s·terra
c s p

Информационная защита облачных сервисов

Руслан Нигматулин

Доклад на V Межбанковской конференции
«УРАЛЬСКИЙ ФОРУМ: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ»

13 февраля 2012 года

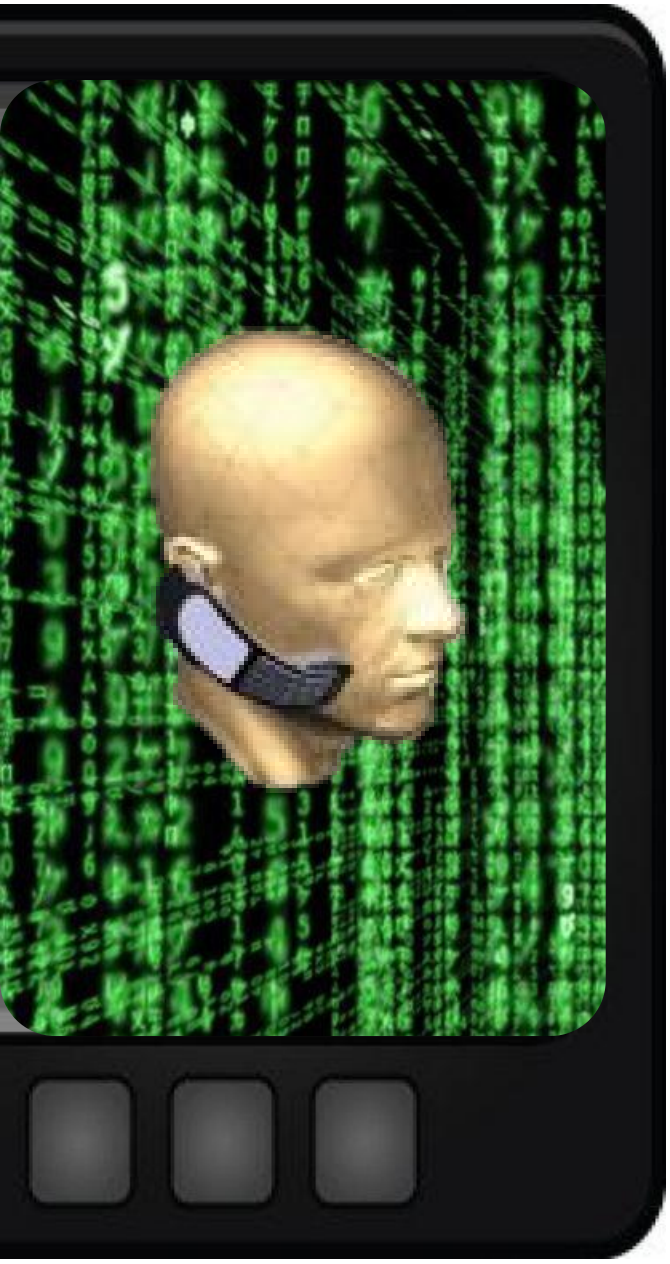
Что угрожает сервисам?
Виртуализация и безопасность
Откуда доступ?

Что угрожает сервисам?

Множество облачных сервисов

Что угрожает облаку

Плюс новые атаки



Облачные технологии не во всём инновация. Сервис –ориентированным структурам как минимум 15 лет.

Но уровень развития всё-таки выше и новые компоненты в современных облаках присутствуют.

Вопрос структуры облаков сложен и неоднозначен.

Однако сегодня во многих случая речь идёт о применении в облачной структуре **виртуализованных ресурсов**.

Для доступа к сервисам – того, ради чего, по сути облака организуются, могут использоваться различные технологии. **Мобильный** доступ – один из основных вариантов.

Эти технологии стоят того, чтобы их рассмотреть отдельно с позиций информационной безопасности

- **защита в виртуальной среде**
- **защита мобильного доступа**

Что угрожает сервисам?
Виртуализация и безопасность
Откуда доступ?

