конференция
РусКрипто'2013

ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет»

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВИРТУАЛИЗИРОВАННЫХ СИСТЕМ

Доктор технических наук, профессор
П. Д. Зегжда

27-30 марта 2013 года

КИБЕРБЕЗОПАСНОСТЬ И НОВЫЕ ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

- Смена объекта защиты: информация (данные) → инфраструктура → управляющие системы → исполнительные механизмы
- Изменение содержания понятий «конфиденциальность», «целостность», «доступность» для систем с открытым периметром и не корпоративных систем
- Разделение среды управления защиты от среды обработки информации
- Стабильное открытие систем как средство обновления
- Новые классификации нарушителей и моделей политик безопасности, переход от доказательной безопасности к допустимому состоянию

ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ – мощнейшее средство защиты, которое позволяет перейти от понятия «защищенная система» к понятию «система с контролируемым поведением»

БЕЗОПАСНОСТЬ КАК СЕРВИС

Унификация ресурсов	•Универсальный интерфейс доступа к информационным ресурсам независимо от их типа •Возможность защищать внешние ресурсы, доступ к которым осуществляется через универсальный интерфейс
Инвариантность средств защиты по отношению к типам ресурсов	• Универсальные средства защиты для всех типов ресурсов
Защита не только информации(данных) но и вычислительных ресурсов	• Вычислительная мощность и дисковое пространство • Пропускная способность • Логические ресурсы (сокеты, потоки, дескрипторы)
Устранение источников уязвимостей	• Минимизация кода средств защиты • Разделение функций защиты и обработки данных • Минимизация привилегированных приложений

НЕМНОГО ИСТОРИИ: ИДЕЯ ВИРТУАЛИЗАЦИИ И МОНИТОР ВИРТУАЛЬНЫХ МАШИН ВОЗНИКЛИ В 60-ЫЕ ГОДЫ КАК СРЕДСТВО АБСТРАКТНОГО РАЗДЕЛЕНИЯ РЕСУРСОВ НА НЕСКОЛЬКО МАШИН

В последнее десятилетие дешевизна компьютеров и многозадачной ОС уменьшает значение виртуализации.

Причины возрождения интереса к виртуализации:

- недогруженность и дороговизна обслуживания мощных компьютеров;
- уязвимость и неустойчивость современных ОС.

«В перспективе виртуализация не только средство организации многозадачности, но и механизм обеспечения безопасности и надежности».

Тэл Гарфинкель

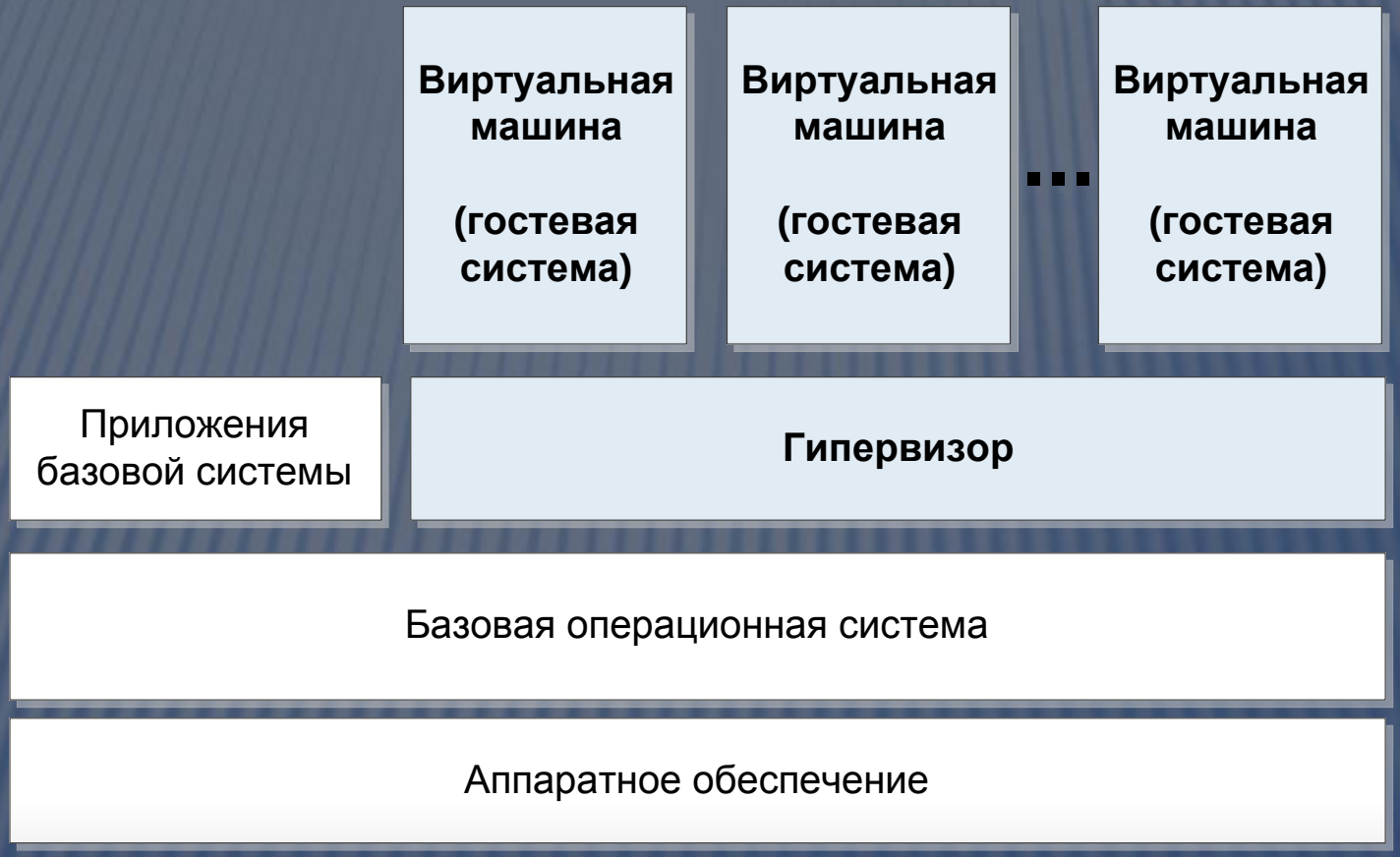
ПРОБЛЕМЫ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ КОНСОЛИДИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

- Высокая степень концентрации функций и наличие закрытых протоколов взаимодействий
- Большой объем взаимодействий, который невозможно контролировать без ущерба для производительности
- Огромный объем кода приводит к появлению уязвимостей
- Трудности адаптации доверенных средств защиты к современным средствам обработки информации

ИНТЕГРАЦИОННАЯ ПАРАДИГМА ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ СИСТЕМ

