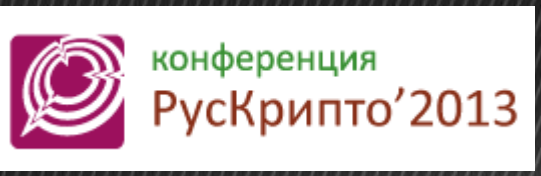


http://www.rusoypto.ru/conference/

СУПЕРКОМПЬЮТЕРЫ И БЕЗОПАСНОСТЬ. НОВЫЕ ЗАДАЧИ И НОВЫЕ ВОЗМОЖНОСТИ

Д.т.н., профессор Зегжда Дмитрий Петрович

Вычислительная мощь … страны

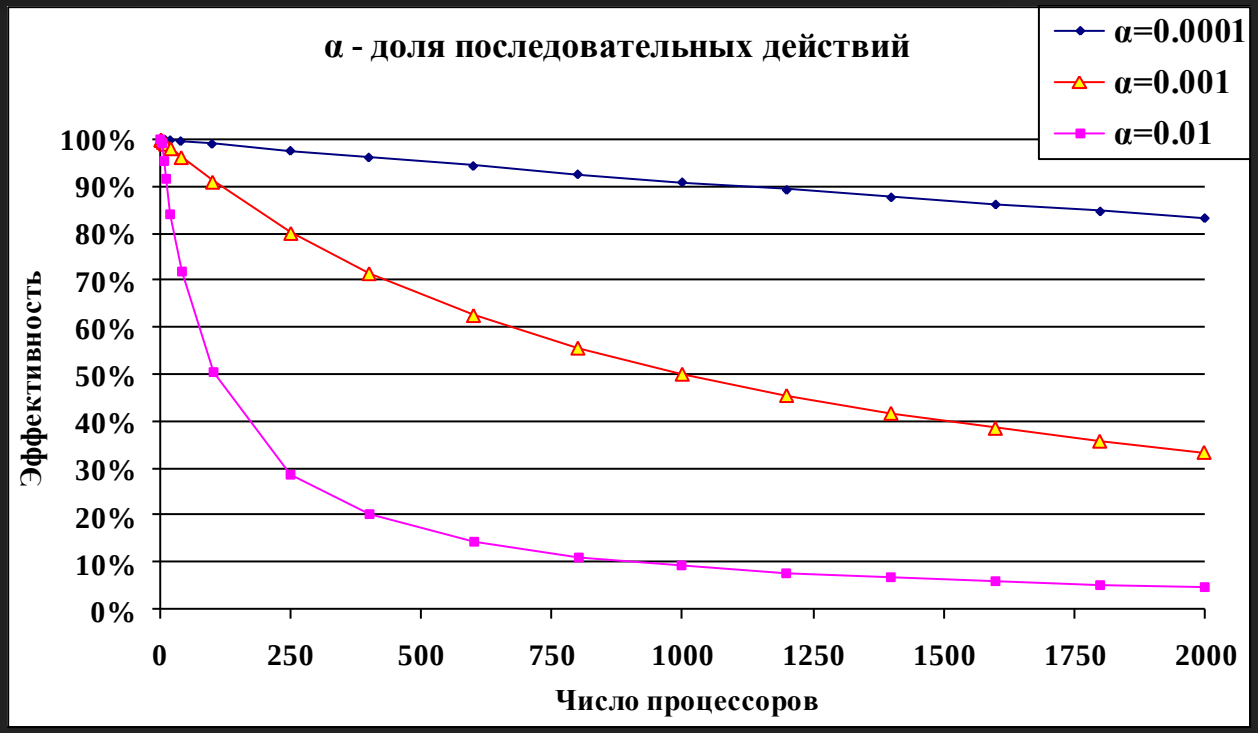
• Суперкомпьютерные технологии становятся одним из решающих факторов научно-технического прогресса и могут стать такой же стратегической отраслью как авиастроение, атомная энергетика, ракетостроение и космическая индустрия

• Конкурентоспособность страны в современных условиях во многом определяется уровнем развития суперкомпьютерных вычислительных технологий

