

**Microsoft®**

# Защищенные облака – наше настоящее и будущее

**Владимир Мамыкин**

*Директор по информационной безопасности*

*ООО «Майкрософт Рус»*

[vladim@microsoft.com](mailto:vladim@microsoft.com)

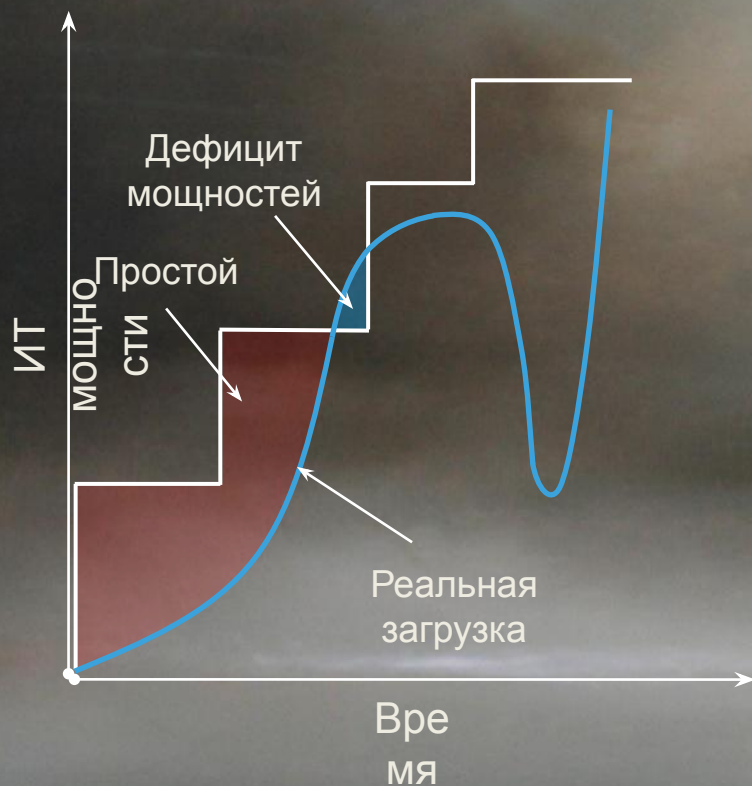
блог: <http://blogs.technet.com/mamykin/>