- Средства защиты должны контролировать все без исключения информационные взаимодействия
- Средства защиты должны быть инварианты по отношению к прикладным программам и опираться на абстрактное представление информационных взаимодействий
- Средства защиты должны контролировать информационные взаимодействия на основе четко определенных правил, составляющих формальную модель
- Должен быть предусмотрен механизм, позволяющий оценить безопасность как настоящего состояния системы так и спрогнозировать безопасность будущих состояний

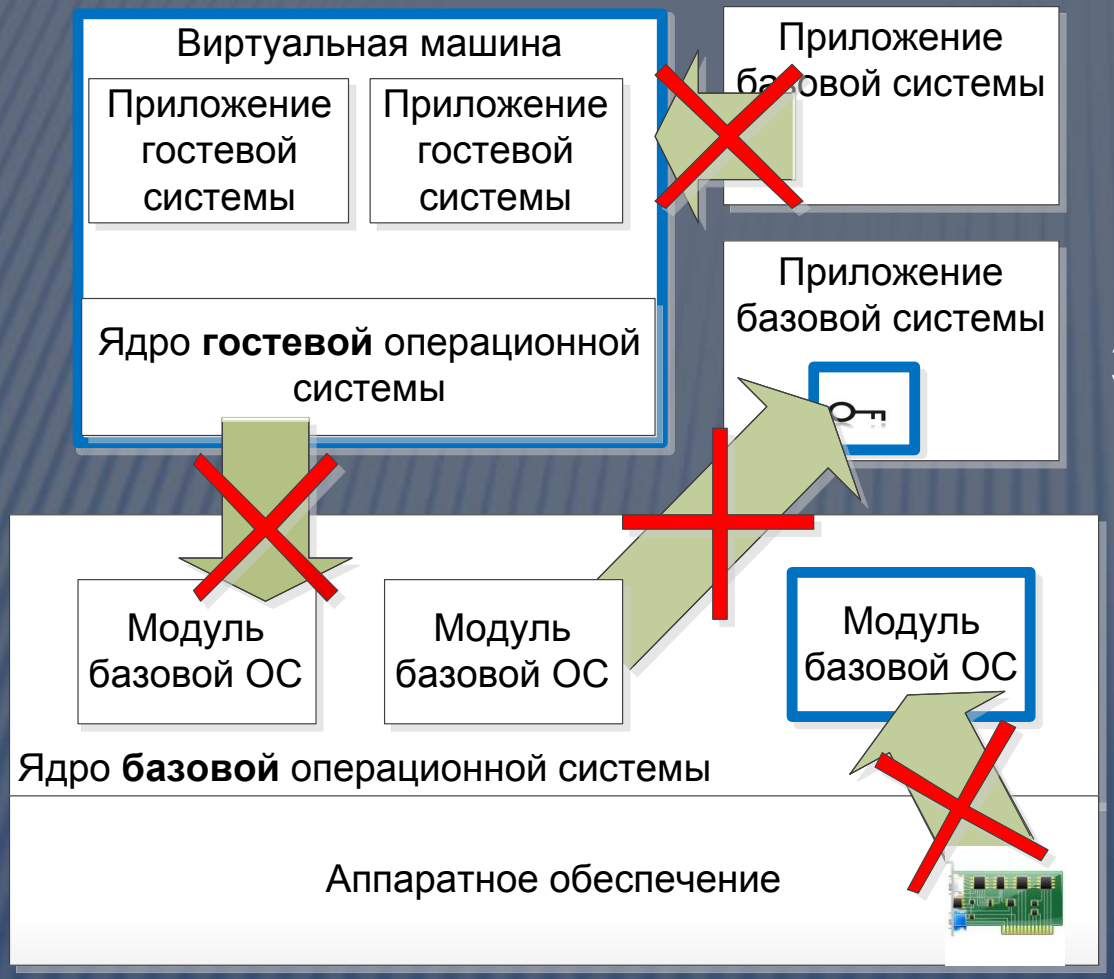
БАЗОВАЯ СХЕМА ВИРТУАЛИЗИРОВАННЫХ СИСТЕМ



ПРЕИМУЩЕСТВА ВИРТУАЛИЗАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

- **Изоляция**
  - Доступность и разделение обязанностей (сбой одной ВМ не влияет на другие)
  - Устранение скрытых каналов утечки информации
- **Централизация управления безопасностью**
  - Управление и механизмы безопасности вынесены вне ВМ
- **Гипервизор проще, чем операционная система**
  - Разрывает канал связи между недоверенным ПО и недоверенным аппаратным обеспечением, может быть формально верифицирован
  - Контроль и мониторинг поведения пользователей и программ, объектов и модулей ядра операционной системы
- **Репликация**
  - Быстрое восстановление после сбоев
  - Возможность сохранить слепок атакованной системы для дальнейшего изучения