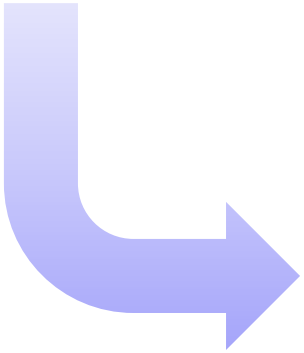
Виртуализация и безопасность

s-terra
csp
Cisco Solution Technology Integrator

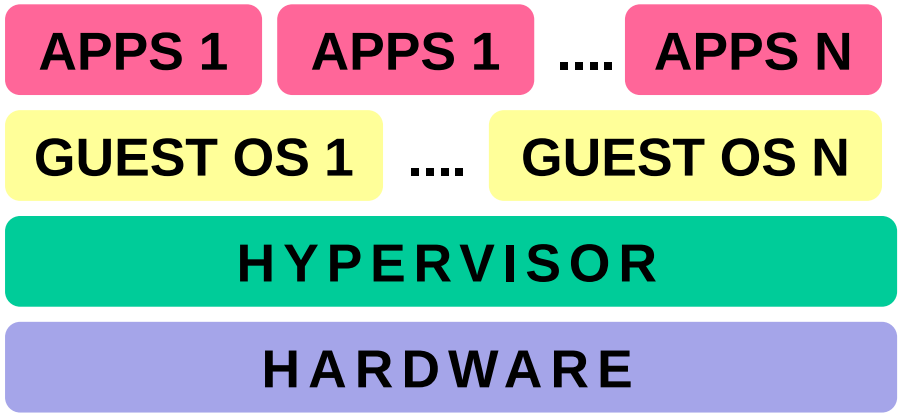
Технологии виртуализации не новы, но…

Application Virtualization

OS virtualization



FULL VIRTUALIZATION



Видов виртуализации много.

Но, с точки зрения безопасности всё-таки наиболее интересен крайний случай – **полная виртуализация**, когда ОС и все приложения полностью находятся в виртуальной среде.

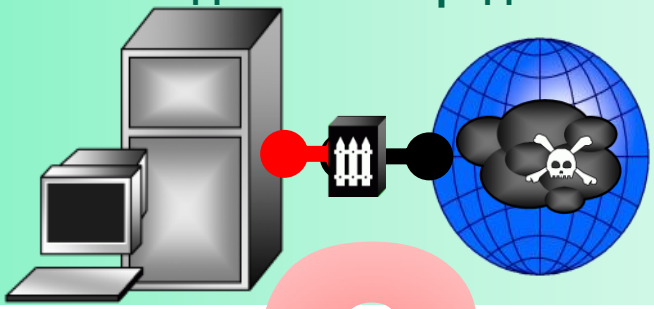
Гипервизор полностью контролирует обмен данными между гостевой ОС и железом.

При всей давности технологий виртуализации, пожалуй лишь недавно был достигнут тот потребительский уровень, когда продукт может использовать даже неквалифицированный пользователь.

Решение шагнуло в массы. Качество перешло в количество.

Прослойка или серьёзнее?

Классическое аппаратное решение – точки входа чётко определены



В виртуальной среде всё по другому

- **Полная виртуализация привносит некоторые негативные влияния на безопасность: дополнительные уровни технологий усложняют управление безопасностью.**
- **Виртуальная среда облегчает переход информации между приложениями, т. е, снижает изоляцию**
- **Высока динамичность виртуальной среды.**
- **Объединение множества приложений на одном физическом сервере – раньше воля сисадмина, в виртуализации – принцип работы.**

Изоляция гостевых ОС

APPS 1 | APPS 1 | .... | APPS N

GUEST OS 1 | .... | GUEST OS N

HYPERVISOR

HARDWARE

- Гипервизор распределяет ресурсы между ОС.
- Разделение может быть физическим или логическим.

- Полная изоляция теоретически достижима.
- На практике для удобства эксплуатации предоставляются инструменты доступа к хостовой ОС или другой гостевой ОС. Это может использоваться для атаки – переноса вредоносного ПО, атаки по сторонним каналам и др.
- Трафик между гостевыми ОС и хостовой ОС не проходит через стандартные узлы сетевой безопасности (МСЭ, IDS и др.) – остаётся полагаться на гипервизор.

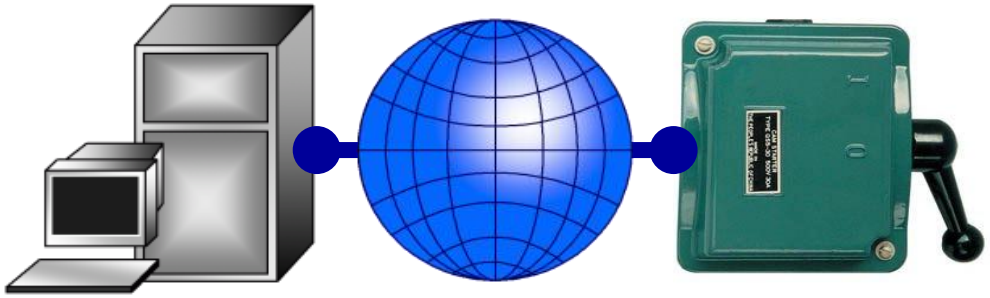
Администрирование образов

- Образ содержит секретные данные (пароли, ПДн и др.) также как и жёсткий диск.
- Сделать снимок файловой системы или образ и украсть гораздо проще, чем жёсткий диск.
- Снимок может содержать содержание RAM памяти, которая не хранится даже на жёстком диске.
- Возможны подмена образа ОС с содержимым в виртуальной среде; бесконтрольное размножение ВМ.

