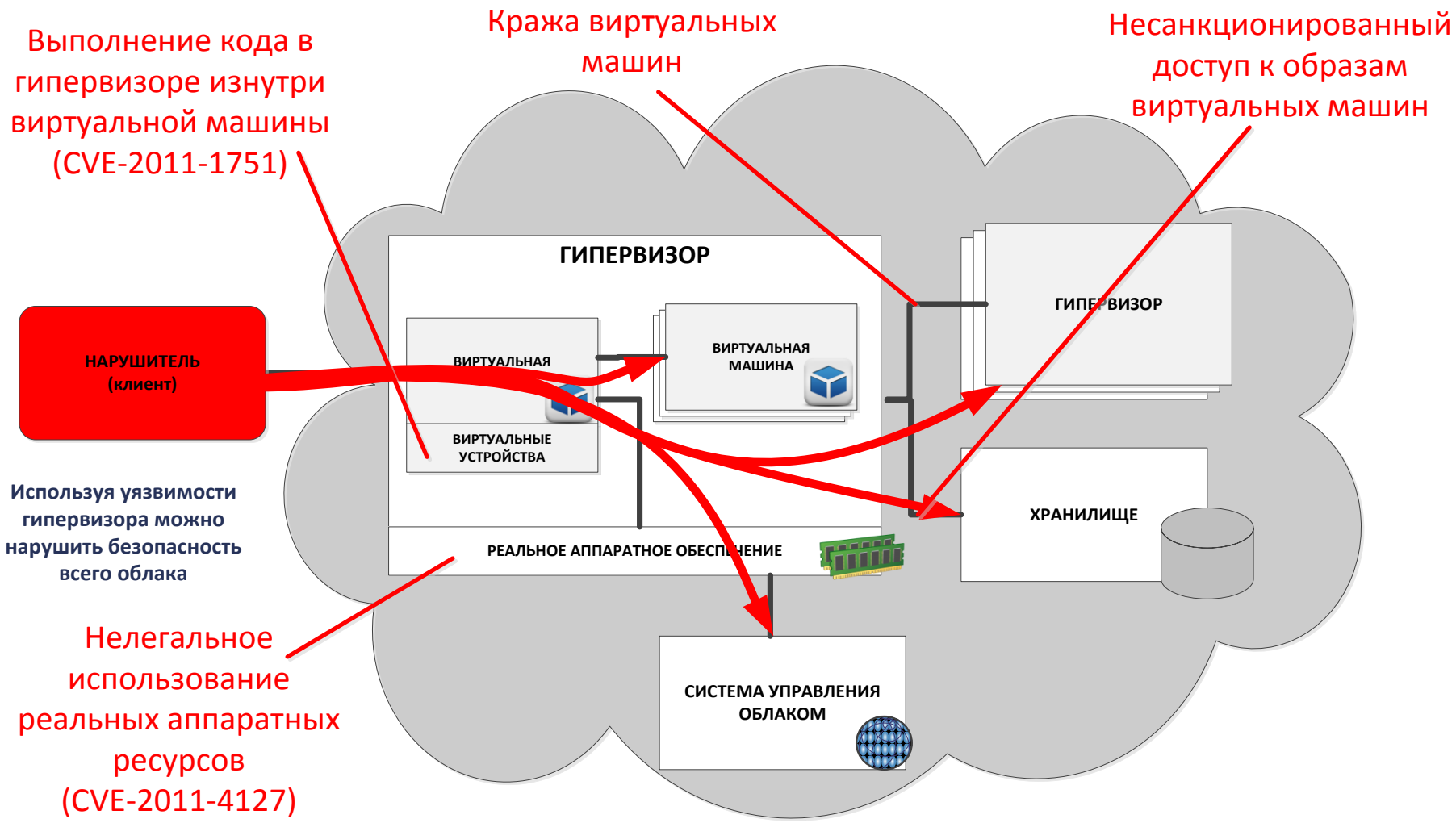


Прочие узявимости: кража ВМ пользователя



VMware: CVE-2009-3733

Существующие гипервизоры небезопасно использовать в облаке



Безопасный гипервизор

- Осуществляет идентификацию пользователей виртуальных машин в облаке
- Обеспечивает контроль доступа пользователей виртуальных машин к ресурсам облака
- Ограничивает права всех эмуляторов устройств до минимально необходимых
- Позволяет обнаруживать атаки на гипервизор и облако со стороны пользователей виртуальных машин
- Позволяет контролировать сетевые взаимодействия

Итог

- ✓ Необходимо создание безопасного гипервизора и специализированных средств защиты гипервизора в облаке

Предлагаемое решение	Результат
Контроль доступа и понижение прав эмуляторов устройств	Защита от атак выхода за пределы ВМ. Нарушитель не получает преимуществ.
Разработка методов обнаружения аномального поведения пользователей виртуальных машин	Обнаружение вторжений в облако через гипервизор
Введение систем контроля целостности для компонентов гипервизора и виртуальных машин	Защита от атак на гостевые ОС
Использование цифровой подписи для всех сетевых взаимодействий в которых участвует гипервизор	Защита от внутреннего нарушителя в облаке