ИЗОЛЯЦИЯ С ПОМОЩЬЮ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ



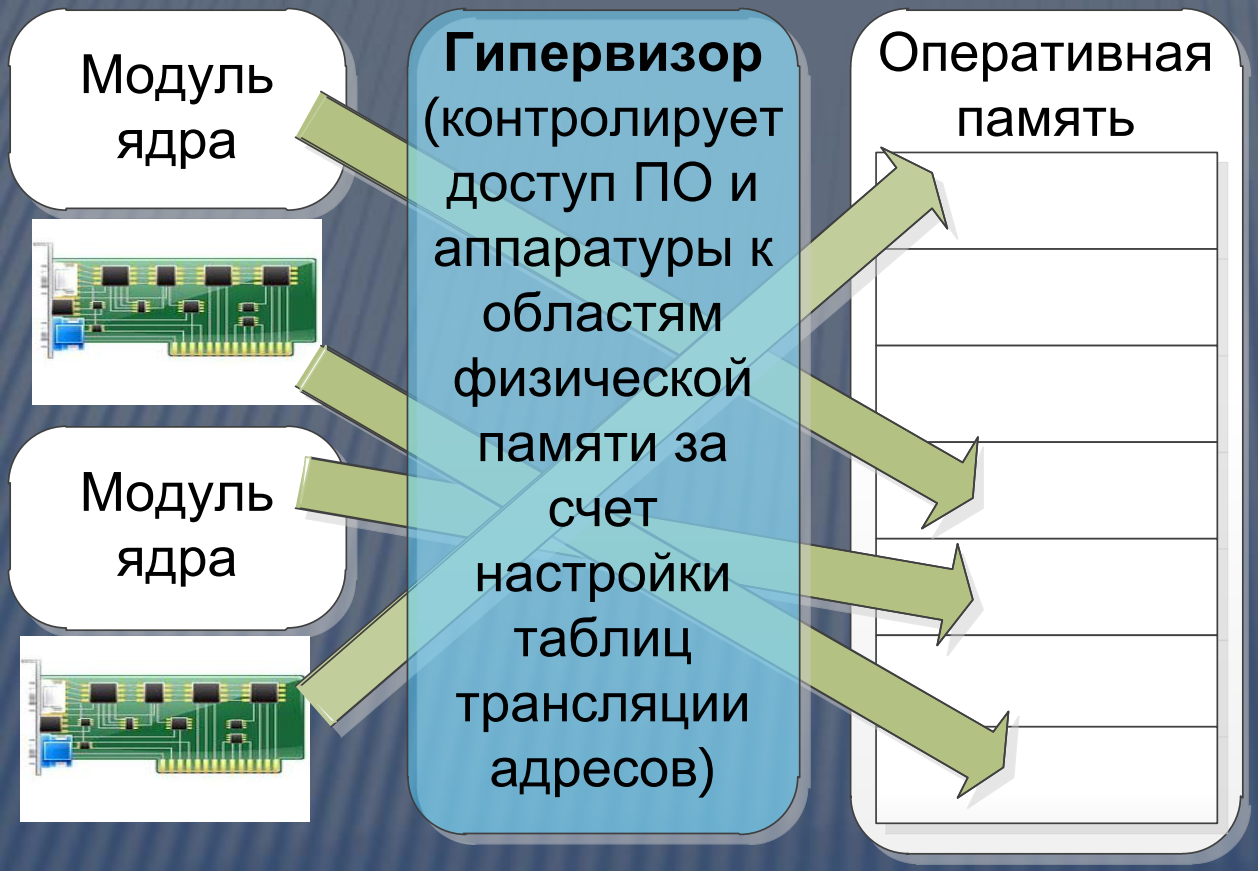
Изоляция

+ ОС
+ программ
+ данных

Защита от недоверенных:

+ ОС
+ программ
+ оборудования

КОНТРОЛЬ И МОНИТОРИНГ ДОСТУПА С ПОМОЩЬЮ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ



Контроль доступа:

- аппаратуры к данным
- модулей ядра операционных систем к данным

Мониторинг:

- действий аппаратуры
- поведения модулей ядра операционных систем и программ

Беспечность есть причина всяких бедствий

Джами Абдуррахман Анураддин ибн Ахмад

ПРОБЛЕМЫ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

Проблема безопасности	**Комментарии**
Отказ в обслуживании гипервизора	Отказ в обслуживании комплекса ВМ
Безопасность взаимодействия ВМ с гипервизором	Подмена механизмов взаимодействия ВМ с гипервизором. Изменение потоков данных в системе
Мобильность ВМ	Понятие физической безопасности компьютеров становится эквивалентным понятию безопасности сменных носителей, а также прав доступа к файлам. При исследовании безопасности нельзя полагаться на инвариантность среды, в которой запускается ВМ.
Проблема разделяемых ресурсов	Разделяемые ресурсы могут быть использованы для НСД к информации. Разделяемые ресурсы могут быть использованы для выхода РПС за пределы виртуальной машины с целью распространения

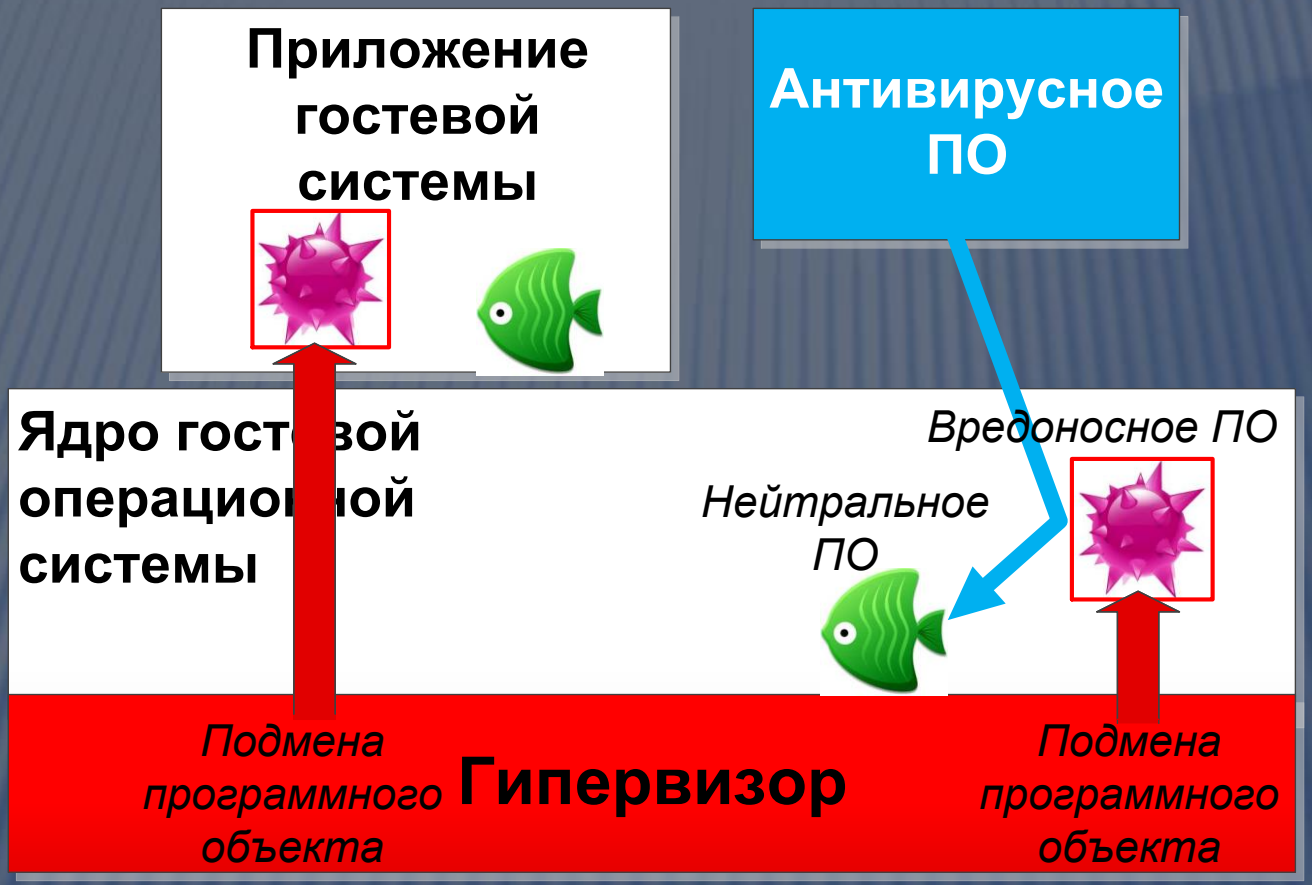
УЯЗВИМОСТИ ВМ ЗА 2012Г. (ПО ДАННЫМ NIST)