- **Управление образами – необходимая, важная и сложная дополнительная задача.**

Удалённое управление на аппаратном уровне

Включен или не включен?



Wake-on-LAN

PXE

Out-of-band management

- Технологии удалённого аппаратного управления – дополнительные риски в системах с виртуализацией.
- Современные возможности BIOS, а также переход с BIOSa на гибкие системы типа UEFI расширяют возможности управления сервером ещё до загрузки ОС
- Выключенный в обычном понимании сервер может таковым не являться.
- Стандартные технологии загрузки ОС по сети – возможность атаки.
- В итоге удобные инструменты удалённого управления одновременно являются дополнительными уязвимостями.

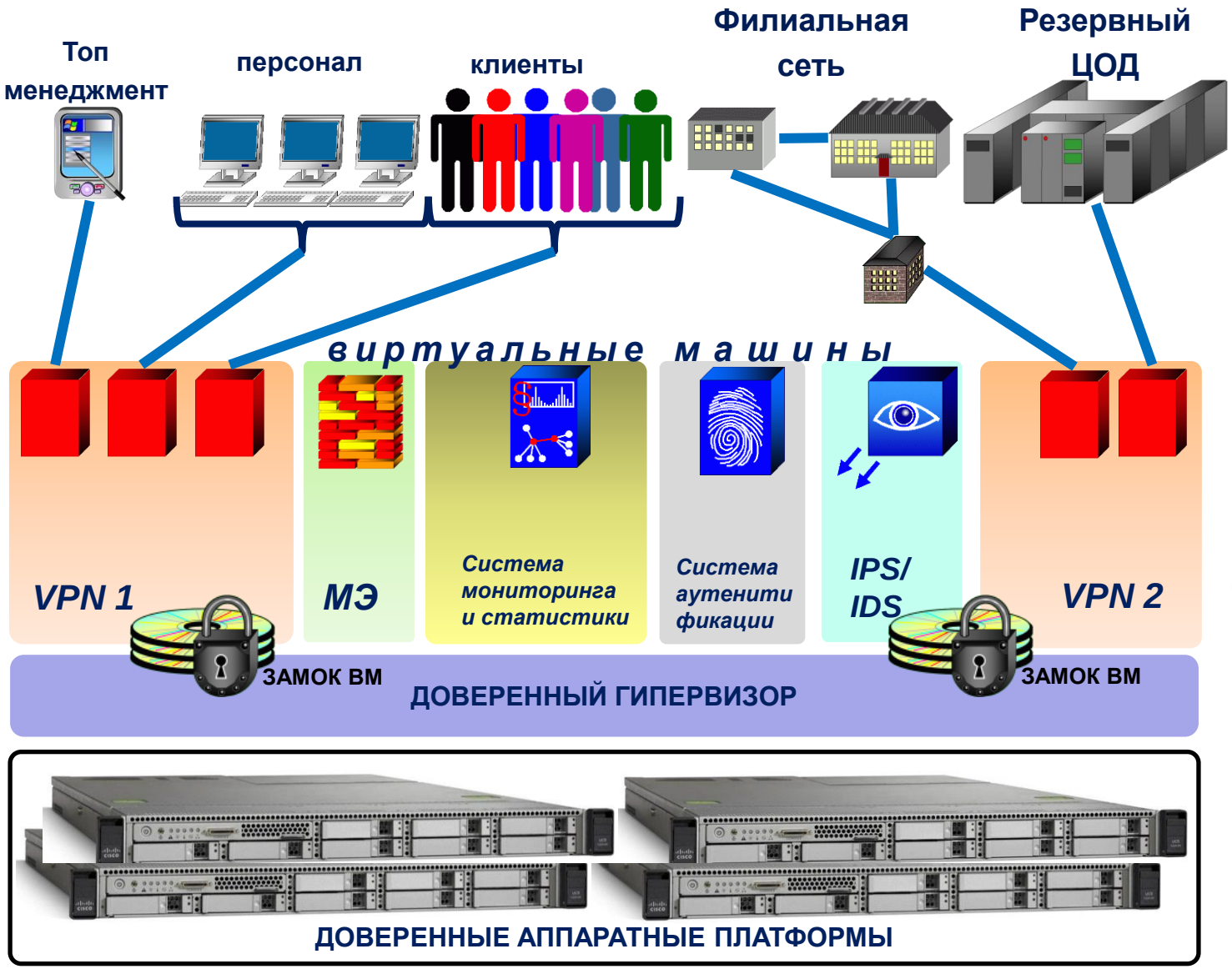
Тотальная виртуализация?

