Microsoft
Secure Software Development

Безопасность облачных вычислений

Бешков Андрей
Руководитель программы информационной безопасности
E-mail: abeshkov@microsoft.com
Twitter: @abeshkov

Содержание

- Вопросы безопасности «облачных» технологий
- Модель безопасности платформы Windows Azure
  - Центры обработки данных
  - Сетевое взаимодействие
  - Изоляция и доступность приложений
  - Разработка приложений
  - Аутентификация и контроль доступа
  - Защита данных
- Заключение

Безопасны ли «облачные» технологии?

Где расположены мои данные?

Можно ли доверять «облаку» Microsoft?

Кто может получить доступ к моим данным?

Как удостовериться, что сервис провайдер следует установленным правилам ИБ?

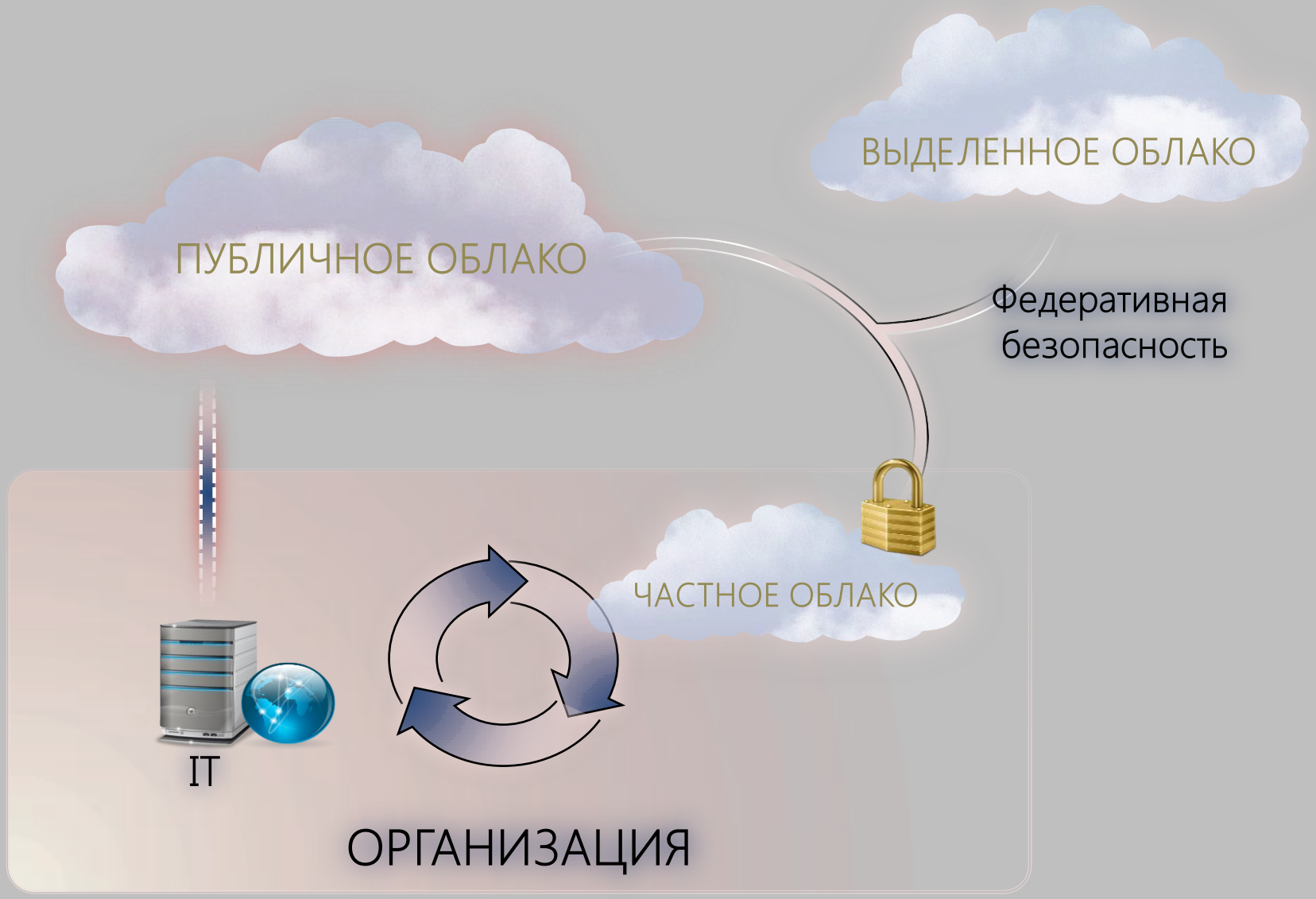
Что случится, если что-то пойдёт «не так»?

The Economist

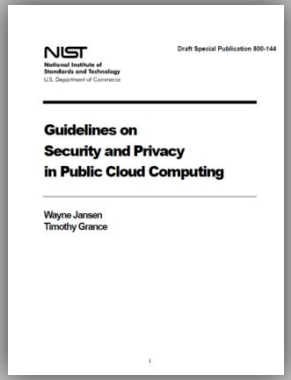
"What is holding IT managers back from going to the cloud is fear about security."

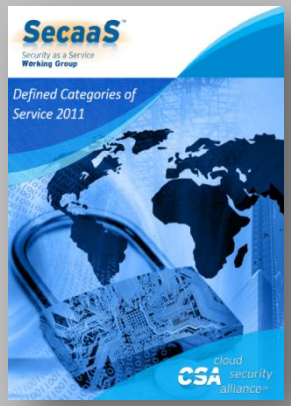
"Cloudy with a chance of Rain", The Economist, March 5, 2010

Модели «облачных» сервисов



Вопросы обеспечения облачной безопасности





Платформа в «облаке»

Windows Azure

- Масштабируемая вычислительная платформа и хранилище
- Автоматизированное управление сервисом
- Привычные инструменты, технологии и языки программирования