ВМ	CVE	Кол-во
VirtualBox	CVE-2013-0420 CVE-2012-0111 CVE-2012-0105	3
VmWare	CVE-2012-6325 CVE-2012-6324 CVE-2012-5055 CVE-2012-5004	4
Xen	CVE-2013-0154 CVE-2012-6314 CVE-2012-5161 CVE-2012-6333 CVE-2012-5515 CVE-2012-5514 CVE-2012-5513 CVE-2012-5512 CVE-2012-5511 CVE-2012-5510	10
Red Hat Enterprise Virtualization Manager	CVE-2012-5516 CVE-2012-2696 CVE-2012-0861 CVE-2011-4316 CVE-2011-2625 CVE-2011-2624	6

ТИПЫ УЯЗВИМОСТЕЙ ВИРТУАЛЬНЫХ МАШИН

- Уязвимости отказа в обслуживании гипервизора.
- Уязвимости, предоставляющие доступ к ресурсам ВМ
- Уязвимости, использующие разделяемые ресурсы для атаки ВМ
- Уязвимости системы управления виртуальными машинами

ПРИМЕР РЕАЛИЗАЦИИ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВИРТУАЛИЗИРОВАННОЙ СИСТЕМЕ



Возможность сокрытия вредоносного ПО в любом модуле операционной системы и приложении за счет подмены адресных пространств

ОБЛАЧНЫЕ ТЕХНОЛОГИИ: НОРМАТИВНЫЕ ДОКУМЕНТЫ NIST (ПРОЕКТ ДО 2020 Г.)

Нормативный документ	**Содержание**
NIST Cloud Computing Reference Architecture (Special Publication 500-292), 2011	Определения и архитектура
US Government Cloud Computing Technology Roadmap Volume I, Volume II, Volume III (Special Publication 500-293) Release 1.0 (Draft), 2011	Требования, стандарты и технологии переносимости, взаимодействия и безопасности.
Challenging Security Requirements for US Government Cloud Computing Adoption (NIST whitepaper), 2011	Требования безопасности и анализ рисков

ОБЛАЧНЫЕ ТЕХНОЛОГИИ. ДОКУМЕНТЫ NIST (ПРОЕКТ ДО 2020 ГОДА).

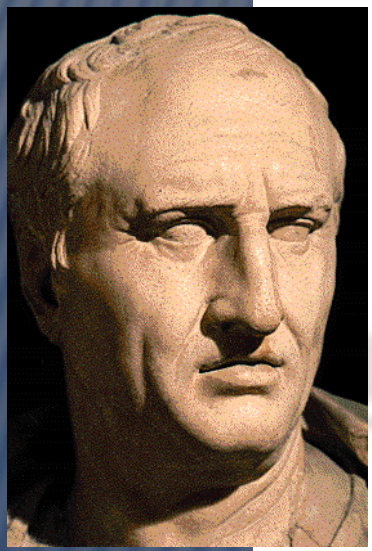
Нормативный документ	**Содержание**
NIST Cloud Computing Reference Architecture (Special Publication 500-292), 2011	Определения и архитектура
US Government Cloud Computing Technology Roadmap Volume I, Volume II, Volume III (Special Publication 500-293) Release 1.0 (Draft) , 2011	Требования, стандарты и технологии переносимости, взаимодействия и безопасности.
Challenging Security Requirements for US Government Cloud Computing Adoption (NIST whitepaper) , 2011	Требования безопасности и анализ рисков

ПОДХОД NIST К БЕЗОПАСНОСТИ ОБЛАКОВ

- Выбор модели облачной системы (SaaS, IaaS, PaaS)
- Учет специфики безопасности выбранной модели
- Разделение обязанностей в смысле безопасности между поставщиком и потребителем системы облачных вычислений
- Обеспечение безопасности облачной системы

ПРЕИМУЩЕСТВА ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ С ТОЧКИ ЗРЕНИЯ NIST

- Уменьшение издержек для правительственных организаций
- Долговременная инвестиция в перспективную технологию