Компьютер пользователя на порядки слабее суперкомпьютера

Производительность и частота процессоров

Ограниченность производительности последовательных алгоритмов



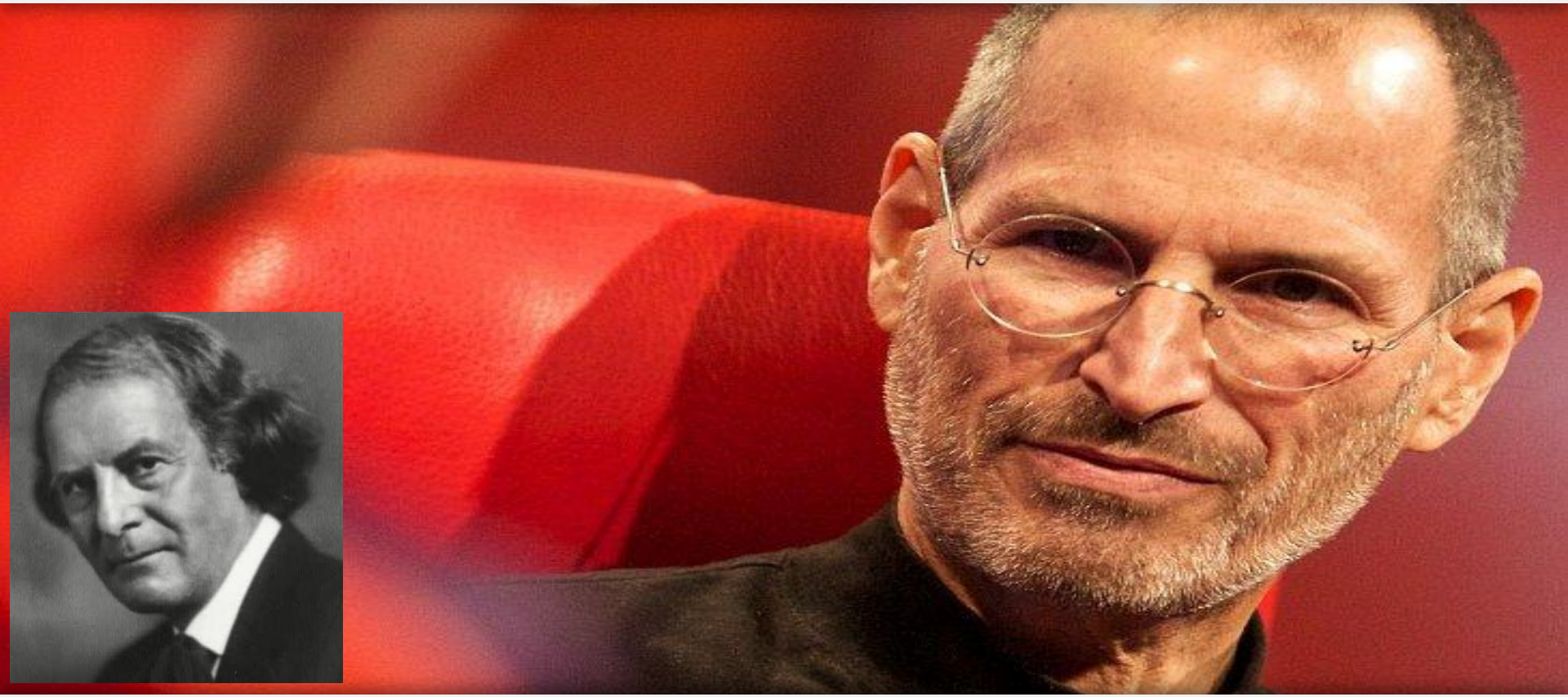
Закон Амдала

$$S(p) = \frac{1}{a + \frac{1-a}{p}}$$

$$E(p) = \frac{1}{1 + a(p-1)}$$

1% последовательных операций - сокращение времени не более чем в 100 раз

Производительность суперкомпьютеров



Одна машина способна выполнить работу 50 заурядных людей, но нет машины, способной выполнить работу одного незаурядного человека.

Элберт Грин Хаббард

Особенности текущего момента

- Потребность в суперкомпьютерах высока
- Эффективность использования суперкомпьютеров низка:

  Не все алгоритмы эффективно выполняются параллельными вычислительным системам

  Использование нескольких ядер последовательной программой составляет проценты и доли процентов

  Внутренние обмены данными, синхронизация, другие дополнительные операции снижают эффективность даже параллельных программ

  При решении конкретной задачи всегда есть минимальный объем вычислений, который имеет смысл возложить на одно процессорное ядро, определяющий максимальное число используемых в расчете ядер

Возможности суперкомпьютеров

• На первый план выходит ***алгоритмическая и программная эффективность решений***, а не рост частоты работы или числа процессоров – «закон Амдала против закона Мура».

• С помощью многопроцессорных суперкомпьютеров не всегда удается ***сокращать время*** решения задачи, но можно ***повышать сложность*** решаемых задач - за счет оперирования *большими объёмами данных*

• С точки зрения безопасности суперкомпьютеры и развернутые на их базе сервисы, в т.ч. облачные – новый и весьма специфический объект защиты

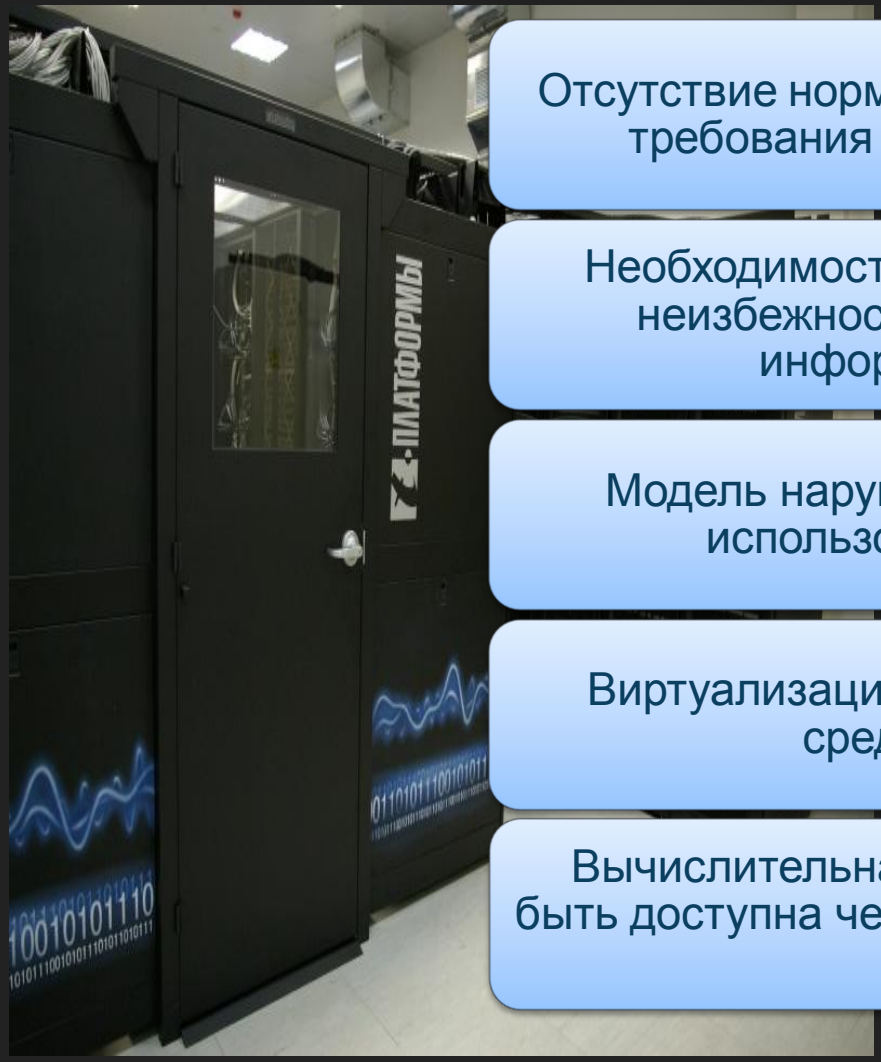
Безопасность суперкомпьютерных вычислений