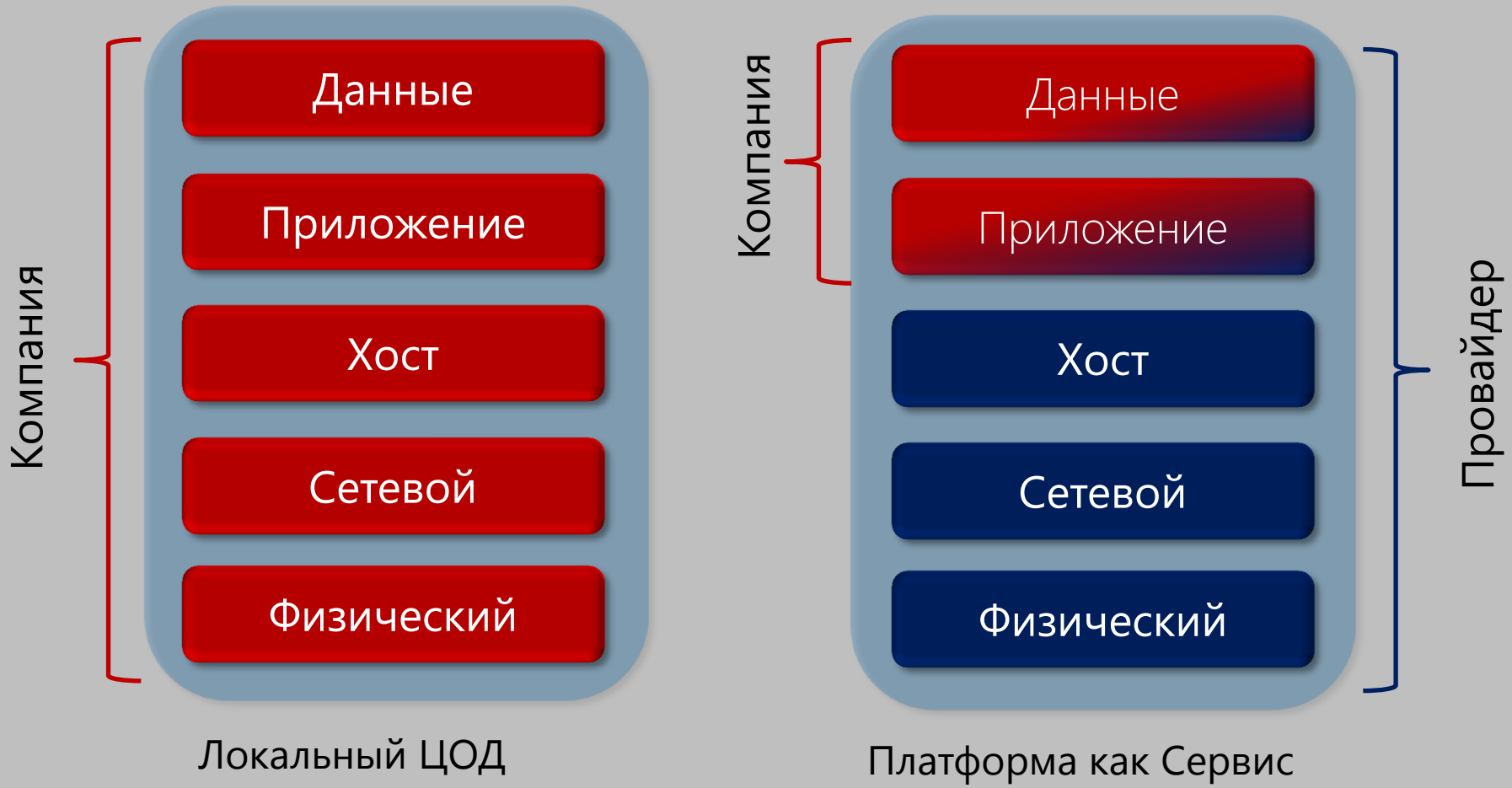
SQL Azure

- Реляционное хранилище в облаке
- Интеграция с инструментами разработки
- Автоматизированное управление БД

Windows Azure platform AppFabric

- Подключение существующего ПО к облаку
- Сервис контроля доступа
- Реализация сервисной шины

Уровни безопасности в PaaS (Windows Azure)



Безопасность ЦОД Microsoft

Безопасность ЦОД Microsoft

Физическая безопасность мирового уровня

- Ограниченный доступ 24x7
- Системы контроля доступа
- Видео-наблюдение
- Датчики движения
- Сигнализация событий нарушения безопасности

Международная сертификация

- Сертификация системы управления безопасностью ISO/IEC 27001:2005
- Ежегодная аттестация SAS-70 Type II
- Разрешение эксплуатации по FISMA

Как проверить безопасность ЦОД?

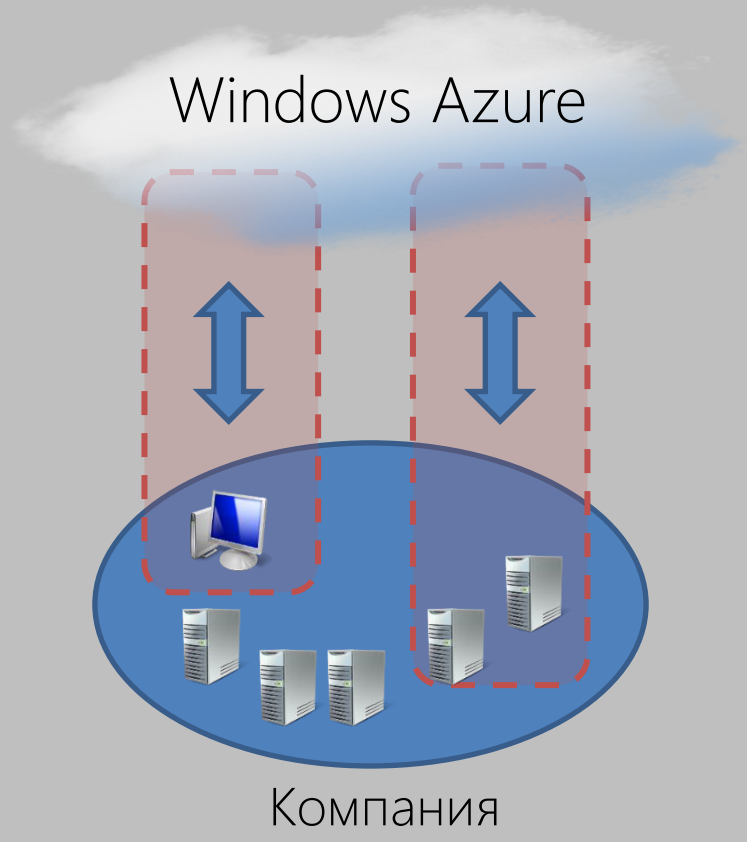
Сертификации ISO/IEC 27001:2005 и SAS 70 Type II