**ИНФОФОРУМ**

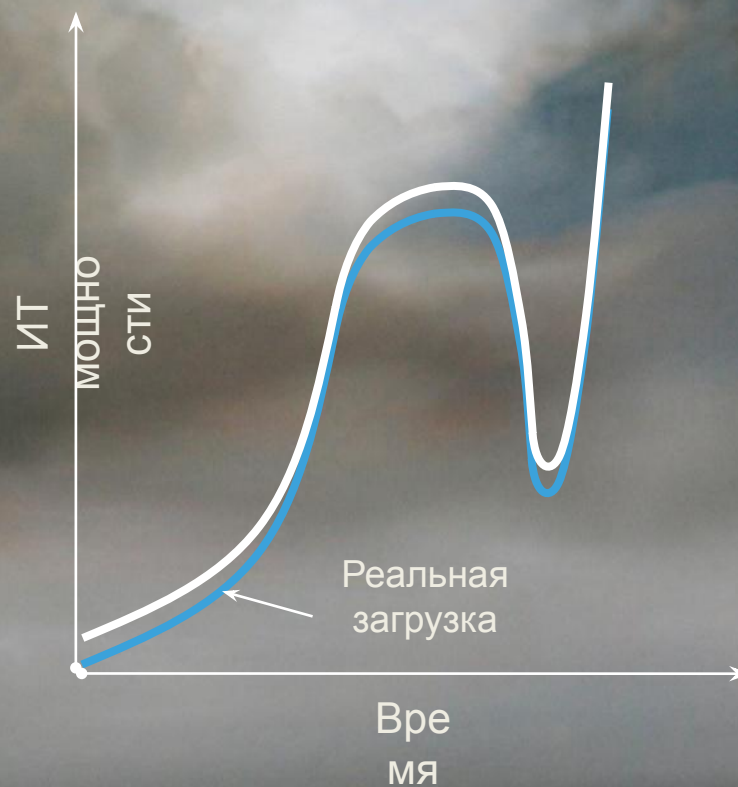
**7 февраля 2011**

# эластичность и масштабируемость

классический ЦОД



облачный ЦОД



# Облака: определения

- **Частные облака (Private Cloud)**
  - Принадлежат одной организации
- **Облака сообществ (Community Cloud)**
  - Инфраструктура сообщества
- **Публичные облака (Public Cloud)**
  - Общее использование
- **Гибридные облака (Hybrid Cloud)**
  - Композиция 2-х или более моделей, описанных выше

# публичные и частные облака



# Облака: что выбрать?



# Облака: новые возможности и новые проблемы

- Информация под контролем провайдера
  - Нет ограничений пространства и географии
- Изменения в ИТ процессах
  - Провайдер может иметь лучше налаженные процессы обеспечения ИБ
  - Физическая безопасность будет обеспечиваться провайдером
  - Юридическая независимость провайдера
- Централизованное хранение данных
  - Экономия за счет масштаба
  - Привлекательность для киберпреступников
- Проблемы хранения персональных данных
- Проблемы проведения расследования киберпреступлений

# Облака: задачи безопасности

1. Соответствие законодательству и управление рисками
2. Идентификация и контроль доступа
3. Целостность сервиса
4. Защита конечных точек
5. Защита информации

# 1. Соответствие законодательству и управление рисками

- Соответствие законодательству продолжает оставаться ответственностью Клиента
- Необходимость управлять рисками – ответственность Клиента
- Основа – взаимодействие Провайдера и Клиента
  - Необходима прозрачность процессов
- Необходима сильная внутренняя команда у Клиента
  - Для взаимодействия по контрактам
  - Для определения уровней контроля и метрик
  - Для интегрирования контроля во внутренние процессы Клиента



## 2. Идентификация и контроль доступа

- Кросс-доменное взаимодействие требует идентификации людей и устройств
- Аутентификация должна проводиться хотя бы для людей
- Идентификация\аутентификация должна быть зависимой от целей – нельзя требовать лишнего
- Основана на стандартах взаимодействия
- Процессы должны позволять работать с различными Провайдерами

# 3. Целостность сервиса

- Провайдер должен обеспечить прозрачность процессов разработки и внедрения сервиса с учетом
  - Обеспечения информационной безопасности и
  - Защиты персональных данных
  - Разработанной и принятой Клиентом Модели угроз
- Клиент должен обеспечить процессы получения сервиса с учетом многих Провайдеров, которые должны включать
  - Мониторинг ИБ Провайдера
  - Аудит
  - Проведение расследований
  - Обработку инцидентов безопасности
  - Непрерывность бизнеса
- Требования должны зависеть от используемых технологий и методов сбора информации

## 4. Защита конечных точек

- Защита конечных точек должна быть неотъемлемой частью рассмотрения обеспечения ИБ любых облачных вычислений т.к.
- Конечные точки являются основой проведения атак с использованием социальной инженерии

# 5. Защита информации

- Классификация данных – основа их защиты в облаке
  - Определите какие данные могут быть размещены в облаке
    - В соответствии с вашими требованиями
    - С требованиями законодательства
  - С какими последствиями
  - При каком уровне контроля с вашей стороны
- Использование технологий для непрерывной защиты
  - Шифрование\ЭЦП
- Определите, как будете решать новые задачи, связанные с
  - Обособленностью данных
  - Доступом к информации
  - С получением данных порциями
  - С новыми процессами обработки данных