Нормативный подход.
Стандарты информационной безопасности. Требования. Сертификация

Теоретический подход.
Моделирование безопасности систем с помощью математических методов. Формальное доказательство безопасности

Практический подход.
Выявление уязвимостей и способность противостоять атакам

Безопасность суперкомпьютеров
Нормативный подход



Отсутствие нормативных документов, регламентирующих требования безопасности для суперкомпьютеров

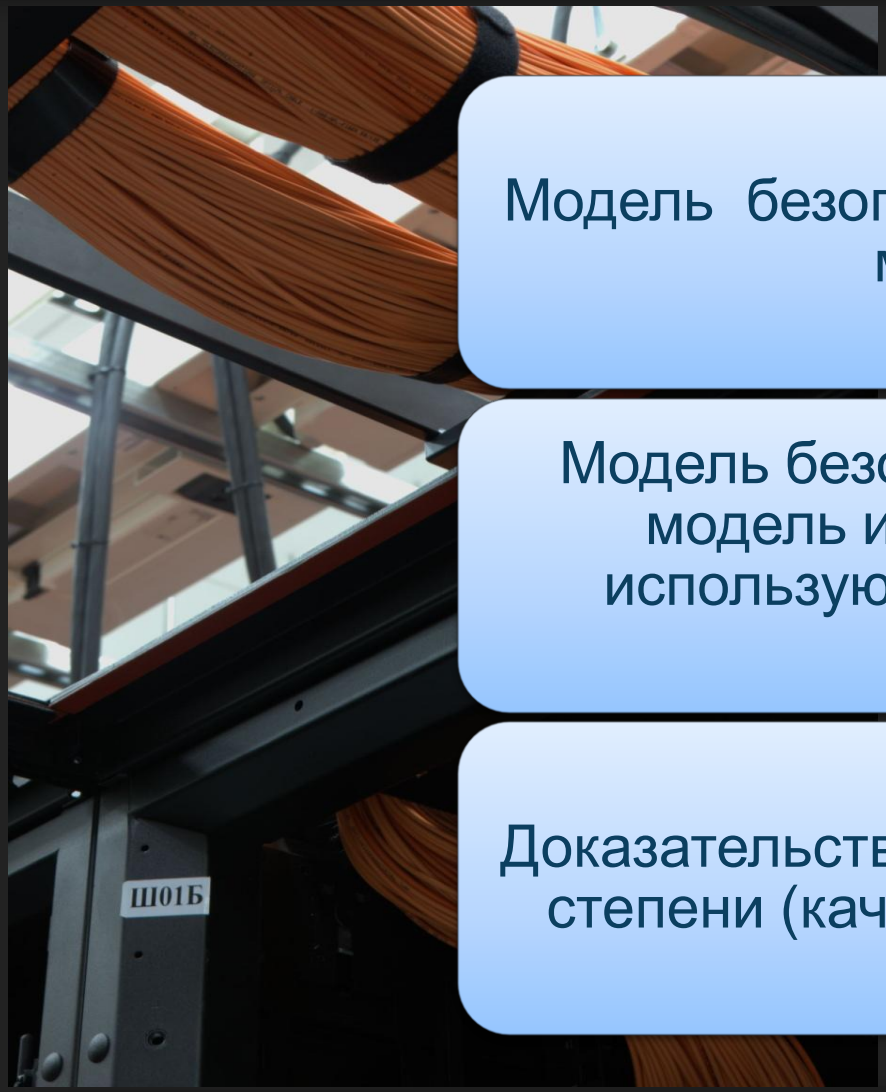
Необходимость разработки стандартов определяется неизбежностью обработки на суперкомпьютерах информации, содержащей гос. тайну

Модель нарушителя должна учитывать совместное использование вычислительных ресурсов

Виртуализация должна рассматриваться как базовое средство разграничения доступа

Вычислительная мощность суперкомпьютеров должна быть доступна через сеть Интернет, в т.ч. с использованием облачных технологий

Безопасность суперкомпьютеров
Теоретический подход



Модель безопасности должна быть подчинена модели вычислений

Модель безопасности трансформируется в модель изолированности процессов, использующих общие вычислительные ресурсы