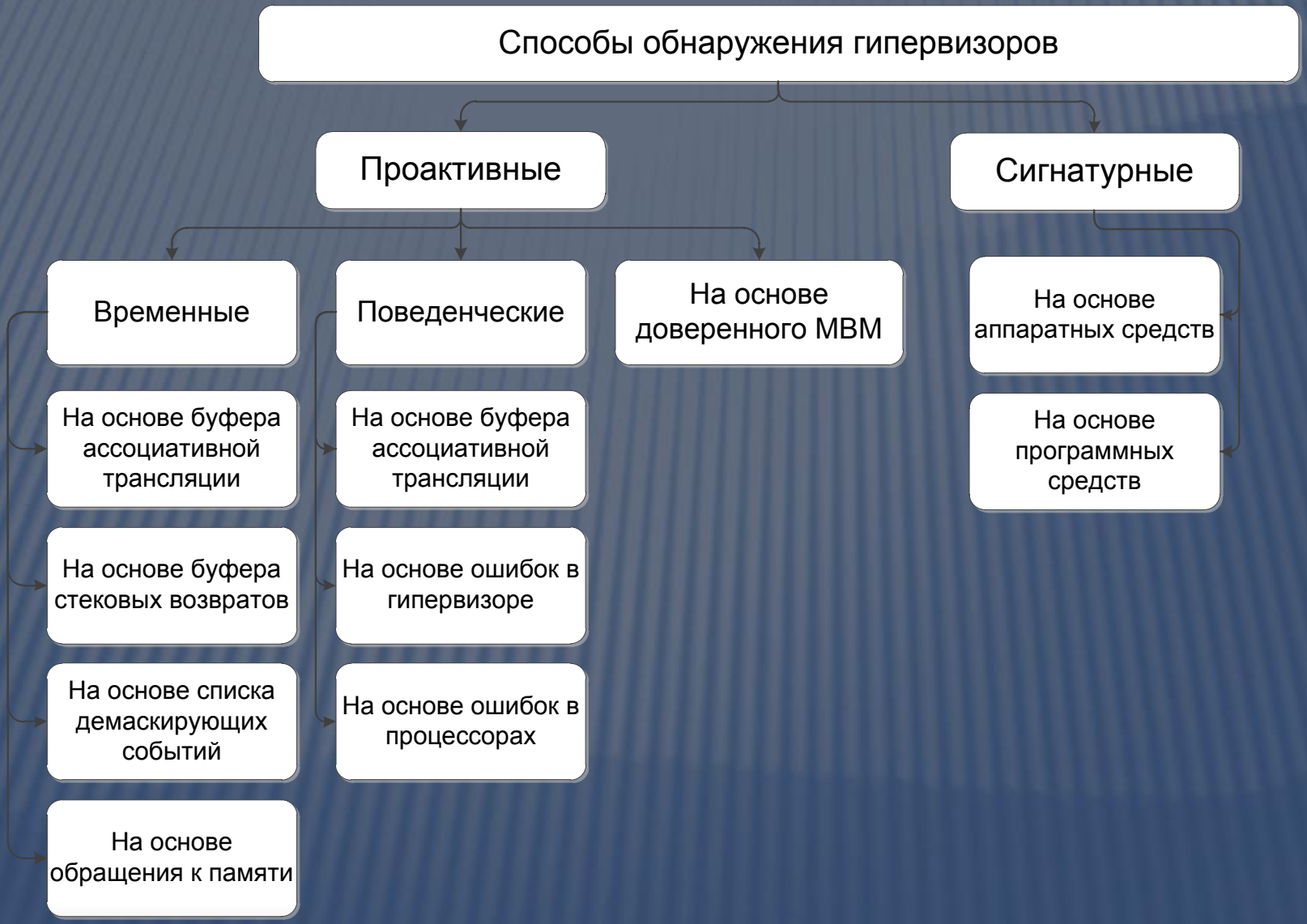


Я буду говорить, ничего не утверждая

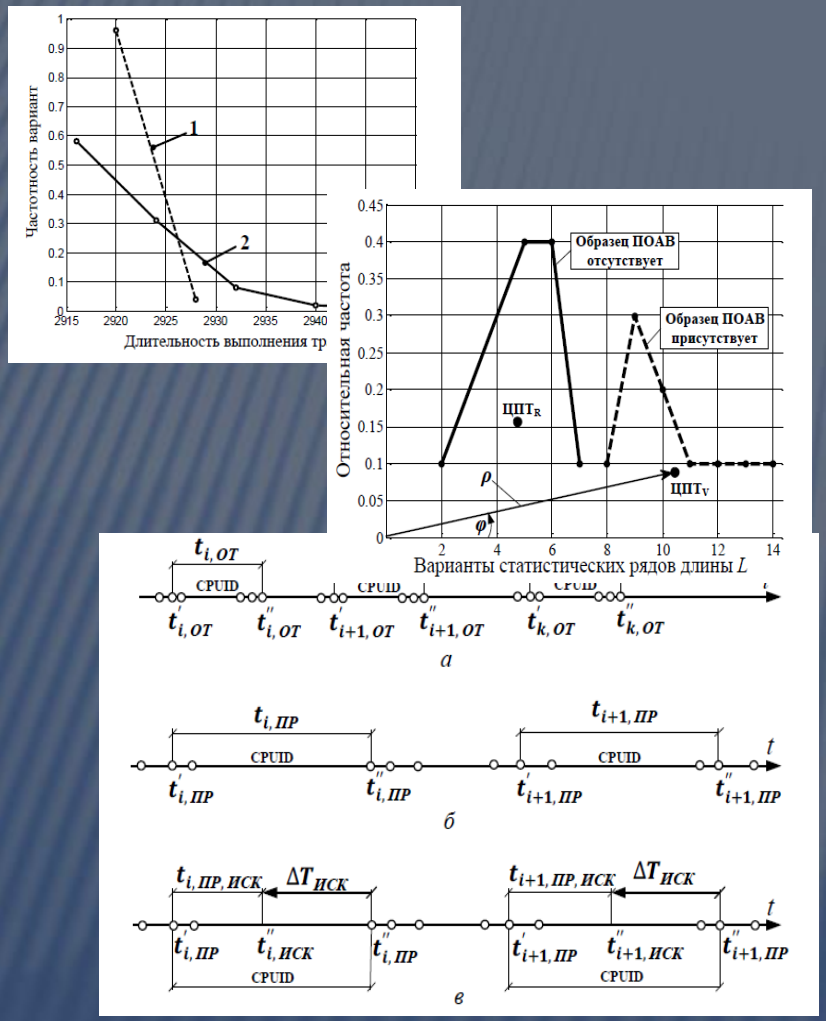
Марк Туллий Цицерон

Возможность изоляции и скрытого управления делает виртуализацию привлекательной для технологии нападения

КЛАССИФИКАЦИЯ СПОСОБОВ ОБНАРУЖЕНИЯ ЭКСПЛУАТАЦИИ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ



ПРИМЕРЫ ПРИЗНАКОВ ЭКСПЛУАТАЦИИ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ



- Аномальное поведение таймеров и системного времени: CMOS RTC, HPET, PIT, TSC, APIC
- Изменение реального размера кэша: страничного,TLB, Stack Return
- Наличие аномалий в карте физической памяти E820
- Относительное снижение скорости работы некоторых инструкций (CPUID, mov CR3)

МЕРЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ВИРТУАЛИЗАЦИИ

- Формальная верификация гипервизора
- Вынесение механизмов безопасности за пределы ВМ
- Ограничение мобильности ВМ
- Устранение разделяемых между ВМ ресурсов

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВИРТУАЛИЗИРОВАННЫХ СИСТЕМ

- Контроль физического и виртуального оборудования
- Контроль целостности ПО виртуализации и образов виртуальных машин
- Минимизация привилегий доступа к гипервизорам по управлению
- Мониторинг скрытой эксплуатации технологии виртуализации

Все просто, если смотреть в правильном направлении

Агата Кристи

МОДЕЛЬ БЕЗОПАСНОСТИ СИСТЕМ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Состояние системы облачных вычислений:

$$\psi = (C, P, U, S, H, I, R, Rp, Soft, Id, Im, Role)$$

- C + граф всех сетевых связей между всеми узлами внутренней сети облака и виртуальными машинами (ВМ)
- V + множество ВМ
- N + множество хостов внутренней сети
- M + множество машин $M = V \cup N$
- O + множество файлов образов ВМ
- R + множество ролей хостов в облаке $\{VmHost, Storage, Controller\} \subseteq R$
- P + множество всех программ и ВМ в облаке
- U + множество всех пользователей облака
- S + множество всех субъектов в облаке
- $Role$ + распределение ролей хостов в облаке $Role : N \to P(R)$
- H + распределения ВМ по хостам $H \subseteq V \times N$
- I + распределение образов ВМ по хостам $I \subseteq V \times P(N)$
- F + распределение ВМ по файлам образов $F \subseteq V \times \mathrm{P}(O)$
- Rp + отношение репликации работы ВМ $Rp \subseteq V \times P(N)$
- $Soft$ + распределение программ по машинам $Soft \subseteq M \times P(P)$
- Id + отношение идентификации $Id \subseteq P \times P(S)$
- Im + отношение имперсонализации $Im \subseteq P \times S$

