



Уральский Центр Систем Безопасности

Технологии защиты бизнеса.

Аудит. Проектирование.

Внедрение. Сопровождение.

Безопасная дорога в облака

Главный инженер департамента системной интеграции ООО «УЦСБ»
Николай Домуховский



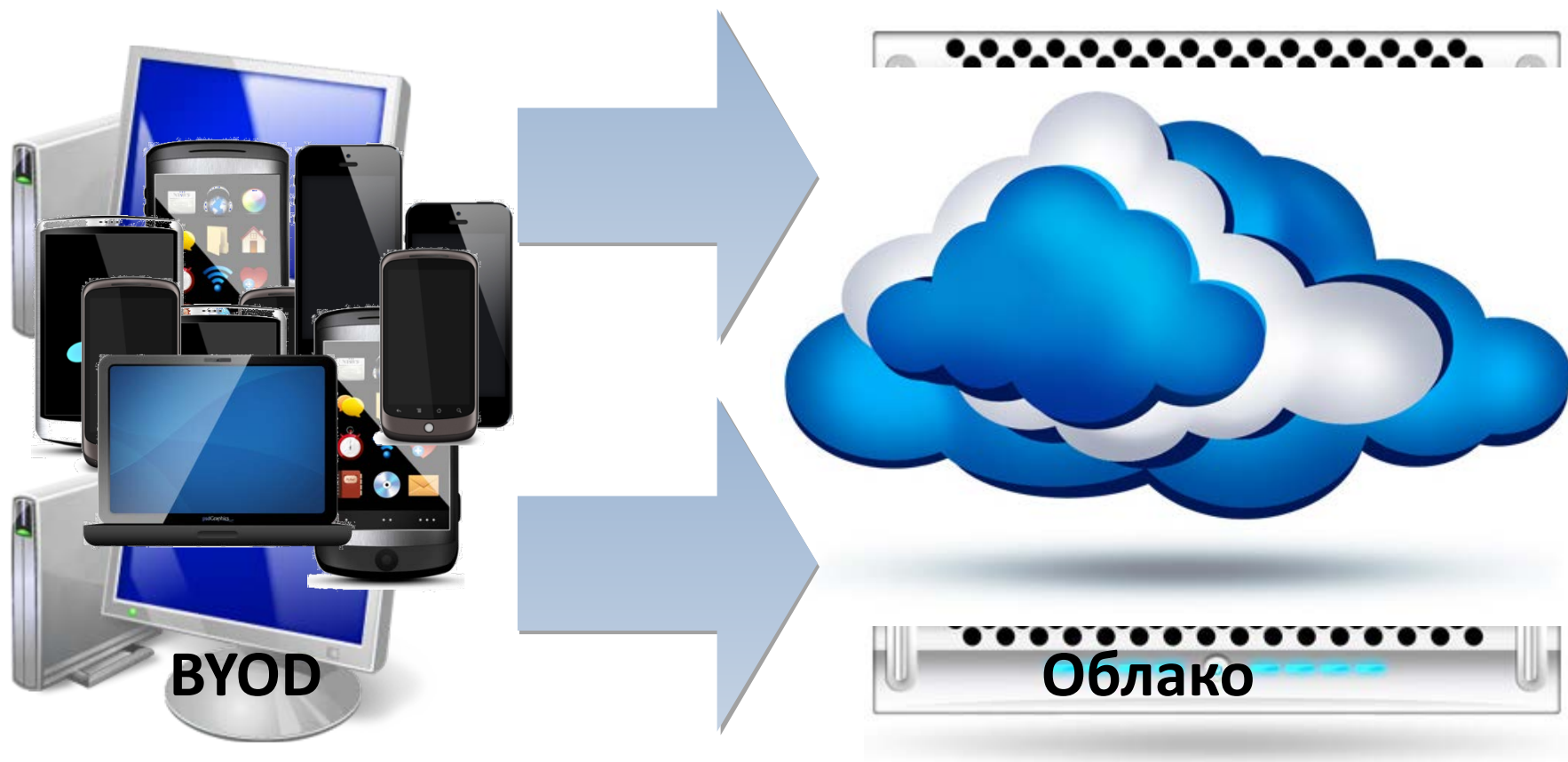
Уральский Центр Систем Безопасности

Технологии защиты бизнеса.

Аудит. Проектирование.

Внедрение. Сопровождение.

Какие две темы звучат сегодня весь день?





А почему еще не все в облаке?

33%

Цена

31%

**Интеграция
с унаследованными
системами**

30%

**Риски утечки
данных**

30%

**Потеря
контроля**

26%

**Потеря управляемости
мощностями и
затратами**

26%

**Проблемы
интеграции
облачных
платформ**

26%

**Вопросы ИБ
(в целом)**

21%

**Риск кражи
интеллектуальной
собственности**

18%

**Требования
регуляторов**

18%

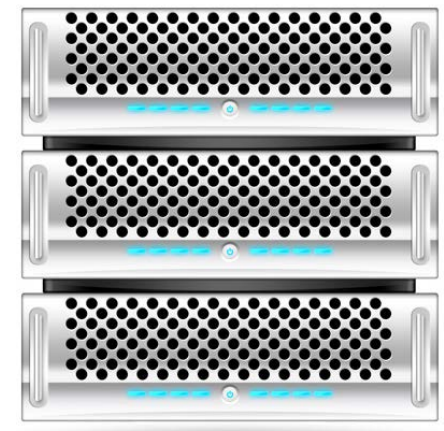
**Отсутствие прозрачности и
контроля над операциями с данными**

*Источник: KPMG International's Global cloud survey:
the implementation challenge*



А что в банках?