Доказательство безопасности основывается на степени (качестве) виртуализации ресурсов

Степень виртуализации

Степень виртуализации (ее качество) – определяется возможностью выявить различие между реальными и виртуальными вычислительными ресурсами

Интеграционная парадигма построения защищенных систем

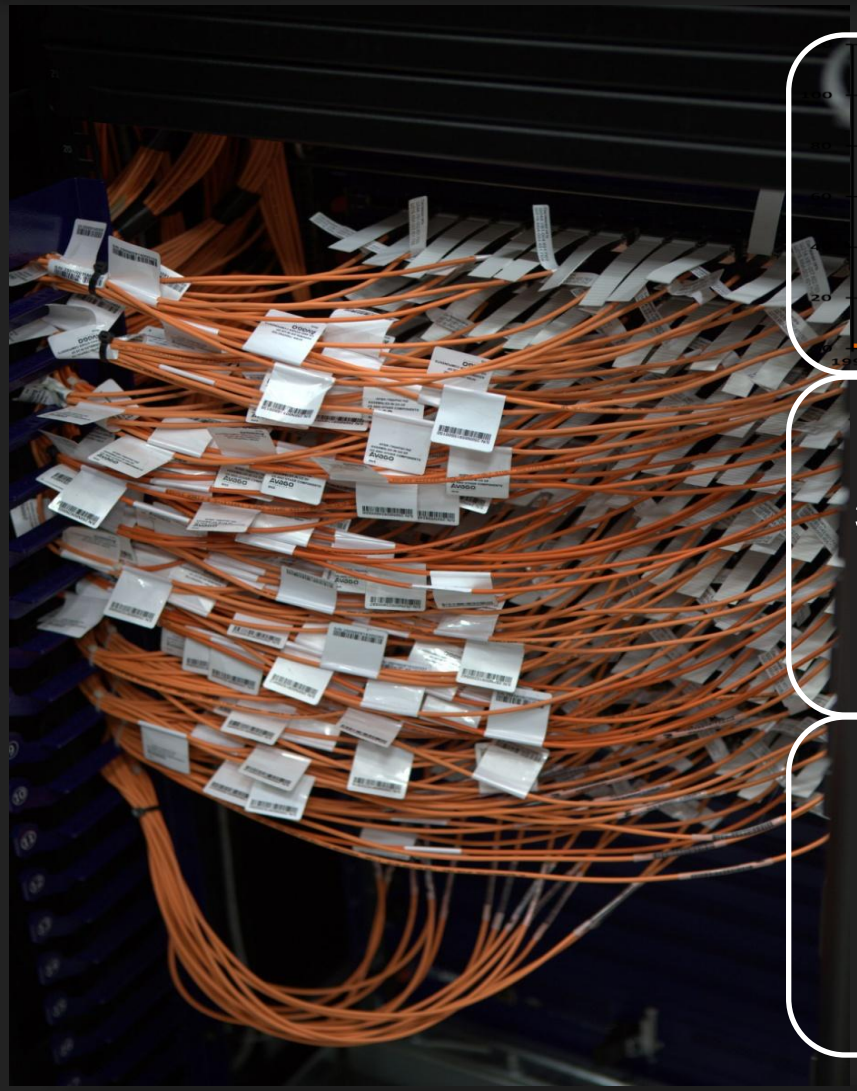
- Средства защиты должны контролировать все без исключения информационные взаимодействия
- Средства защиты должны быть инварианты по отношению к прикладным программам и опираться на абстрактное представление информационных взаимодействий
- Средства защиты должны контролировать информационные взаимодействия 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

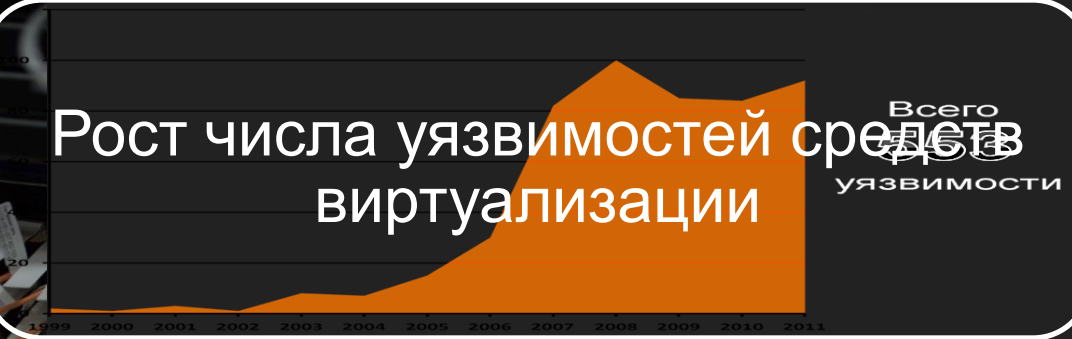
Безопасность суперкомпьютеров

Реальность всегда впереди теории.

