Microsoft

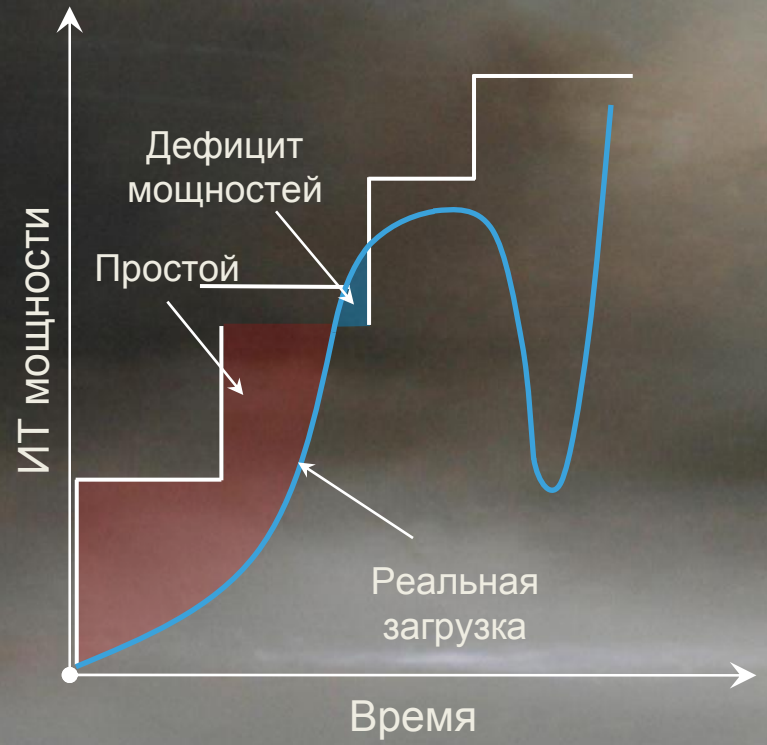
Безопасность облачных вычисленгий

Владимир Мамыкин
Директор по информационной безопасности
ООО «Майкрософт Рус»
vladim@microsoft.com
блог: http://blogs.technet.com/mamykin/

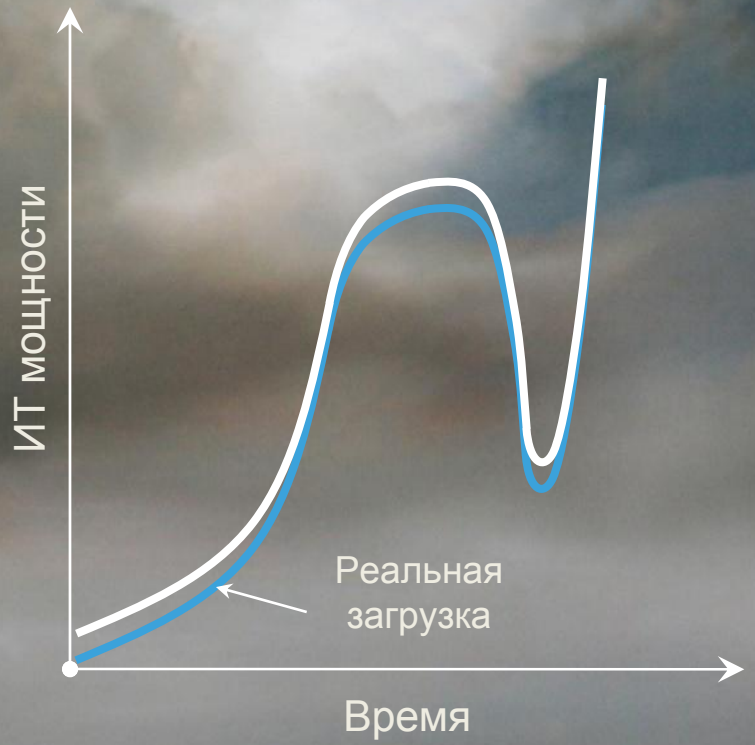
Москва
31 мая 2011

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

Источник: NIST (http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc)

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
  - Для российских государственных организаций это, в том числе, использование сертифицированных по требованиям ФСБ и ФСТЭК продуктов
- Необходимость управлять рисками – ответственность Клиента
- Основа – взаимодействие Провайдера и Клиента
  - Необходима прозрачность процессов
- Необходима сильная внутренняя команда у Клиента
  - Для взамодействия 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 проводится 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
- Лучшее решение – многофакторная аутентификация: USB-токены, смарт-карты

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 приложений и используемой ими информации

4. Защита конечных точек

- Защита конечных точек должа быть неотъемлемой частью рассмотрения обеспечения ИБ любых облачных вычислений так как
  - 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 соглашений !