- Облако:
 - Инфраструктурные сервисы
 - Электронные коммуникации
 - Информационные системы
- Традиционная инфраструктура:
 - процессинг
 - АБС
 - Скоринговые системы
 - Специализированные сервисы



Облако. Новые решения – новые проблемы

- Изоляция виртуализованных приложений
- Разделение полномочий
- Новые каналы утечки информации





Рекомендации по безопасному использованию облака (PCI Security Standards Council)

Требование	Рекомендации
Требование 3. Обеспечить безопасное хранение данных о держателе карт	• Использовать шифрование виртуальных дисков • Хранить ключи шифрования за пределами гипервизора
Требование 7. Ограничить доступ к данным о держателях карт в соответствии со служебной необходимостью	Использовать специализированные инструменты, которые позволят разграничить доступ к виртуальным машинам, виртуальным устройствам и т.п.



Уральский Центр Систем Безопасности

Технологии защиты бизнеса.

Аудит. Проектирование.

Внедрение. Сопровождение.

Схема решения защищенной платформы виртуализации





SafeNet ProtectV – безопасность виртуальных сред

Основные возможности ProtectV:

- Централизованное управление доступом, регистрация и учет доступа к защищаемым данным
- Защищенное хранение и управление жизненным циклом криптографических ключей
- Прозрачное шифрование виртуальных жестких дисков



Компоненты решения

- **ProtectV client** – компонент виртуальной машины, обеспечивает прозрачное шифрование и доверенную загрузку
- **Protect V manager** – централизованное управление доступом к защищенным виртуальным машинам
- **KeySecure/DataSecure** – централизованное защищенное хранение и управление жизненным циклом криптографических ключей



Преимущества решения

- Доверенная загрузка
- Шифрование компонентов виртуальных машин: системный раздел, «мгновенные снимки» и резервные копии, раздел данных
- Возможность реализации разделения полномочий (в том числе разделение секрета на несколько частей)
- **Соответствие рекомендациям PCI Security Council в части защиты данных платежных систем при использовании средств виртуализации**



BYOD – ближайшие перспективы

- 2015 г. – соотношение разработки приложений для ПК и мобильных устройств достигнет 1:4
- 2016 г. – более половины корпоративных пользователей электронной почты будут использовать web-интерфейсы, мобильные устройства или планшетные компьютеры

Источник: «Gartner's Top Predictions for IT organizations and Users, 2012 and Beyond: Control Slips Away», Gartner.com

BOYD - ВЫЗОВЫ

- Аутентификация
- Построение профилей устройств
- Распространение параметров безопасности

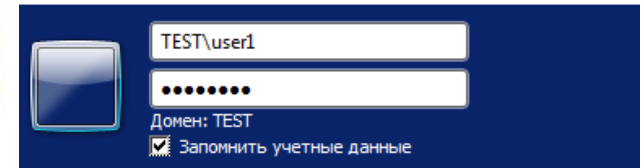
Источник: Strategic Road Map for Network Access Control. Gartner Inc.





Развитие методов аутентификации

- Парольная аутентификация:
 - Низкая надежность
 - Дороговизна эксплуатации
- Усиленная аутентификация
 - Необходимо отчуждаемое защищенное ключевое хранилище
 - А у мобильных устройств как правило нет интерфейсных портов
- Одноразовые пароли
 - Сложность интеграции с конечными сервисами
 - Обязательный OOB канал





Уральский Центр Систем Безопасности

Технологии защиты бизнеса.

Аудит. Проектирование.

Внедрение. Сопровождение.

Схема решения по доступу с помощью одноразовых ключей





SafeNet Authentication Services. Компоненты решения

- **Сервер SAS** – центральная часть системы, обеспечивающая взаимодействие с корпоративными сервисами и управление жизненным циклом токенов
- **Агент SAS** – специализированный программный модуль, обеспечивающий взаимодействие с поддерживаемым корпоративным сервисом
- **Токен** – генератор одноразовых ключей (приложение для смартфона, SMS шлюз, аппаратные генераторы OTP и др.)



SafeNet Authentication Services. Преимущества решения

- Развитые средства интеграции с приложениями:
 - Стандартные протоколы (RADIUS, SAML)
 - Специализированные агенты (IIS, Citrix Web Interface, Cisco, Juniper и др.)
 - SDK для подключение произвольных приложений
- Две редакции:
 - Service Provider Cloud Service (облако SafeNet)
 - Enterprise Cloud Service (частное облако заказчика)



Уральский Центр Систем Безопасности

Технологии защиты бизнеса.

Аудит. Проектирование.

Внедрение. Сопровождение.

Безопасная дорога в облака

Спасибо за внимание!

**Все упомянутые в презентации продукты доступны
для ознакомления на стенде**

ООО «УЦСБ»

Николай Домуховский

Главный инженер департамента системной интеграции
ООО «УЦСБ»

620026, Екатеринбург, ул. Красноармейская, д.78Б, оф.902

Тел.: +7 (343) 379-98-34

Факс: +7 (343) 264-19-53

info@ussc.ru

www.USSC.ru