Дуглас Хурд

Безопасность суперкомпьютеров
Практический подход





Рост числа уязвимостей средств виртуализации

Отсутствие дополнительных эшелонов защиты – механизмов предотвращения эксплойтов (типа ASLR, NXbit, UAC)

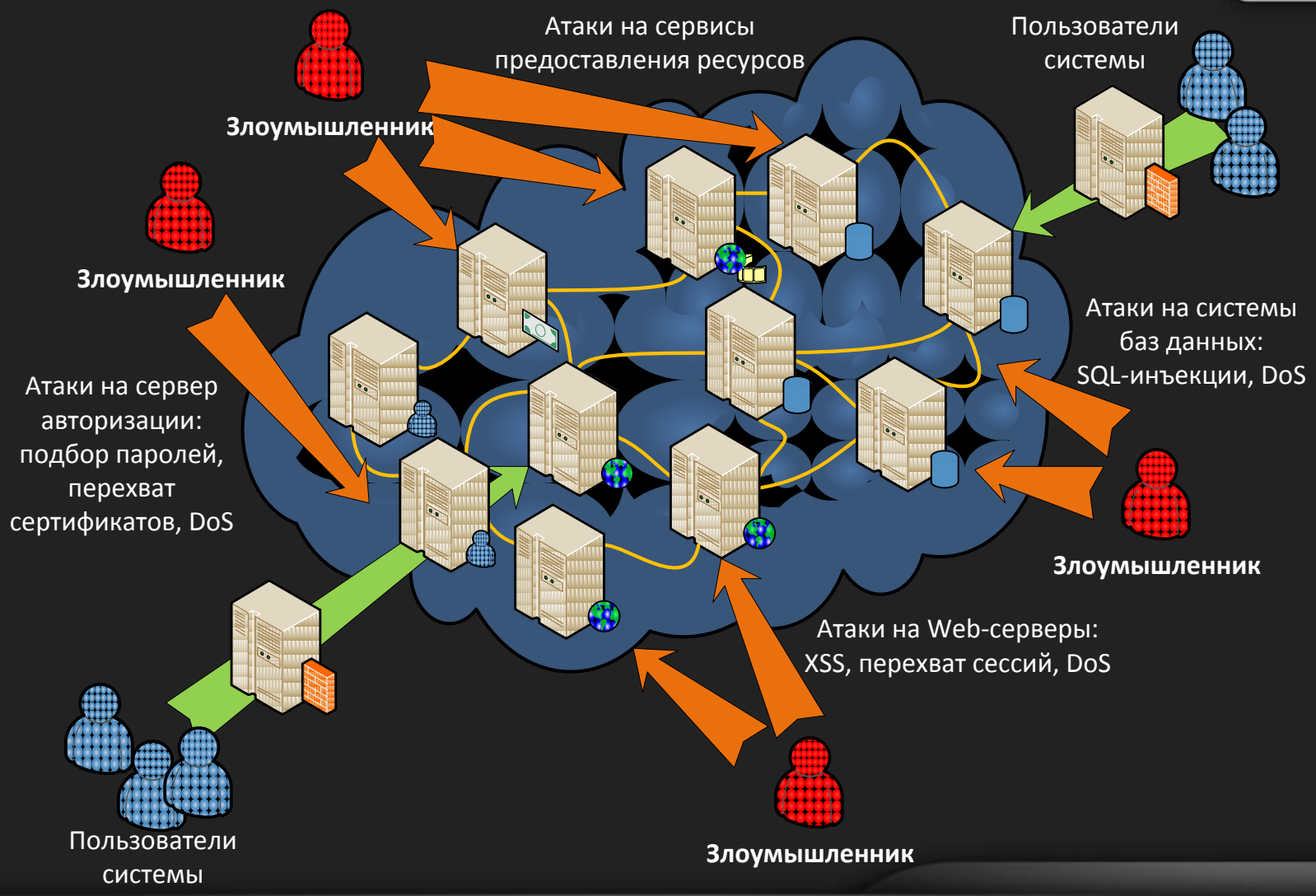
Использование возможностей виртуализации для скрытия действий злоумышленника (типа Blue-Pill)

Уязвимости суперкомпьютеров

Нет ничего настолько исправного, чтобы в нем не было ошибок.