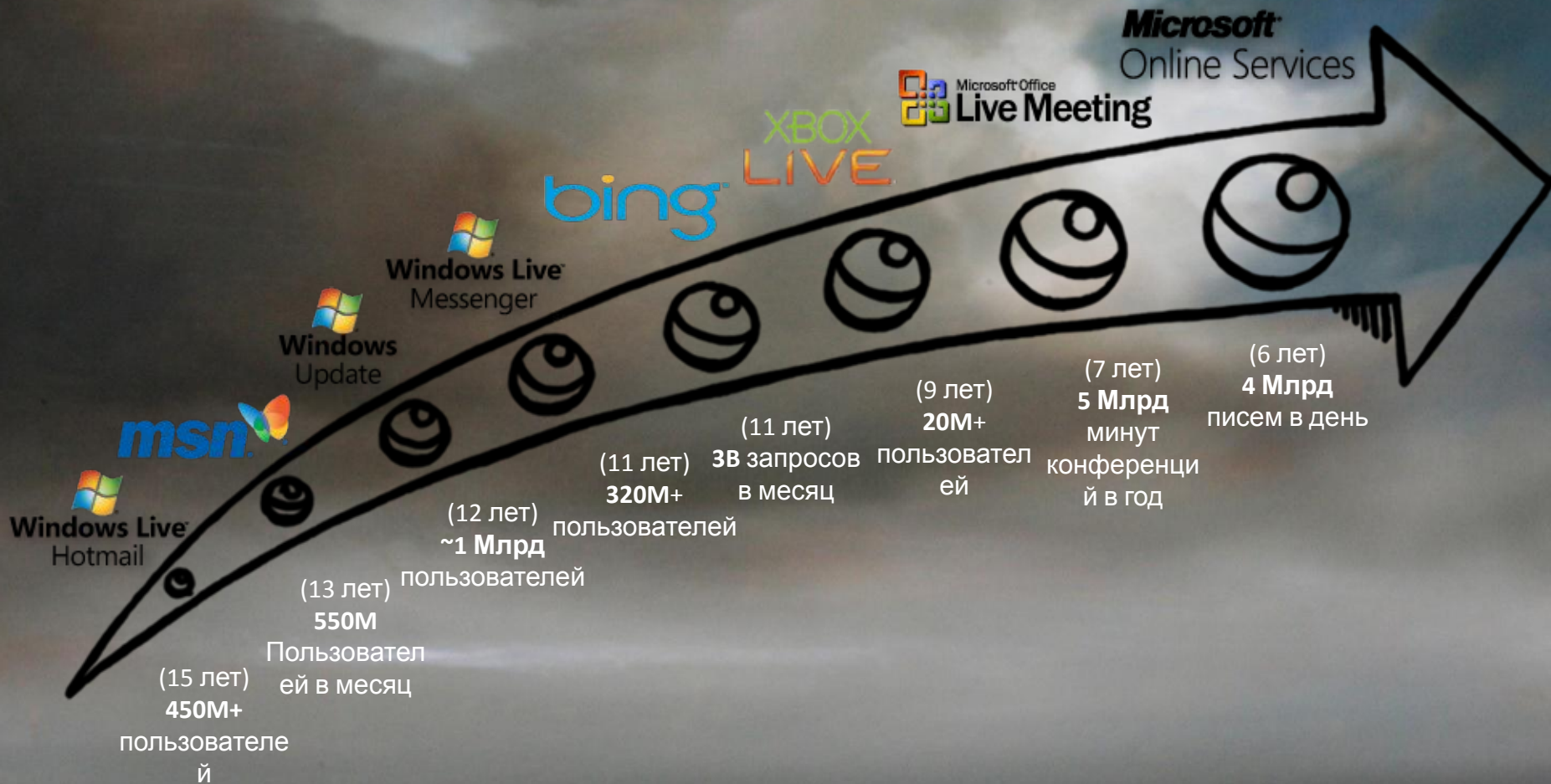
# национальное регулирование и глобальный характер услуг

- Требования территориальности
- Владение данными
- Защита информации
- Требования доступности для расследований
- Предотвращение доступа третьих сторон
- Налогообложение

Поставщик облачных услуг должен  
удовлетворять всем этим требованиям

Хорошая тема для международных  
сессий!

