ЭЛВИС-ПЛЮС

«Облака», виртуальная инфраструктура и безопасность информации

Начальник лаборатории
доверенной среды
ОАО «ЭЛВИС-ПЛЮС»
Олег Вернер

2012 год

ЭЛВИС-ПЛЮС

ОСНОВНЫЕ ПРОБЛЕМЫ ИБ В «ОБЛАКАХ»

При организации защиты «облачных» технологий возникают две взаимосвязанные группы проблем:

✓ **Нормативно-правовые**

- Нет нормативов и требований по защите и типовой модели угроз
- Нет концептуальных подходов к безопасности
- Нет правовой основы отношений провайдер/пользователь
- Не урегулированы отношения при трансграничности облачной среды

✓ **Технологические**

- Сужение возможности использования традиционных средств защиты
- Непрозрачность процедуры управления инфраструктурой для пользователя
- Проблема конфиденциальности и целостности удаленного доступа
- Обязательное наличие виртуализатора и проблема его целостности
- Проблема динамичности ВМ и наличия бездействующих клонов

Для решения этих проблем необходимо создание «доверенного облака»

ЭЛВИС-ПЛЮС

ТРИЕДИНАЯ ЗАДАЧА СОЗДАНИЯ «ДОВЕРЕННОГО ОБЛАКА»

Защиту «облаков» в общем случае логически можно представить в виде трех подсистем:

- Подсистема безопасности пользовательской (виртуальной) ИС
- Подсистема безопасности провайдера (серверы, БД, ПО, виртуализатор)
- Подсистема обеспечения доверия пользователя к провайдеру

Актуальна задача построения технологической составляющей системы безопасности, поднимающей доверие пользователя к провайдеру выше, чем это обеспечивается простым заключением Соглашения об обеспечиваемом уровнем услуг

ЭЛВИС-ПЛЮС

КЛЮЧЕВАЯ ПРОБЛЕМА ОБЛАЧНЫХ ТЕХНОЛОГИЙ

ДОВЕРИЕ ПОЛЬЗОВАТЕЛЯ К ПРОВАЙДЕРУ
должно обеспечиваться как юридическими, так и техническими методами:

- Созданием правовой основы отношений провайдер/пользователь
- Заключением Соглашения об обеспечиваемом уровне услуг
- Прозрачностью действий провайдера для пользователя
- Возможностью удаленной аттестации платформы провайдера
- Страхованием рисков при обработке по облачным технологиям

Одной из ключевых проблем «облаков» является вопрос доверия пользователя провайдеру.

ЭЛВИС-ПЛЮС

СЕГРЕГАЦИЯ ДАННЫХ ПОЛЬЗОВАТЕЛЯ В «ОБЛАКЕ»

Сегрегацию критичной для пользователя информации при использовании облачной инфраструктуры возможно достичь построением комплекса связанных друг с другом систем:

- Доверенного контроля целостности виртуальной среды
- Контролируемого пользователем прозрачного шифрования виртуальных дисков критичных серверов
- Контролируемого пользователем шифрования виртуальных сетевых взаимодействий (VPN)

Первым шагом для построения такого комплекса должна стать проверка ПО, используемого для создания виртуальной инфраструктуры, на отсутствие НДВ

ЭЛВИС-ПЛЮС

КОНТРОЛЬ ЦЕЛОСТНОСТИ ВИРТУАЛЬНОЙ СРЕДЫ

Система доверенного контроля целостности виртуальной среды должна обеспечивать доверенную загрузку виртуальной среды и контроль целостности виртуализатора.

И только в случае положительных результатов такой проверки, ключи аутентификации физического сервера могут быть доступными.

Ядром такой системы является независимый аппаратно-программный компонент, хранящий критичную информацию (ключи, контрольные суммы) в защищенном виде и обеспечивающий доступ к результатам контроля только по защищенному каналу.

Такая система существенно облегчает решение задачи снижения и других специфических для облачных технологий рисков.

ЭЛВИС-ПЛЮС

ШИФРОВАНИЕ ВИРТУАЛЬНЫХ ДИСКОВ

Система контролируемого пользователем шифрования виртуальных дисков критичных серверов должна обеспечивать шифровать данные на диске пользовательской виртуальной машины как в выключенном, так и в работающем состоянии прозрачным образом.

При этом доступ к ключу шифрования контролирует пользователь виртуальной машины, который и принимает решение о предоставлении доступа к нему на основании строгой аутентификации аппаратно-программной платформы физического сервера и результатов контроля целостности виртуализатора.

Процедура работы с ключами может происходить как в «ручном» так и в автоматическом режиме.

Такая система решает также проблему конфиденциальности при восстановлении данных (резервировании).

ЭЛВИС-ПЛЮС

ШИФРОВАНИЕ ВИРТУАЛЬНЫХ ВЗАИМОДЕЙСТВИЙ

Система контролируемого пользователем шифрования виртуальных сетевых взаимодействий (VPN) может быть развернута на базе любой системы защиты сетевых взаимодействий (IPsec, SSL).