почему Microsoft

ресурсы Microsoft: около 100 ЦОДов



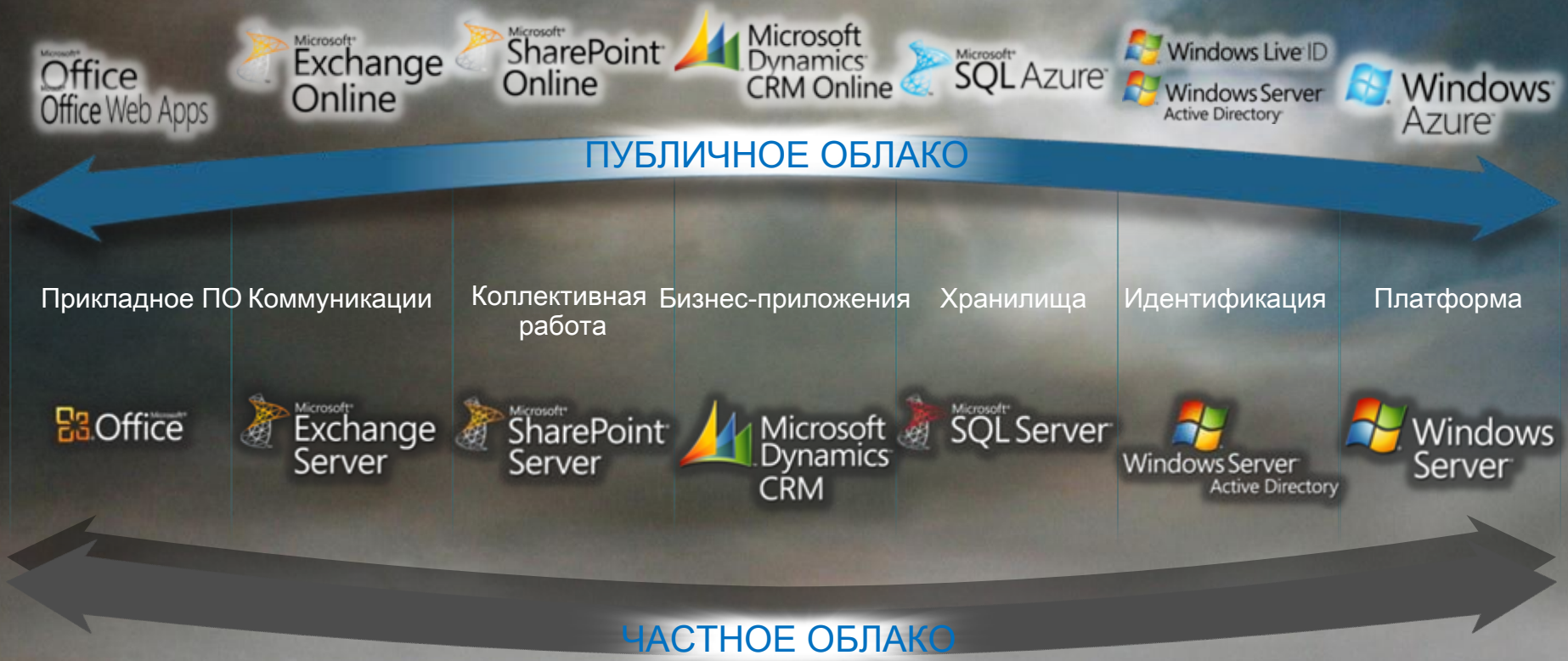


ЦОДы 4 поколения

...из них для публичного облака

6 собственных датацентров и будет больше
+ облака партнеров

общий подход к частному и публичному облаку



Продукты, используемые в частных облаках

- сертифицированы ФСТЭК (все)

- сертифицированы ФСБ (основные платформенные)

Microsoft

СПАСИБО !!!

Владимир Мамыкин
vladim@microsoft.com