# почему Microsoft



# ресурсы Microsoft: около 100 ЦОДов



ЦОДы 4  
поколения



# ...ИЗ НИХ для публичного облака

## Серверная и Южная Америка



## Европа, Средний Восток и Африка



## Азия и Океания



6 собственных датацентров и будет больше  
+ облака партнеров



# поколения облаков

## 0 Мэйнфрейм

Черный ящик

## 1 NOaaS

Обычный DC

## 2 IaaS

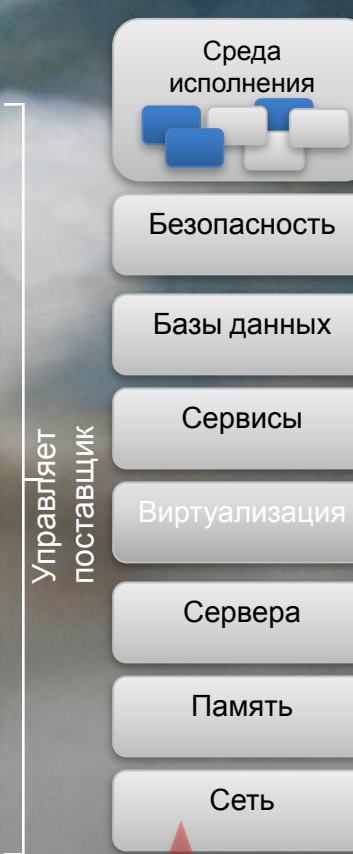
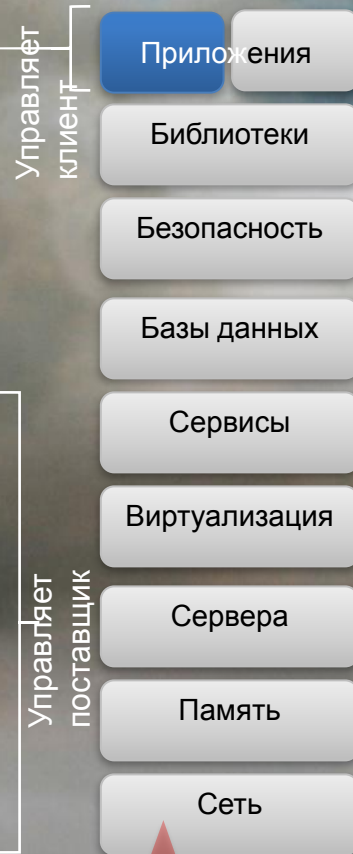
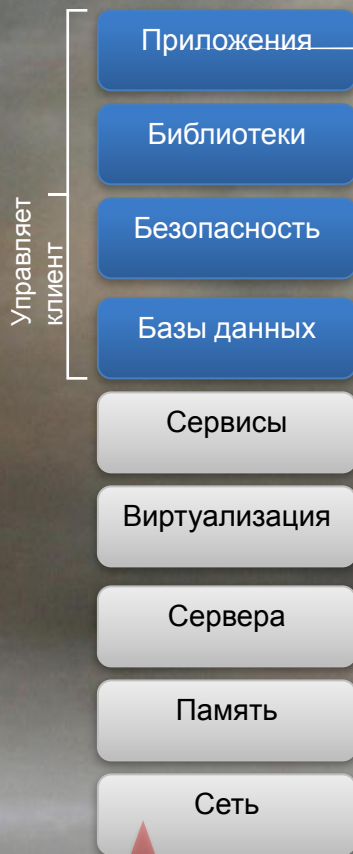
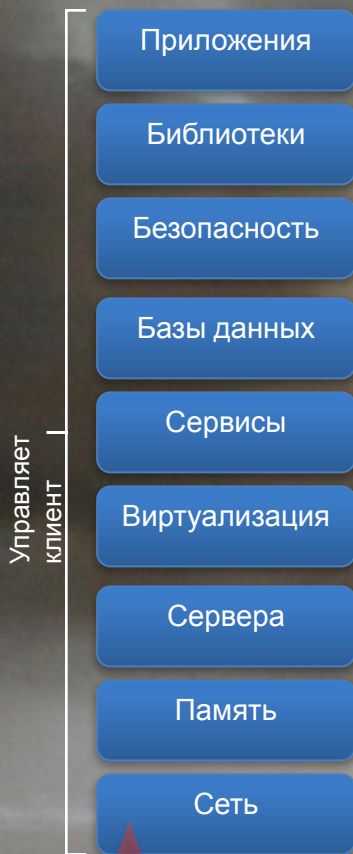
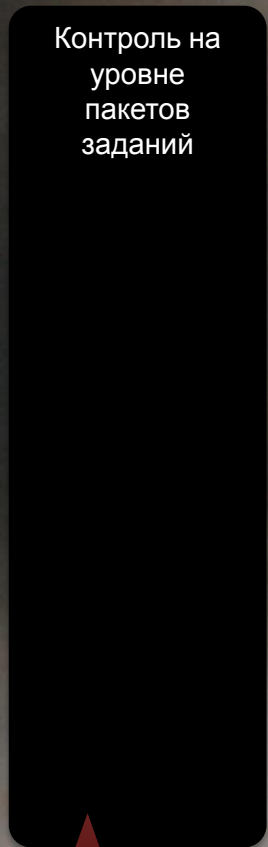
DC с виртуализацией  
и провиженингом