- Для своей «облачной» инфраструктуры Microsoft проводит ежегодную аттестацию по SAS 70 Type II и достигла сертификации ISO/IEC 27001:2005
  - т.е. Безопасность ЦОД Microsoft прошла все этапы сертификации
  - В Global Foundation Services реализованы более 150 контролов, описанных в ISO 27001
- «Облачная» инфраструктура получила авторизацию Federal Information Security Management Act (FISMA) на эксплуатацию для федеральных органов власти

Подключение сети к «облаку»

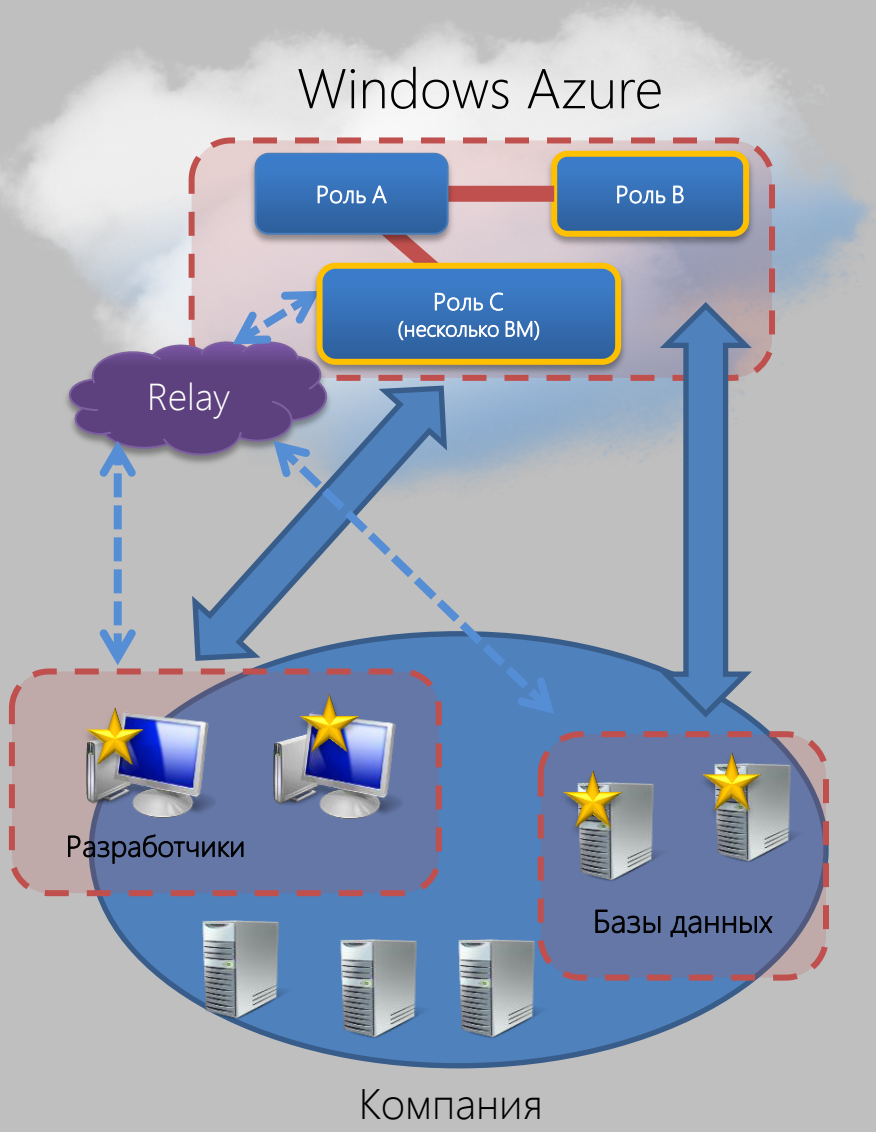
Windows Azure Connect

- Защита сетевого взаимодействия между локальной сетью и «облаком»
  - Поддержка стандартных IP-протоколов
  - IPsec используется для прозрачной защиты канала
- Позволяет реализовать «гибридную» прозрачную модель доступа к локальной сети
- Обеспечивает удаленное управление приложениями Windows Azure