- **А как часто в облачной структуре нужны именно «виртуальные» средства защиты?**
- **Корпоративному порталу, ориентированному на внутренних пользователей, многие из свойств «виртуальности» не нужны или нужны в ограниченном объеме:**
  - замена аппаратных решений на виртуальные (где практика исследований и сертификация ?)
  - консолидация *разнородных* ресурсов (дешевле эксплуатация известных продуктов)
  - *эластичность* ресурсов (кто заплатит за избыток резервных ресурсов и дорогое, «облачное» управление ими?)

Размещение в облаке критичных объектов

- Усилия, чтобы обезопасить в публичном или кооперативном облаке критичные с точки зрения безопасности объекты, могут быть дорогими, сложными в эксплуатации и неэффективными.

Объекты ИБ в отдельном сегменте



Сегментирование, комбинирование объектов ИБ по группам может дать хороший выигрыш в эксплуатации, сведя к минимуму риски виртуализации.

Отчего защищаемся?
Виртуализация и безопасность
Откуда доступ?

Откуда доступ?

Необходимость мобильных решений

- Мобильные платформы (коммуникаторы, планшеты) на сегодня стали насущной потребностью и рабочим инструментом широких народных масс.
- Мобильные устройства используются практически всеми, востребованы и удобны.
- В то же время, ряд вопросов по поводу их безопасности и, отдельно, по поводу сертификации средств защиты для них, остается открытым.

Преимущества или недостатки?

- Мобильные устройства портативны; имеют скрытые высокоёмкие носители; имеют массу способов скрытого ввода информации, включая средства фото- и видеосъёмки; не имеют исчерпывающего набора средств контроля для периферии ввода/вывода
- имеют несколько коммуникационных каналов; часть из них зашифрована провайдером, часть – может быть шифрована пользователем; высока скорость перехода мобильных устройств из одной среды передачи в другую, не исключена возможность «гладкого» перехода от между режимами передачи во время одной сессии; всё это – классические каналы утечки данных
- пользователь в массе своей неспособен к контролю за безопасностью гаджета; malware может управлять устройством без его ведома
- отдельные образцы техники и даже отдельные прошивки одного и того же образца – часто очень различные по функциональности объекты