СВОЙСТВА ГИПЕРВИЗОРОВ И ВИРТУАЛЬНЫХ МАШИН В СИСТЕМАХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ (1)

- Использование виртуальных машин в качестве узлов сети в облаке

$$V \subseteq M$$

- Миграция виртуальных машин

$$H^{\tilde{\psi}} = H^{\psi} \setminus (v_i, n_j) \cup (v_i, n_k), v_i \in V^{\psi}, n_j \in N^{\psi}, n_k \in N^{\psi}$$

- Репликация работы виртуальных машин

$$Rp \subseteq V \times P(N)$$

УСЛОВИЯ БЕЗОПАСНОСТИ ГИПЕРВИЗОРОВ ВИРТУАЛИЗИРОВАННЫХ СИСТЕМ (1)

- Виртуальная машина – программа, работающая под управлением гипервизора. В каждой виртуальной машине также выполняются программы:

$$\begin{cases} V \subseteq P \\ \forall v_j \in V : \exists P_{v_j} \subset P, (v_j, P_{v_j}) \in Soft \end{cases}$$

- Для любой программы в виртуальной машине существует по крайней мере два субъекта в облаке:

$$\forall v_i \in V, n_j \in N, P_{v_i} \in P, p_{v_i} \in P_{v_i}, (v_i, n_j) \in H, (v_i, P_{v_i}) \in Soft :$$
$$\exists s_v, s_v, \{s_v, s_v\} \subset S_u, (v_i, s_n) \in Id \wedge (p_{v_i}, s_v) \in Id$$

s_v — субъект, который соответствует программе, запущенной в виртуальной машине

s_n — субъект, который соответствует программе, запущенной на хосте

СВОЙСТВА ГИПЕРВИЗОРОВ И ВИРТУАЛЬНЫХ МАШИН В СИСТЕМАХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ (2)

- Разделение среды хранения и выполнения виртуальных машин

$$\forall v_i \exists N_{v_i} \subseteq N :$$

$$(v_i, N_{v_i}) \in I \wedge \nexists n_j \in N_{v_i}, VmHost \in Role(n_j)$$

- Возможность объединять виртуальные машины в изолированные виртуальные сети

$$C_v \subset C$$

- несвязный граф виртуальных машин

УСЛОВИЯ БЕЗОПАСНОСТИ ГИПЕРВИЗОРОВ ВИРТУАЛИЗИРОВАННЫХ СИСТЕМ (2)

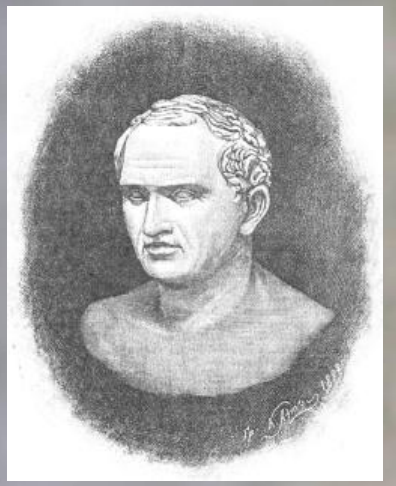
- Все виртуальные машины в облаке идентифицируются в гипервизорах только субъектами, которые принадлежат множеству пользователей, работающих в этих виртуальных машинах:

$$\forall v_i \in V, s_v \in S, n_j \in N,$$

$$P_v \subset P, (v_i, n_j) \in H, (v_i, P_v) \in Soft :$$

$$\nexists p_k \in P_v, s_k \in S, (p_k, s_k) \in Id$$

$$\wedge \{s_v, s_k\} \in S_u \wedge (u, S_u) \in Im$$

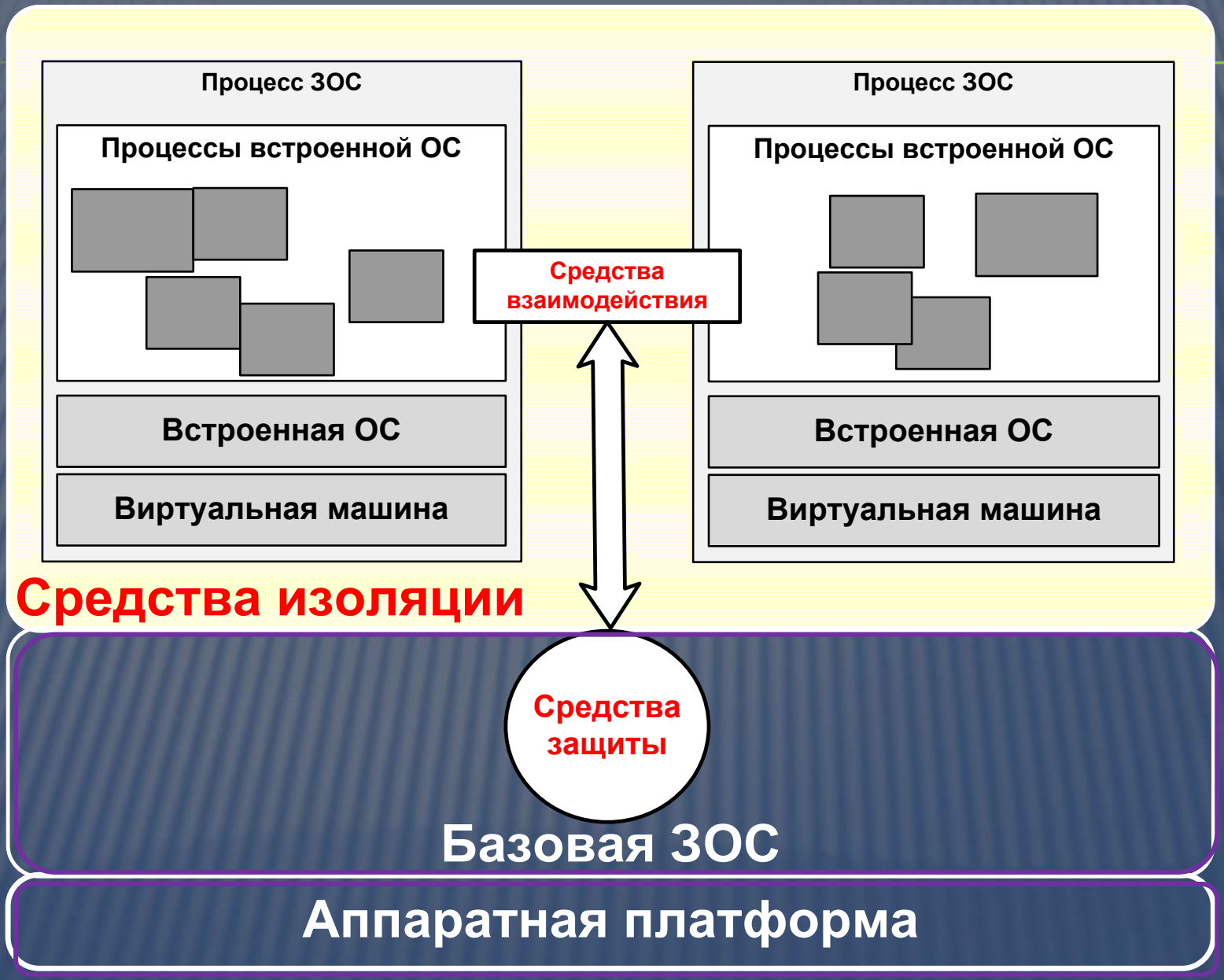


Если наши соображения правдоподобны, то не следует стремиться к большему

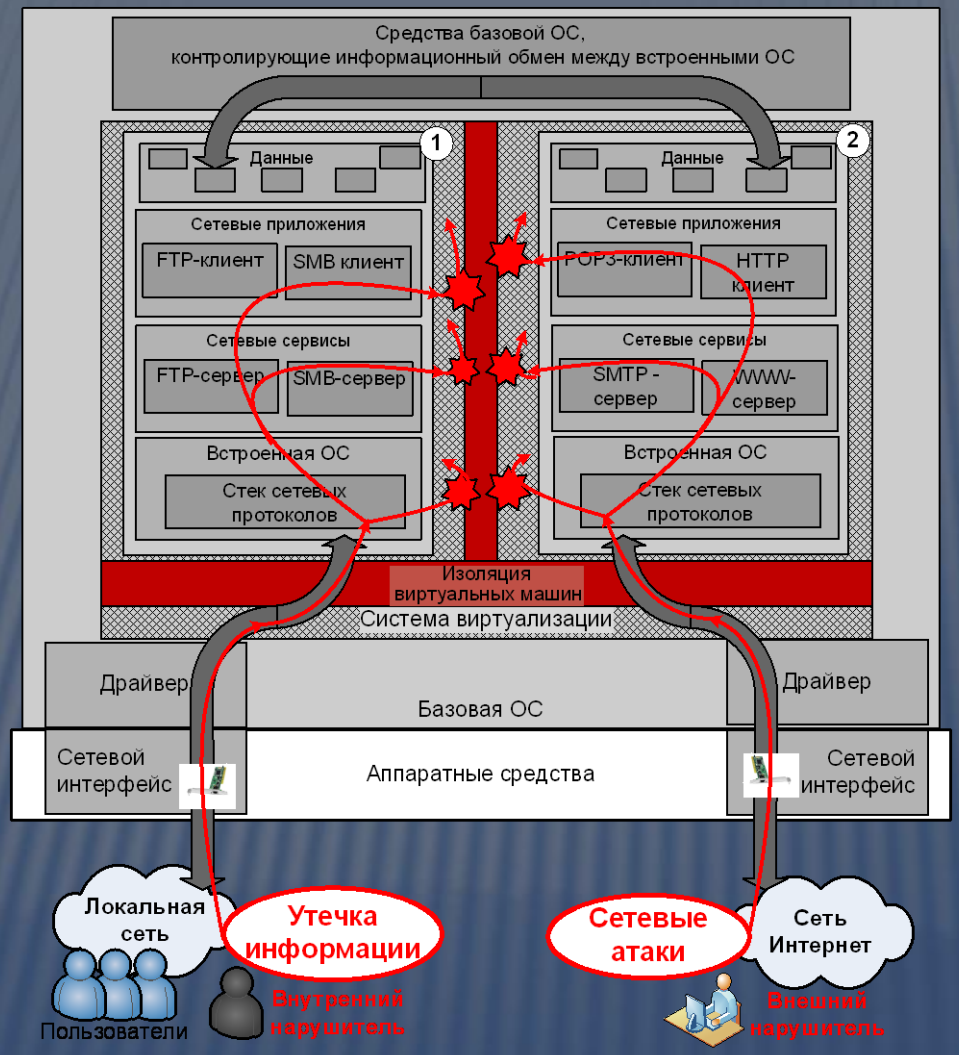
Марк Туллий Цицерон

Гибридная система – виртуализация на основе доверенной ОС – механизм сокращения угроз и создание безопасной виртуализации

ГИБРИДНАЯ СИСТЕМА



ГИБРИДНАЯ СИСТЕМА ДЛЯ РАБОТЫ В СРЕДЕ ИНТЕРНЕТ И КОРПОРАТИВНОЙ СЕТИ



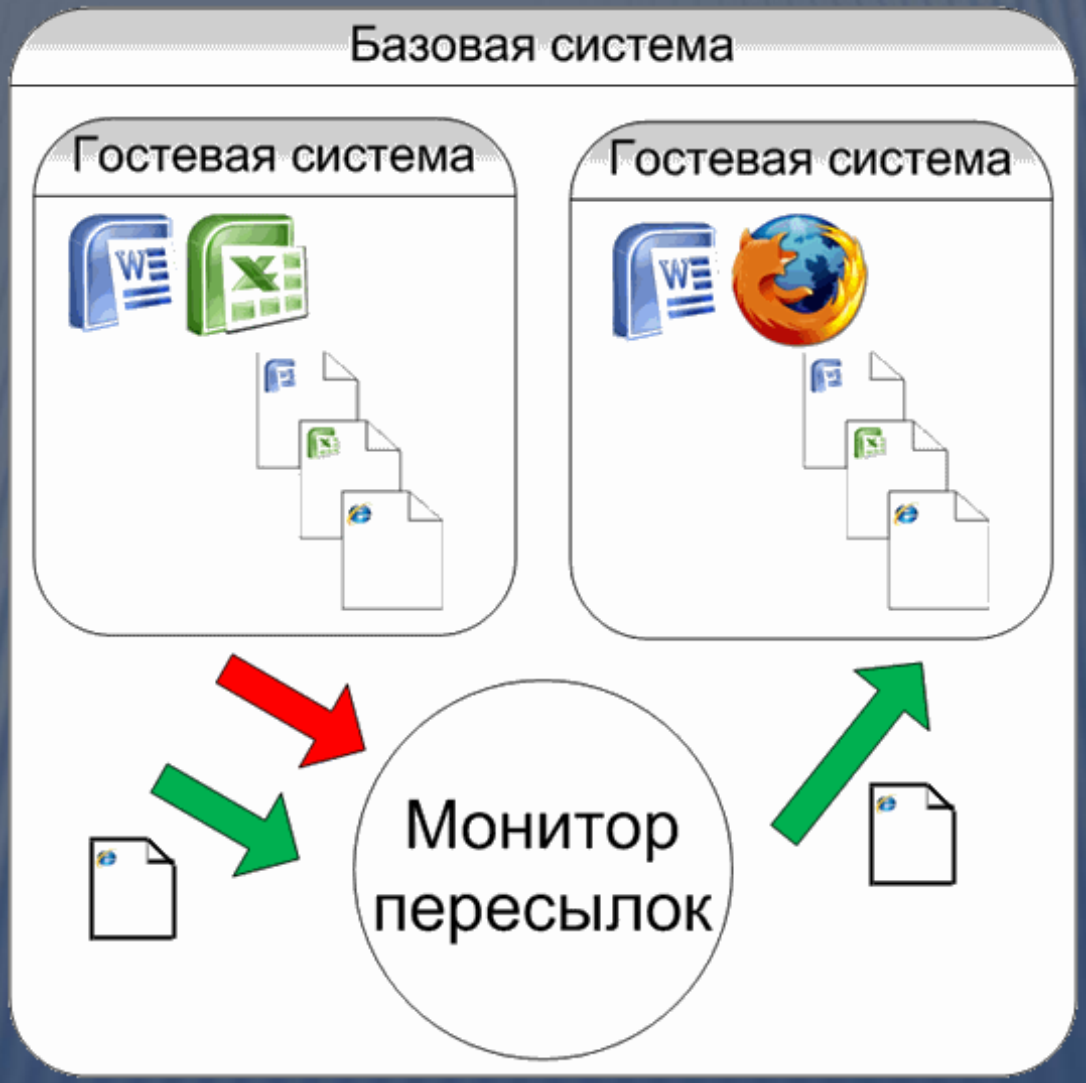
Безопасность гостевой системы определяется безопасностью базовой и виртуализацией ресурсов