Windows Azure Connect

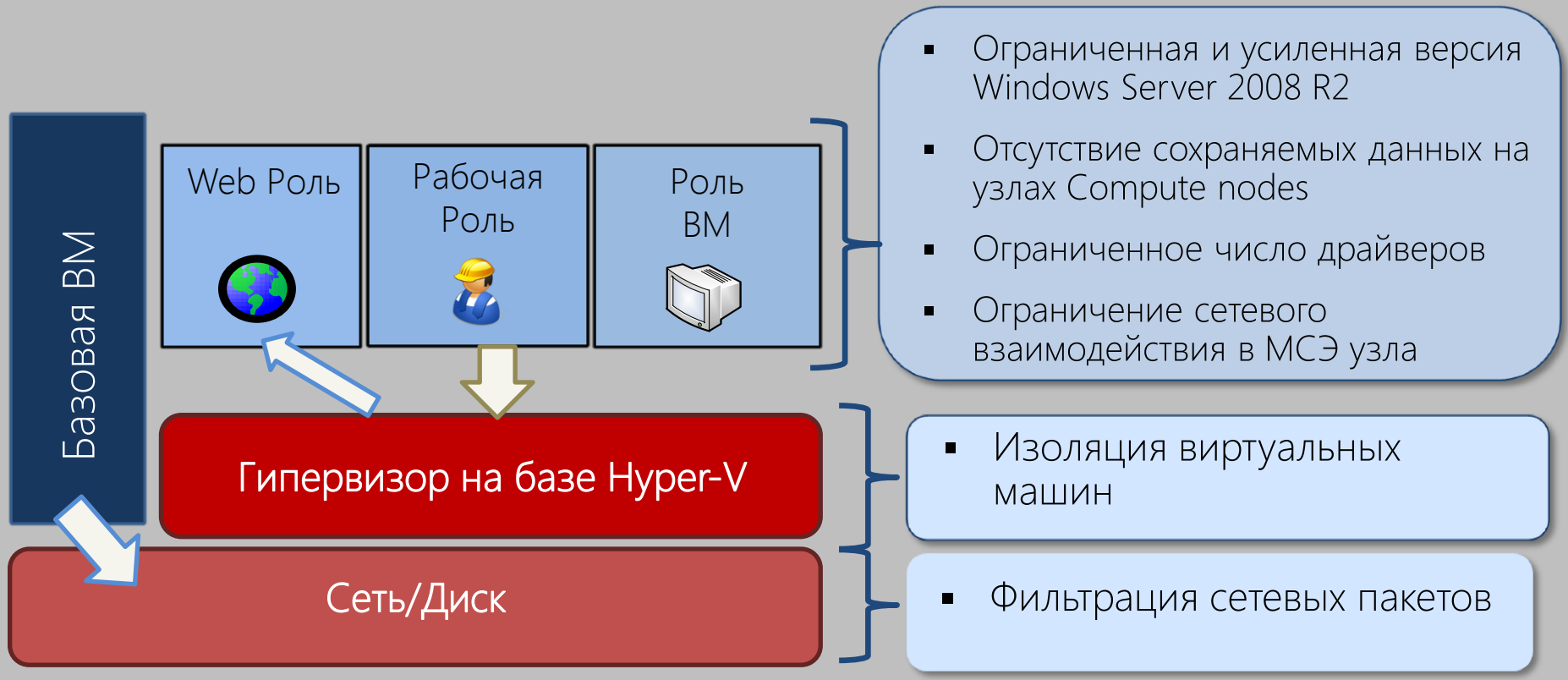
Управление доступом



- Управление политикой сетевого доступа через портал Windows Azure
  - Гранулярный контроль взаимодействия ролей Windows Azure и внешних компьютеров
- Автоматическая настройка IPsec
  - TLS-туннелирование через МСЭ/NAT с помощью ретранслятора в «облаке»
  - Политики доступа строго контролируются и обеспечивается полная защита канала с помощью сертификатов в IPSec

Изоляция приложений в Windows Azure

Гипервизор и «песочница»



- Код заказчика выполняется на выделенных виртуальных машинах
- ВМ изолированы с помощью основанного на Hyper-V гипервизора
- Весь доступ к сети и диску проходит через «базовую» ВМ

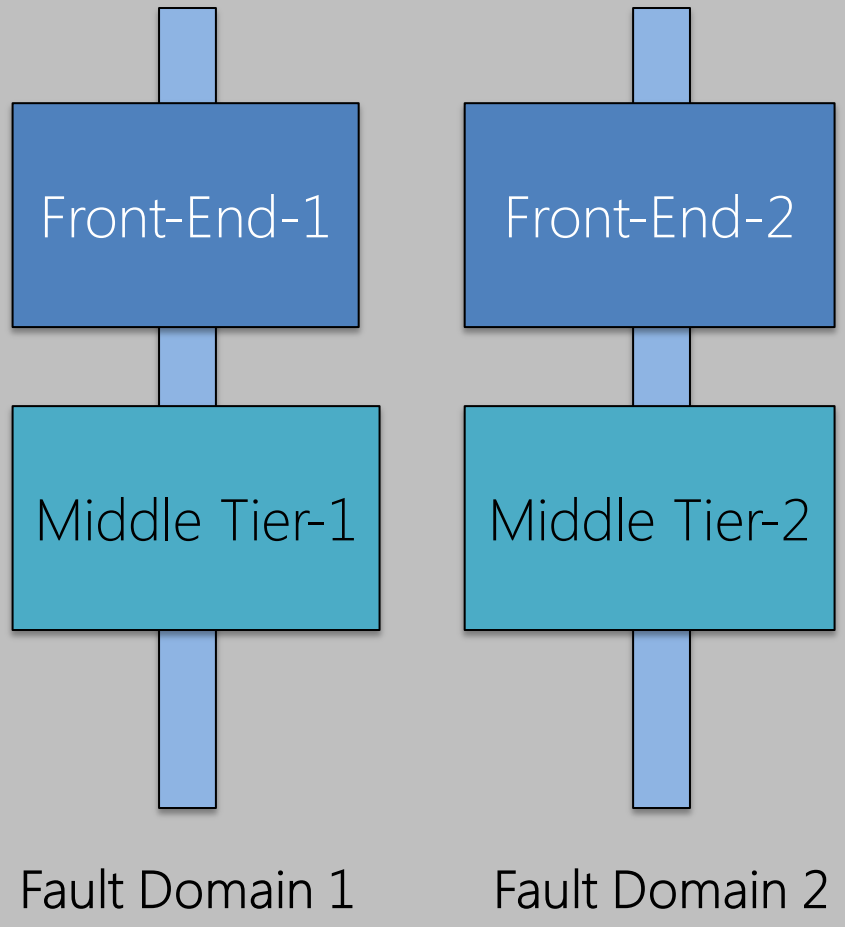
Безопасность Windows Azure Compute Node

Контроль границ безопасности

- Виртуальная машина является границей безопасности, на которой основана модель безопасности Windows Azure
  - ОС хоста и Fabric Controller являются доверенными
  - Нет доверия агенту в гостевой ОС
  - Агент Fabric Controller обеспечивает ограничение доступа ВМ только к IP-адресам виртуальных машина того же сервиса
    - А также контролирует доступ к интернет
- Fabric Controller использует сертификаты и правила МСЭ для авторизации доступа к ресурсам ЦОД