Франческо Петрарка

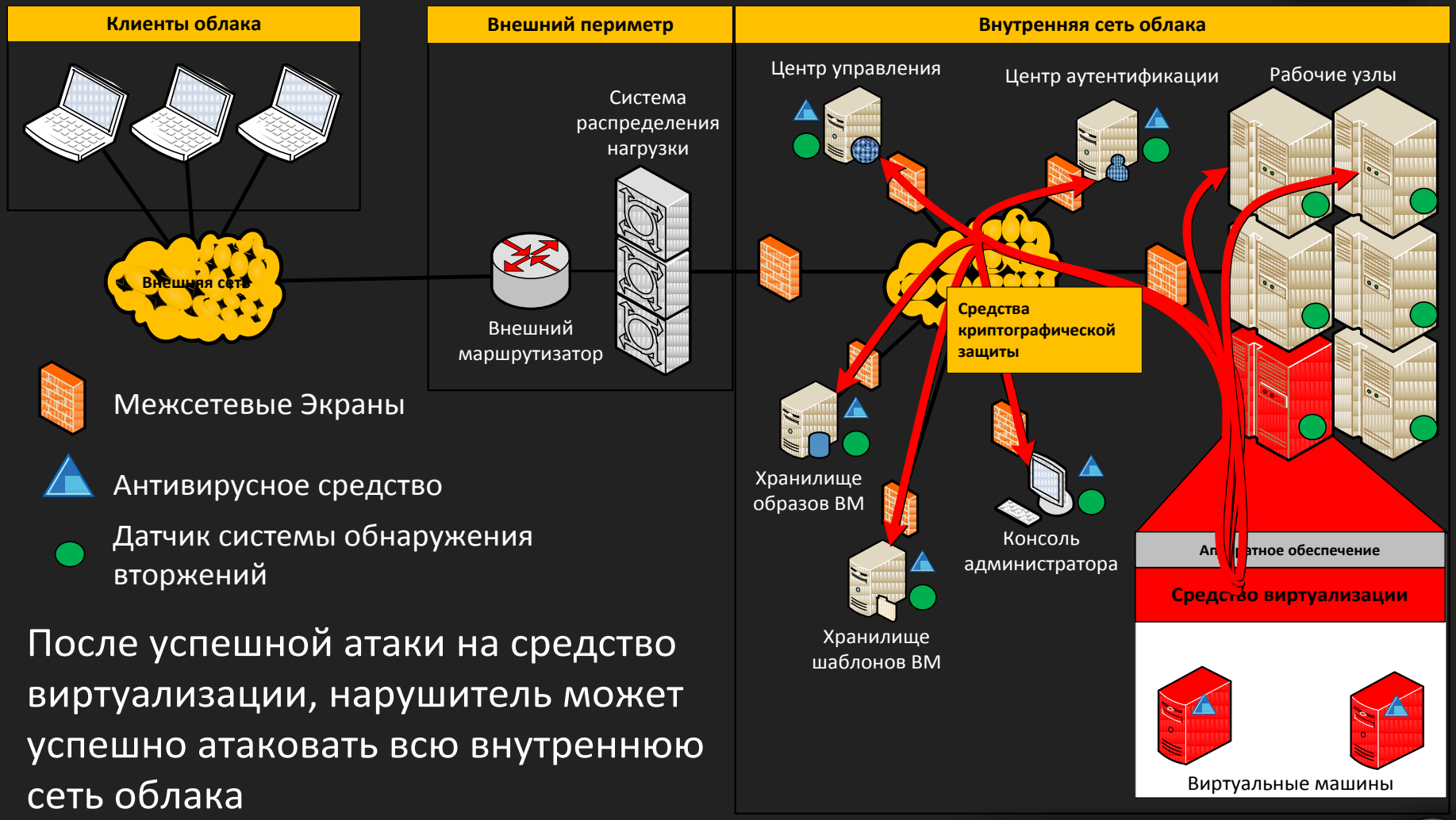
Атаки на системы облачных вычислений



Эффективны ли стандартные средства защиты для облака?

Существующие средства защиты не предотвращают атаки на средства виртуализации из виртуальной машины

Комплексная атака на облако



После успешной атаки на средство виртуализации, нарушитель может успешно атаковать всю внутреннюю сеть облака

Комплексная атака на систему облачных вычислений

1. Атака на ВМ из внешней сети
   - Запуск кода внутри ВМ
2. Выполнение кода в ядре ОС в ВМ
   - Взаимодействие с виртуальным оборудованием напрямую
3. Выполнение кода в гипервизоре
   - Атака на другие ВМ на том же узле сети
   - Выполнение кода на узле внутренней сети облака
4. Прослушивание траффика внутренней сети облака
   - Прослушивание данных пользователей
   - Получение доступа к другим ВМ в облаке
   - Модификация данных ВМ
5. Выполнение DoS атак на другие узлы и ВМ
   - Запуск механизмов самовосстановления облака
   - Инициация механизмов миграции ВМ
6. Атаки на системы управления облаком
   - Получение контроля за всем облаком

Не знаю, что лучше - зло ли, приносящее пользу , или добро, приносящее вред

Микеланджело Буонаротти

Использование суперкомпьютеров для решения задач безопасности

- Криптоанализ
- Анализ результатов мониторинга
- Поиск уязвимостей
- Моделирование противостояния в сети Интернет

Развитие средств защиты

Время - величайший из новаторов

Роджер Бэкон

Объекты глобального мониторинга

Действия программ и процессов

Сетевой трафик

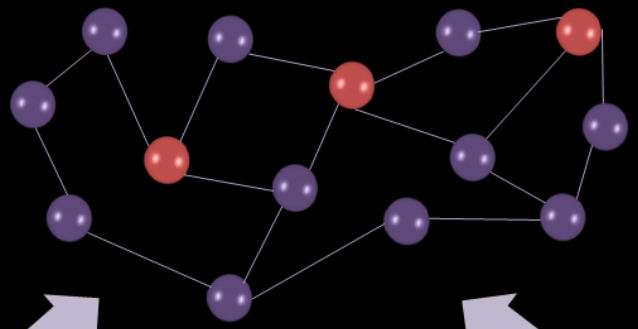
Активность пользователей в сети интернет, социальных сетях и т. д.