Гостевая система наследует свойства безопасности базовой системы при соблюдении определенных условий

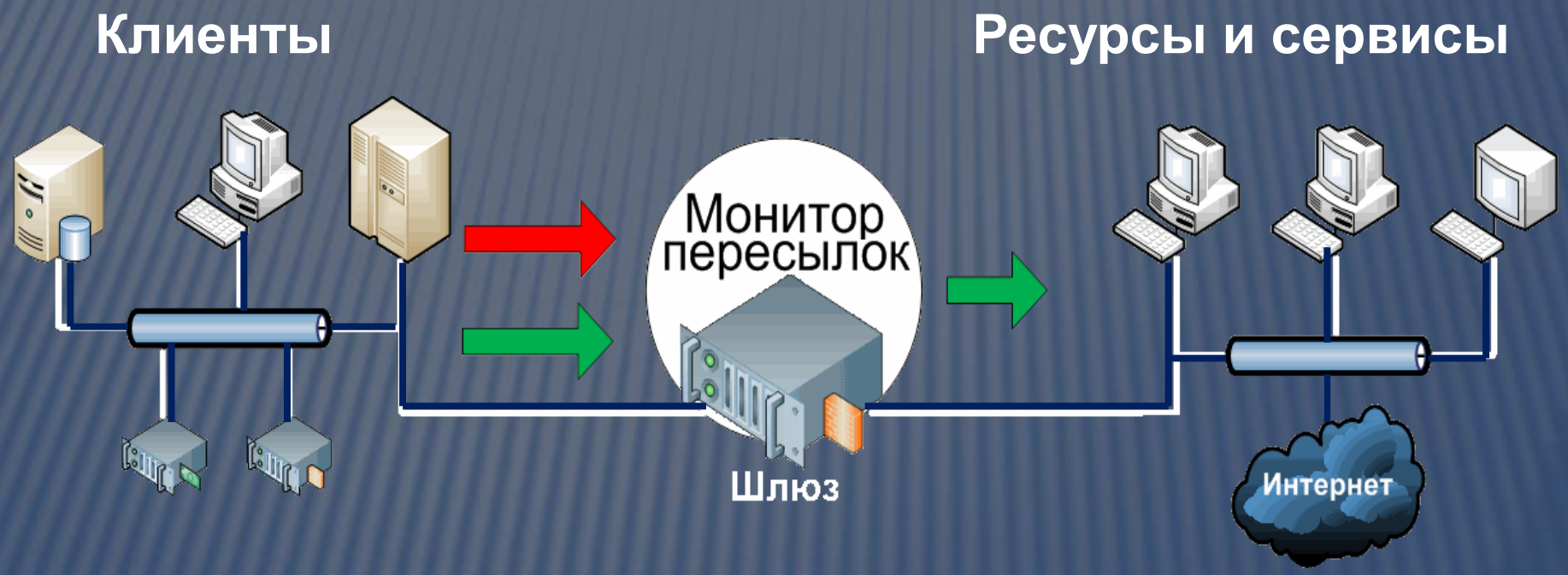
УСЛОВИЕ БЕЗОПАСНОЙ ВИРТУАЛИЗАЦИИ РЕСУРСОВ

Гостевая система наследует свойства безопасности базовой, при условии соблюдения гомоморфизма между отношениями типов ресурсов и инжективности их отображения в ходе виртуализации.

МОНИТОР ПЕРЕСЫЛОК В ГИБРИДНЫХ СИСТЕМАХ



МОНИТОР ПЕРЕСЫЛОК В РАСПРЕДЕЛЕННЫХ МНОГОЗВЕННЫХ СИСТЕМАХ (ШЛЮЗ КОНТРОЛЯ ДОСТУПА)



ВЫВОДЫ

1. Механизм виртуализации может эффективно использоваться для решения защиты, т. к. позволяет разделить среду обработки информации и среду функционирования средств защиты и обеспечивает дополнительный уровень изоляции.

2. Для успешного применения данного подхода необходимо:
   - обеспечить высокую степень виртуализации(прозрачность базовой системы для гостевых);
   - соблюдать сформулированные условия при виртуализации ресурсов.

Тысяча путей уводит от цели и лишь один ведет к ней.

Мишель Эйкем де Монтень

«ДОРОЖНАЯ КАРТА» ВНЕДРЕНИЯ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ ПРИ РЕШЕНИИ ЗАДАЧ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

- Принятие
  - *открытости* (связи с сетью Интернет)
  - *эластичности* (динамического перераспределения ресурсов)
  - *масштабируемости* (разрыва сред хранения, обработки и передачи данных)

  как неотъемлемых свойств современных инфосистем
- Формирование понятия изолированной критической среды как эквивалента доверенной среды
- Создание новых средств и систем кибербезопасности с учетом свойств современных инфосистем и критических сред

СЦЗИ, кафедра ИБКС
ФГБОУ ВПО «СПбГПУ»

Санкт-Петербург, ул.Политехническая, д.29, Главное здание, К. 173

тел: +7(812) 552-64-89,
552-76-32

Web: HTTP://IBKS.FTK.SPBSTU.RU
E-mail: ZEG@ IBKS.FTK.SPBSTU.RU