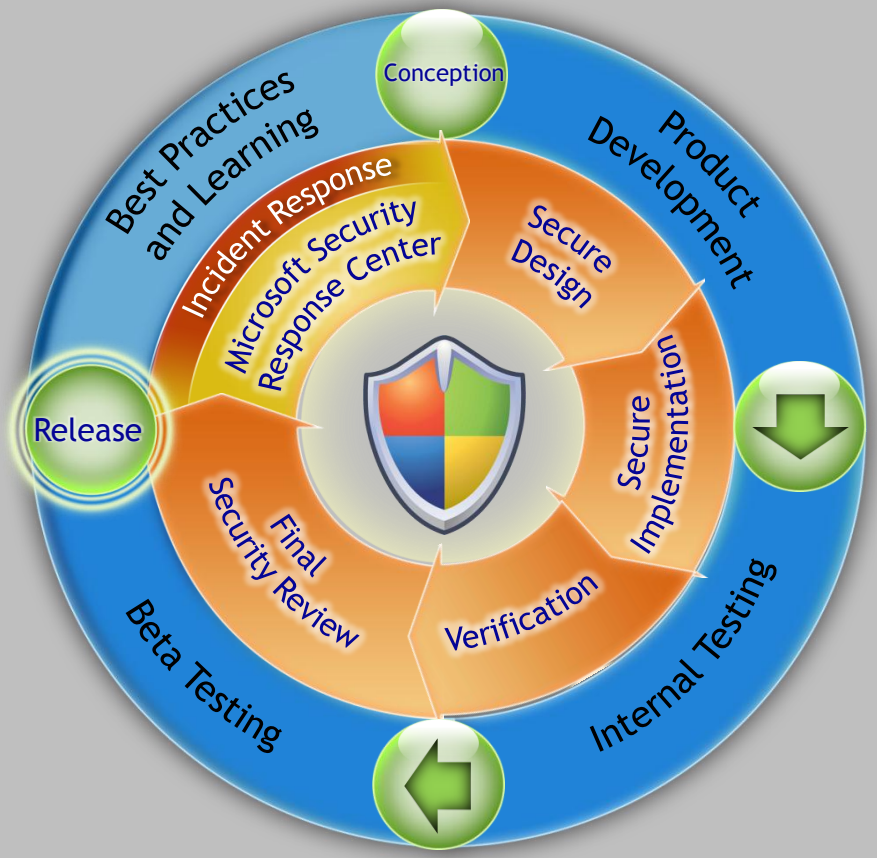
Доступность приложения
Fault Domain

- Потенциальный элемент выхода из строя в топологии ЦОД
  - Например, коммутатор в серверной стойке
- Windows Azure использует данные элементы при выделении сервисных ролей
  - 2-а fault domain на сервис
  - Алгоритм попытается обеспечить распределение сервиса между разными fault domain



Разработка безопасных приложений

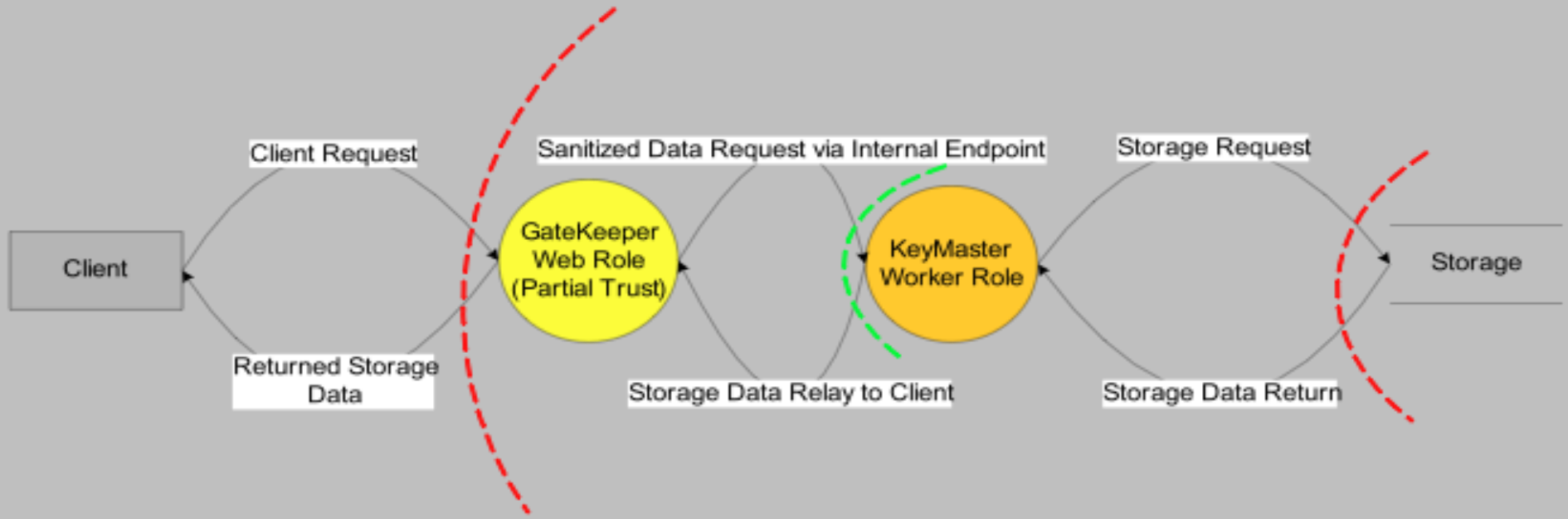
Применение Security Development Lifecycle



- Проверенная временем методология
  - Практический подход
  - Не ограничен Windows или Microsoft!
  - Проактивный – не просто «поиск ошибок»
  - Нахождение проблем как можно раньше в цикле разработки (TM)
- Защищает клиентов платформы Windows Azure:
  - Уменьшение количества уязвимостей
  - Уменьшение уровня уязвимостей