Анализ данных мониторинга

Многоагентные системы сбора информации

Граф агентов: $G = (V, E)$

Тип агента:
управляющий центр / рядовой узел



Матрица смежности
$M_{v \times v} = \{m_{i,j}\}$

- Имитационные модели
- Игровые модели
- Вероятностные модели
- Графовые модели

Анализ Интернет-коммуникаций и социальных сетей

Виртуальная среда и виртуальные идентичности

Пользователи

Виртуальная идентичность

Виртуальная среда и пространство интернет-коммуникаций

АНАЛИЗ

АНАЛИЗ

Интернет

Анализ информации о пользователе

Анализ информации о группе

Общество

3

Поиск уязвимостей с помощью суперкомпьютеров

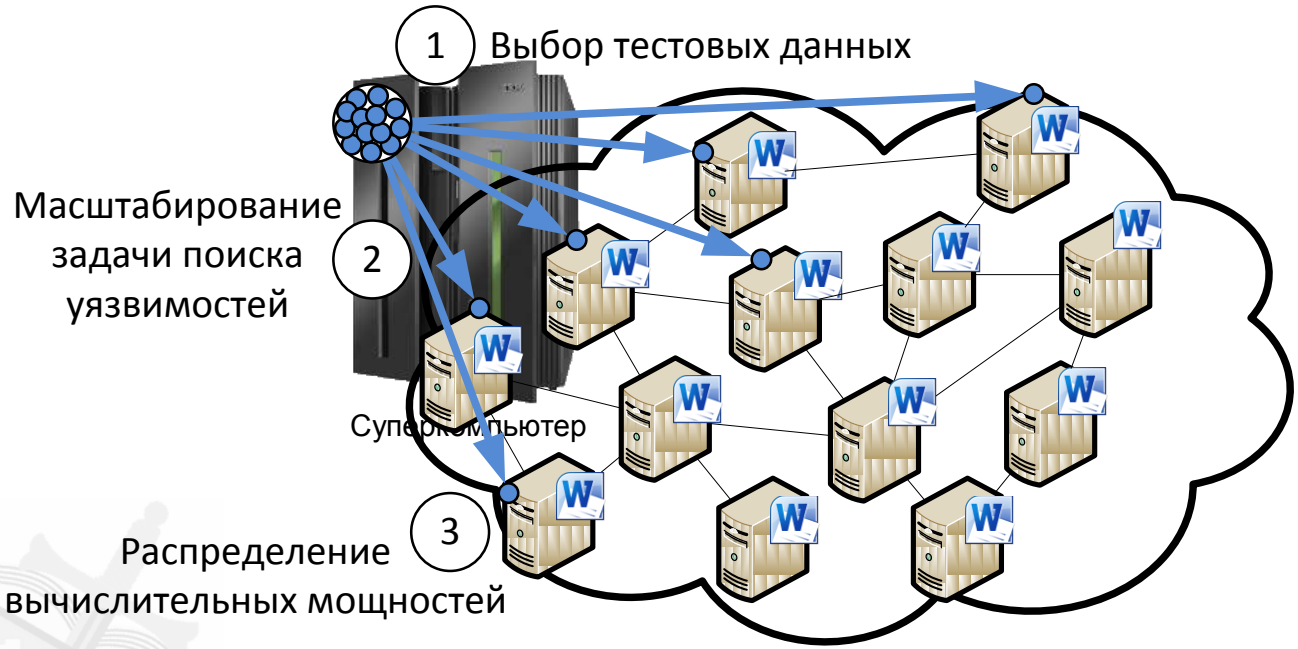
$$\frac{\partial}{\partial a}\ln f_{a,\sigma^2}(\xi_1)=\frac{(\xi_1-a)}{\sigma^2}\qquad \int T(x)\cdot\frac{\partial}{\partial\theta}f(x,\theta)dx=\mathrm{M}\left(T(\xi)\cdot\frac{\partial}{\partial\theta}\ln L(\xi,\theta)\right)$$

Тысячи путей уводят от цели, и лишь один единственный ведет к ней.

Мишель Монтень

Поиск уязвимостей

Масштабирование задачи поиска уязвимостей



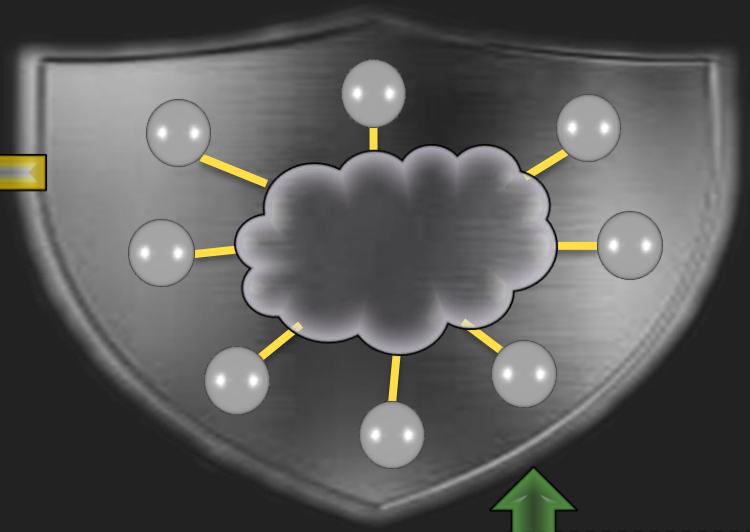
Мысль должна быть направлена на необъятное.