## 3 PaaS+SaaS

Платформа и/или  
ПО

## 4 CloudOS

Контроль  
объектов



Это – уже история

Состояние большинства

Пионеры облаков

Передавая линия

Перспективные разработки Microsoft

# общий подход к частному и публичному облаку



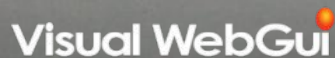
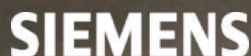
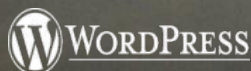
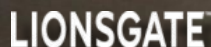
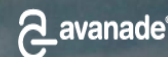
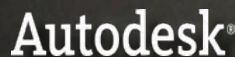
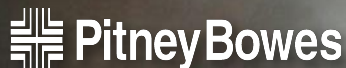
# решения с поставщиками серверов в

## разработке



Hyper-V Cube	Business Ready Configuration	Dynamic Infrastructure	Hitachi Unified Computing
<p>Integrated Management System Center/OpenView</p>	<p>Integrated Management System Center/Open Manage</p>	<p>FlexFrame for SAP ManageNow</p>	<p>Integrated Management System Center</p>
<p>Pre-configured Workloads SQL, Exchange, VDI</p>	<p>Pre-configured Workloads Virt, VDI, Exchange, DPM, Horizontal</p>	<p>Pre-configured Workloads (Specific Workloads TBD)</p>	<p>Pre-configured Workloads Horizontal</p>
<p>Windows Server 2008 R2 Hyper-V</p>	<p>Windows Server 2008 R2 Hyper-V</p>	<p>Windows Server 2008 R2 Hyper-V</p>	<p>Windows Server 2008 R2 Hyper-V</p>
<p><b>Blade System and P400</b></p>	<p><b>PowerEdge/EqualLogic</b></p>	<p><b>Primergy CX1000</b></p>	<p><b>Hitachi Unified Computing</b></p>
<p>G7 Blade System Technology</p>	<p>Dell PowerEdge R410, R710/R810/R910</p>	<p>Primergy Servers</p>	<p>Hitachi Blade Symphony Symphony 1000, Symphony 2000</p>
<p>Converged Fabric Network/iSCSI</p> <p>Virtual Connect/Flex-10</p> <p>P4000 Storage Coupled with HA/DR</p>	<p>Converged Fabric Network/iSCSI</p> <p>Cisco Blade Switch</p> <p>Dell PowerVault &amp; EqualLogic</p>	<p>TBD</p> <p>Eternus Storage FC or iSCSI</p>	<p>3rd Party SAN/Networking</p> <p>Brocade, Ciena, Cisco, Emulex, QLogic</p> <p>Hitachi Universal Storage Platform</p>

# в облака с Microsoft



**СПАСИБО**

**!!!**

**Владимир**

**Мамыкин**

[vladim@microsoft.com](mailto:vladim@microsoft.com)