Рекомендуемая архитектура приложений

Диаграмма потоков данных в модели Gatekeeper

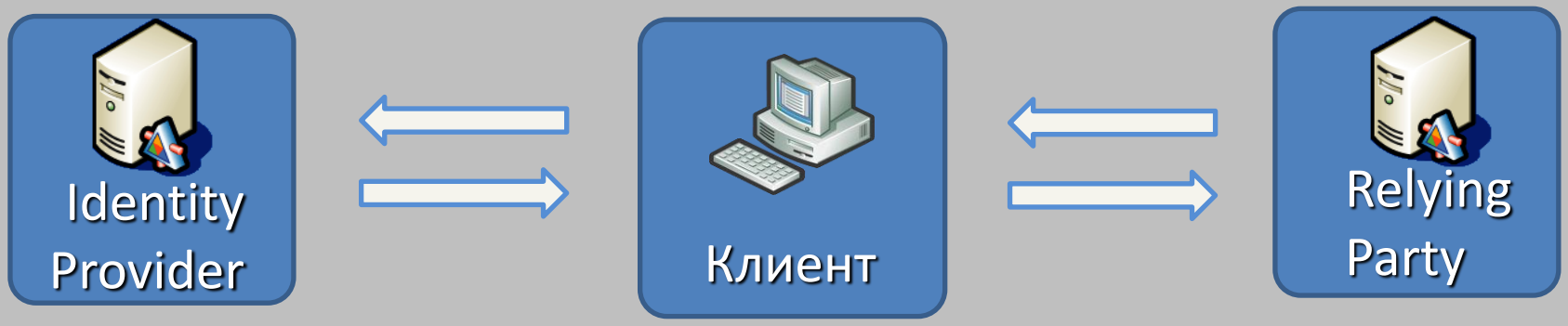


- Изолированная web-роль и разделение полномочий ролей для максимального использования модели Windows Azure Partial Trust
- Модель Gatekeeper для разделения полномочий ролей и изолирования привилегированного доступа
- Использование нескольких ключей доступа для ограничения доступа к данным (если используется другая архитектурная модель)

Модель аутентификации на основе «заявок»

- Уровень абстракции управления идентификационными данными
- Основанный на международных стандартах набор технологий

1. Получение политики (WS-MetadataExchange)
Describes the Required Claims



2. Получение токена (WS-Trust)
Tokens Contains Claims

3. Использование токена (WS-Security)
Associate Tokens with Messages

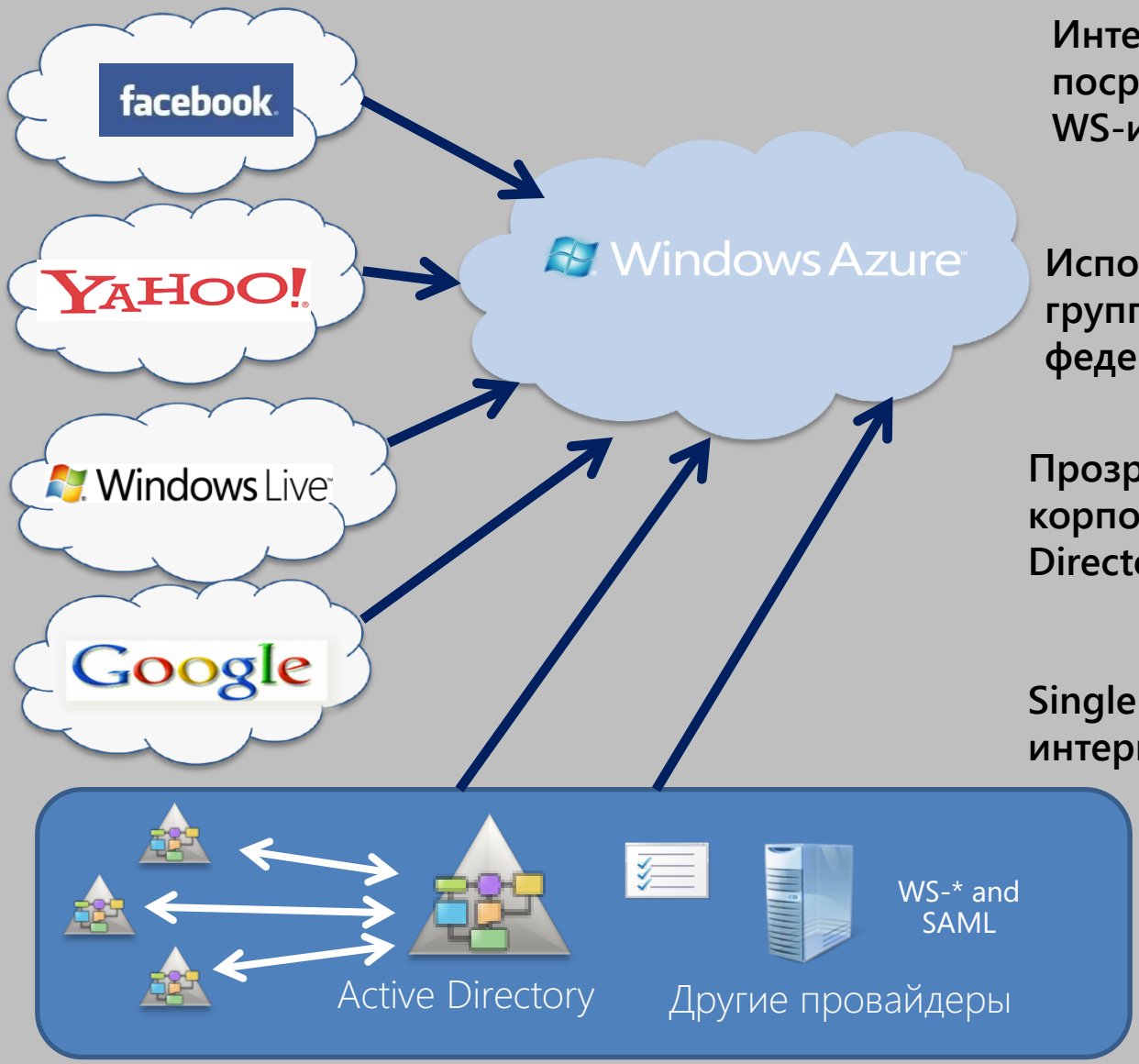
- Токены SAML
- WS-* (WS-Security, WS-Trust, WS-Federation)