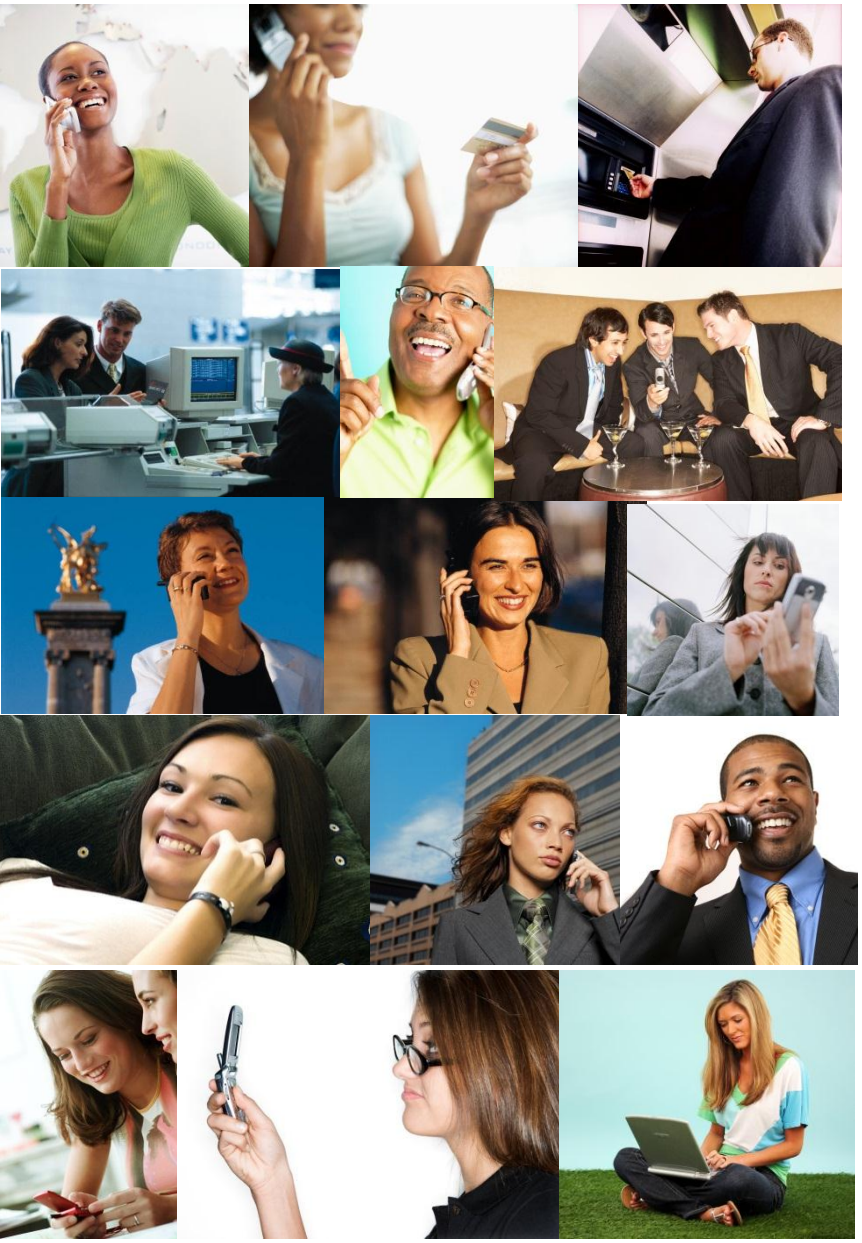
Принципиальное противоречие

Попытка выставить массовый продукт как специально защищённым не профессиональна, не безопасна и может привести к плачевным последствиям.

- **Мобильные платформы (планшетники, смартфоны) – продукт для массового потребления.**
- **Продукт, соответствующий требованиям регулятора – специализирован.**
- **Отсюда принципиальное противоречие:**

производителю мобильных устройств, делающему продукт для массового рынка по своей бизнес-модели, сложно реализовать безопасность в понимании спецтребований.

Кого защищаем?



- **Защитить всех и вся одним решением невозможно, это будет дорого и сложно в эксплуатации; необходимо чётко сегментировать пользователя.**
- **Применяемые решения разделяются по типовому пользователю – корпоративные сотрудники, клиенты банка (юр. лица, физ. лица: мелкие ИП и ООО или компании с миллиардным оборотом); и по типу информации: ДСП, ПДн и др.**
- **Применяемые решения могут быть различными.**

BYOD

- Надо ли исключать использование сотрудником его личного устройства для корпоративного доступа?
- BYOD – это корпоративная политика, предписывающая носителю гаджета ряд организационных и технических правил:

- требования к устройству – установить пароль, использовать антивирус и т. п.;

- требования к архитектуре доступа – корпоративное облако, выполняющее хранение и обработку данных только на серверах, на мобильном устройстве после сеанса могут стираться кэши и прочие временные данные.

- Достаточное большая сфера применения: образование, медицина, корпоративный уровень ДСП и др
- На рынке есть комплексные решения для BYOD (компания CISCO).

Когда BYOD недостаточно

Какие действия предпринимать, если требуется высокий уровень безопасности при мобильном доступе?

- **Использовать корпоративный гаджет**
- **Не разводить зоопарк, использовать строго ограниченный набор классов строго одинаковых в классе гаджетов**
- **Проводить работы по ограничению количества приложений на гаджете**
- **Усилить аутентификацию**
- **Применять файловое шифрование и защту канала связи; установить на все интерфейсы изолирующую политику сетевого доступа, разрешив доступ только к нужным ресурсам и только по шифрованному каналу.**
- **Наладить с производителем защиты взаимодействие для модернизации ПО и поддержки**
- **Использовать сертифицированные продукты**
- **Использовать MDM решения.**

Что мы имеем для предприятия

- Компания С-Терра предлагает сертифицированные VPN-продукты для мобильных бизнес-планшетов под управлением Windows
- BYOD решение для ОС Android
- Подготовленные к сертификации продукты защиты для наиболее популярных устройств (планшетов и смартфонов) под управлением ОС Android.
- Решения работают в едином комплексе со всеми продуктами компании С-Терра.

КОНТАКТЫ

e-mail: information@s-terra.com
web: http://www.s-terra.com/

Тел.: +7 (499) 940 9001
+7 (495) 726 9891
Факс: +7 (499) 720 6928

Вопросы?

Обращайтесь к нам!

s·terra
c s p
Cisco Solution Technology Integrator