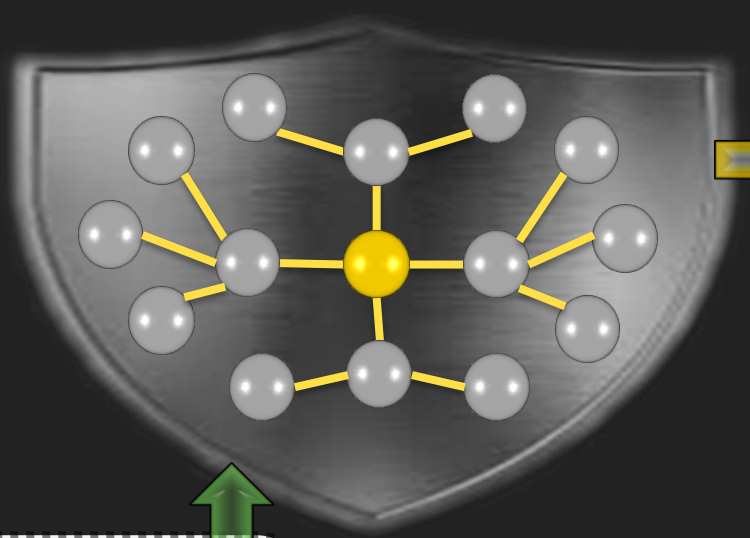
Марсилио Фичино

Противостояние ботсетей и систем защиты

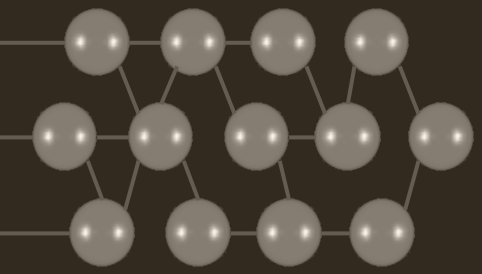
Системы защиты

Ботсеть



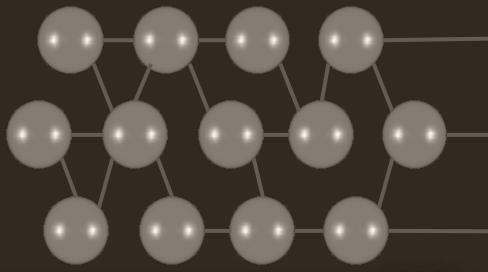


Ациклический граф



Противостояние = константность функционирования + нейтрализация противника

Случайный граф



Безопасность для суперкомпьютеров и суперкомпьютеры для безопасности

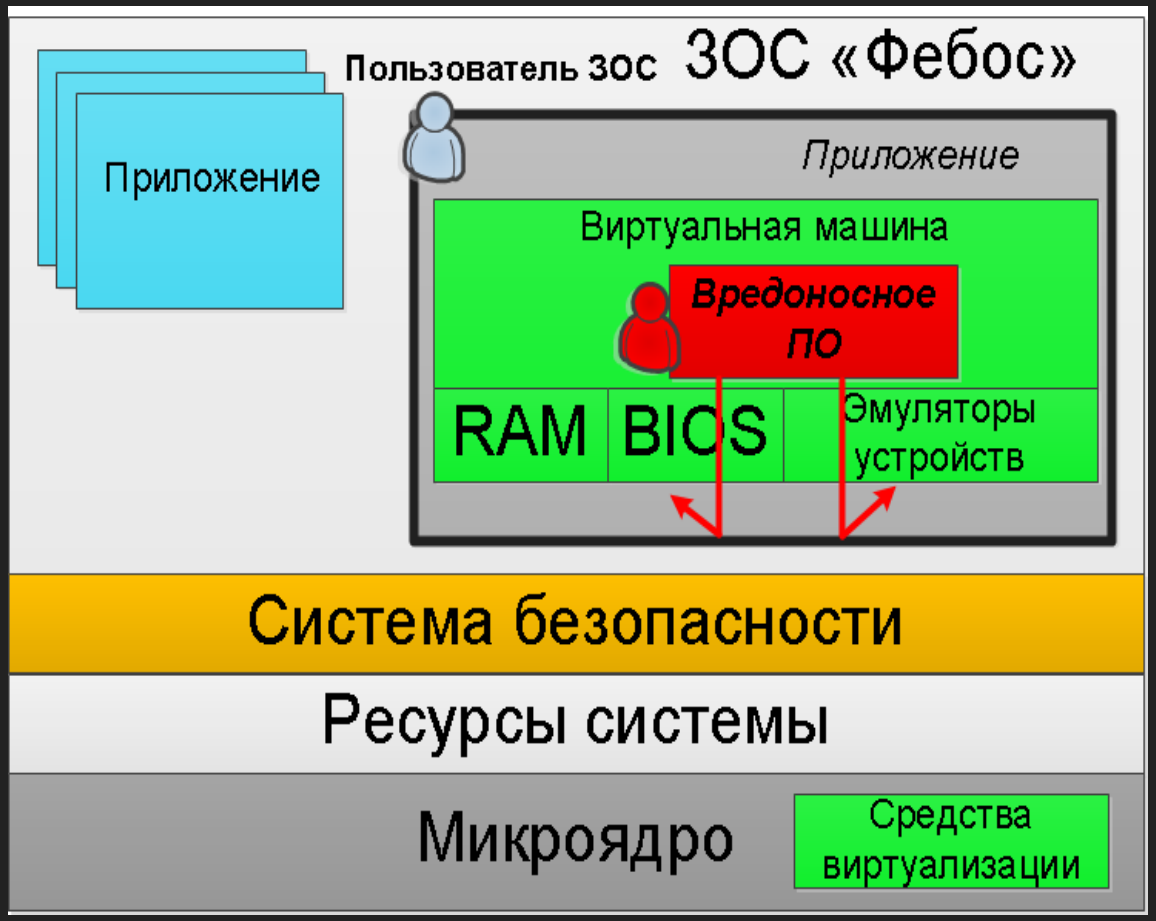
Виртуализация – основной инструмент обеспечения безопасности суперкомпьютерных вычислений

Использование суперкомпьютеров для обработки данных мониторинга и обеспечения апостериорной защиты

Применение суперкомпьютеров для выявления уязвимостей и моделирования кибербезопасности


НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
НЕОБИТ

Создание защищенной виртуальной среды



Средства виртуализации интегрированы в микроядро ЗОС

Компоненты ВМ изолированы внутри приложения ЗОС

Все действия пользователей ВМ ограничены и находятся под контролем системы безопасности ЗОС