OASIS

W3C

Как выполняется аутентификация

Сервис Azure Access Control



Интеграция с другими системами посредством открытых стандартов WS-и SAML 2.0

Использование Active Directory и групп (ролей) посредством федерации

Прозрачный доступ для корпоративных приложений с Active Directory

Single sign-on с популярными интернет-провайдерами

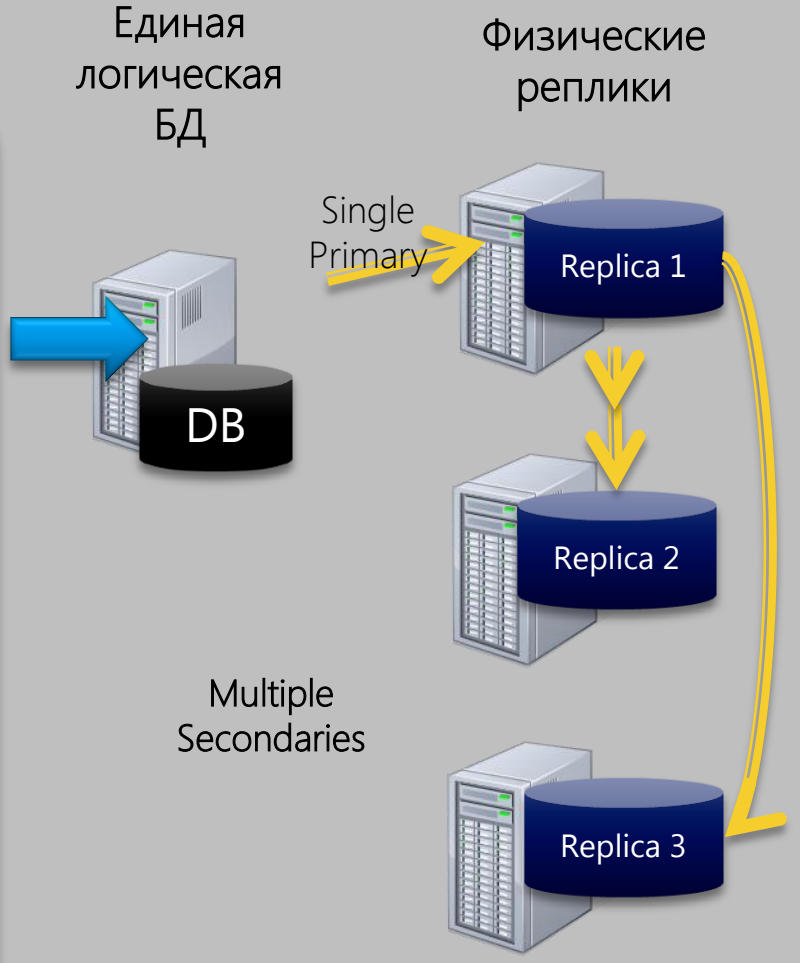
Безопасность SQL Azure

Microsoft SQL Server

- SQL и интегрированая Windows аутентификации
- Авторизация на основе пользователей и ролей в БД
- Серверные роли serveradmin, securityadmin и dbcreator
- Доступ посредством TDS + SSL по порту TCP 1433
- Использование МСЭ хоста для блокирования IP-пакетов
- Поддержка встроенного шифрования (TDE)

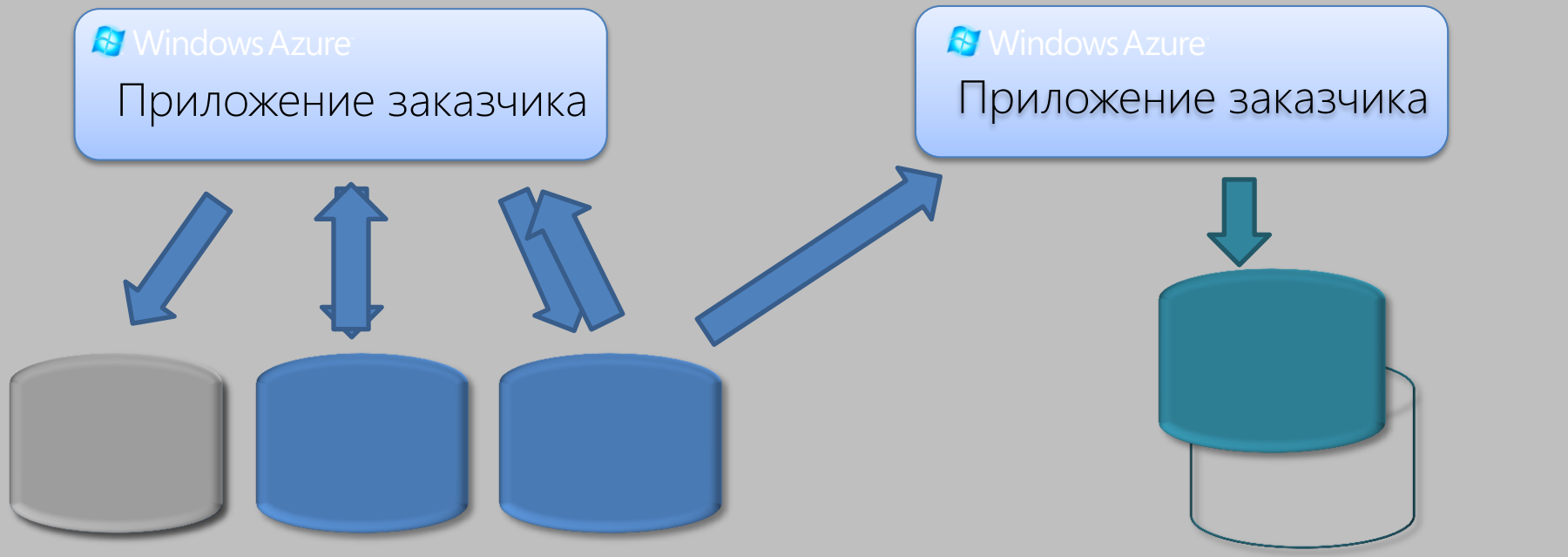
Microsoft SQL Azure

- Только SQL аутентификация
- Авторизация на основе пользователей и ролей в БД
- Добавлены роли loginmanager и dbmanager в Master DB для эмулирования серверных ролей
- Доступ посредством TDS + SSL по порту TCP 1433
- Встроенный МСЭ SQL Azure
- Остутствует встроенное шифрование (сейчас)



Доступность данных в Windows Azure Storage

Надежность за счёт избыточности (и локального резервирования)



Физические хранилища Azure

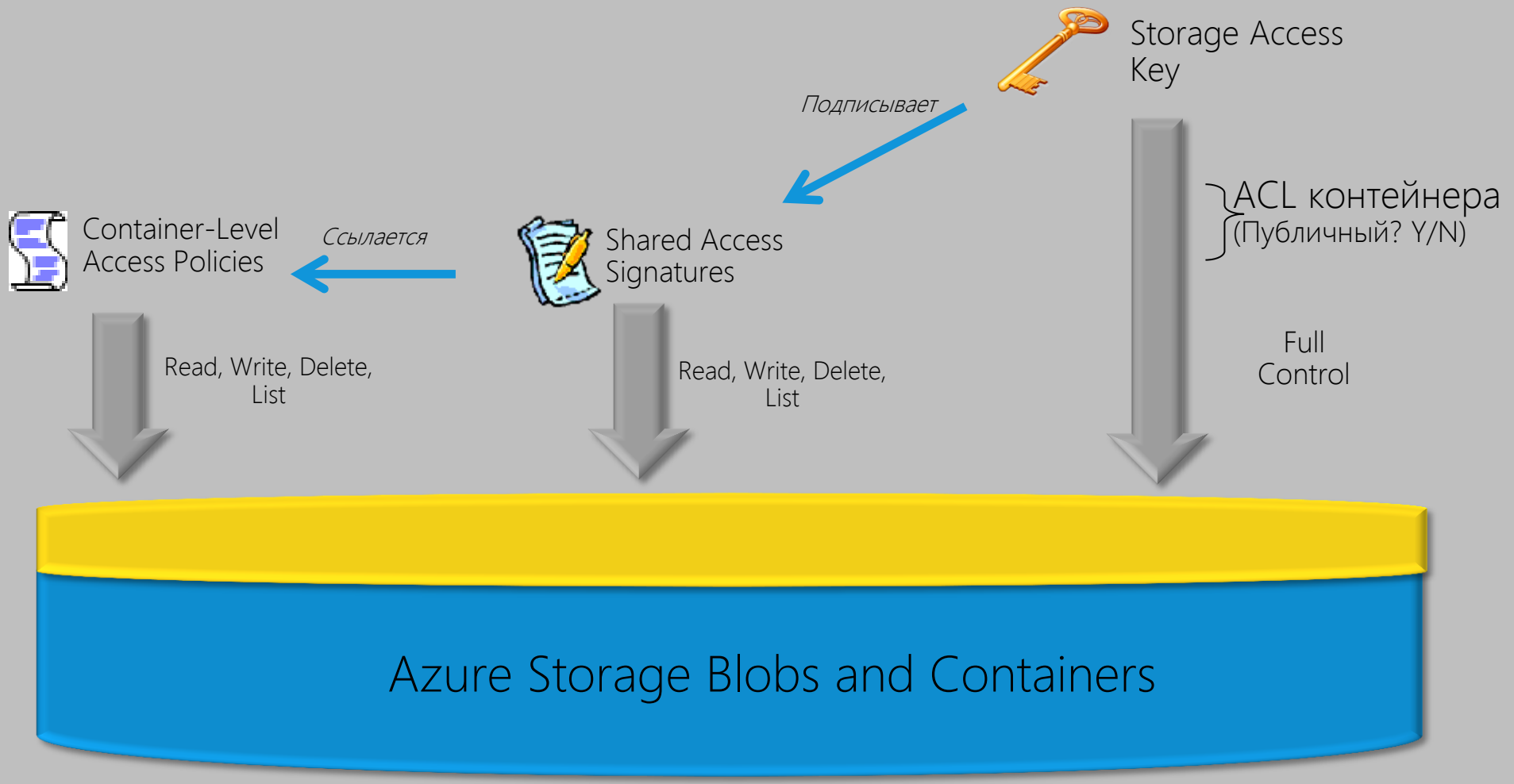
Для обеспечения высокой доступности данные в Windows Azure Storage Service реплицируются в три различных хранилища

Хранилище у заказчика

Заказчик всегда может создать приложения для локального резервирования данных

Безопасность Windows Azure Storage

Контроль доступа



Данные пользователей хранятся отдельно и организованы в контейнеры со строгим контролем доступа на основе секретных ключей (2 для плавного ключевого перехода)

Защита данных в Windows Azure

Шифрование в Windows Azure

- Данные при передаче защищены TLS
  - Как для Azure Storage Services, так и для SQL Azure
- Шифрования данных при хранении в Windows Azure с помощью Trust Services
  - Другая модель защиты секретного ключа для облачного сервиса
  - Доступны модули .Net Crypto и управления сертификатами
- Если необходимо обрабатывать конфиденциальные данные, то перед передачей данные должны шифроваться локально в доверенной среде
  - Возможно разбивая на части персональные данные, например медицинские (как сделано в Microsoft HealthVault)

Безопасность Windows Azure

Многоуровневая защита

Уровень	Защита
Данных	▪ Ключи контроля доступа к данным ▪ Защита траффика с помощью SSL
Приложений	▪ Код .Net исполняется с ограниченным доверием ▪ Учётные записи Windows с минимальными привилегиями
Хоста	▪ Защищенный образ Windows Server 2008 R2 ▪ Границы хоста защищены внешним гипервизором
Сетевой	▪ МЭ хоста ограничивает доступ к вирт. машинам ▪ VLANы и пакетные фильтры в роутерах
Физический	▪ Физическая безопасность мирового класса ▪ Сертификации ISO 27001 и SAS 70 Type II процессов эксплуатации ЦОД

Ресурсы

- http://blogs.msdn.com/b/windowsazure/
- http://www.microsoft.com/windowsazure/Whitepapers/securityoverview/
- http://www.globalfoundationservices.com/security/
- http://blogs.technet.com/securityrus

Спасибо за внимание!

Thank you!

Бешков Андрей
Руководитель программы информационной безопасности
E-mail: abeshkov@microsoft.com
Twitter: @abeshkov