Для сегрегации передаваемых данных и защиты сетевых взаимодействий от администраторов облачной инфраструктуры создается выделенная защищенная подсеть, построенная по схеме «точка-точка». Применима также «вложенная» архитектура.

Управление доступом к ключам пользователя осуществляется в этом случае аналогично системе шифрования виртуальных дисков.

Такая система также позволяет изолировать критичные данные пользователя и от администраторов облачной инфраструктуры.

ЭЛВИС-ПЛЮС

«ДОВЕРЕННОЕ ОБЛАКО»

Для решения проблемы повышения доверия пользователя к провайдеру облачных сервисов, самому пользователю необходимо:

- заключить с провайдером Соглашение об обеспечиваемом уровне услуг, оговорить все нюансы обработки информации
- получить подтверждение того, что ПО облачной инфраструктуры не имеет НДВ
- убедиться, что ПО провайдера позволяет изолировать информацию
- убедиться, что ПО исключает доступ к оперативной памяти администратора
- установить на ВМ приложение для шифрования данных на диске ВМ
- обеспечить контроль доступа к ключу шифрования
- установить приложение для создания VPN-соединение по схеме «точка-точка»

ЭЛВИС-ПЛЮС

«ДОВЕРЕННОЕ ОБЛАКО»

Для решения проблемы повышения доверия пользователя к провайдеру облачных сервисов, провайдеру необходимо:

- развернуть прозрачную для пользователя ПБ ВИ
- предоставить механизмы для построения эффективной ПБ пользовательской ИС
- заключить с пользователем Соглашение об обеспечиваемом уровне услуг, оговорить все нюансы обработки информации

Построение ПБ ВИ и эффективное применение СЗИ для виртуализованных ИС является актуальной задачей не только для владельца публичного или частного «облака», но для любой организации, использующей технологии виртуализации.

ЭЛВИС-ПЛЮС

ЗАЩИТА ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

Основные группы угроз ИБ при применении технологии виртуализации

- Угрозы процессам аутентификации:
  - средств виртуализации;
  - администраторов управления средствами виртуализации;
  - терминальных устройств виртуальной инфраструктуры;
- Угрозы НСД к средствам виртуализации;
- Угрозы атаки на ВМ со стороны других ВМ;
- Угрозы создания несанкционированных потоков информации:
  - между гостевыми ВМ;
  - по периметру ВИ;
- Угрозы атаки на каналы передачи данных внутри виртуальной среды;
- Угрозы атаки на процесс загрузки ПО серверов виртуализации;

ЭЛВИС-ПЛЮС

ЗАЩИТА ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

Основные группы угроз ИБ при применении технологии виртуализации

- ✓ Угрозы атаки на процесс загрузки ПО ВМ;
- ✓ Угрозы сокрытия событий, связанных с нарушением безопасности информации в виртуальной среде;
- ✓ Угрозы НСД путем нарушения целостности конфигураций элементов виртуальной инфраструктуры;
- ✓ Угрозы потери данных и ПО при реализации атаки вызывающей отказ в доступе к ВИ или уничтожение ее элементов;
- ✓ Угрозы потери данных/информации при сбое или отказе технических средств

Помимо необходимости портирования в ВИ существующих механизмов защиты, появляется новая задача – изоляция пользовательских данных внутри ВМ или обеспечение доверия к платформе виртуализации.

ЭЛВИС-ПЛЮС

ДОВЕРЕННАЯ ПЛАТФОРМА ВИРТУАЛИЗАЦИИ

Комплекс задач по обеспечению доверия к виртуализатору:

- Обеспечение доверия к платформе виртуализации
  - экспертные оценки конкурентных предложений
  - сертификаты регуляторов
  - доверенный канал поставки
  - управление набором доверенных ресурсов (trusted pool)
- Аудит или контроль установки и конфигурирования виртуальной платформы
- Контроль целостности виртуализатора

ЭЛВИС-ПЛЮС

ОСНОВНЫЕ ПЛАТФОРМЫ ВИРТУАЛИЗАЦИИ

- С гипервизором (аппаратная виртуализация)
  - VMware View
  - Microsoft Hyper-V
  - Citrix XenDesktop
  - Parallels Server Bare Metal
- Контейнерного типа (виртуализация уровня ОС)
  - Parallels Viruozzo (OpenVZ)
  - FreeBSD Jail
  - VDSManager

vmware

Windows Hyper-V

CITRIX

Parallels

FreeBSD

VDS manager

ЭЛВИС-ПЛЮС

ОБЕСПЕЧЕНИЕ ДОВЕРИЯ К ВИРТУАЛИЗАТОРУ

С точки зрения ИБ виртуальная инфраструктура это:

- СЗИ, реализующее определенные функции безопасности
- Среда, в которой функционируют наложенные СЗИ (виртуальные МЭ, Антивирусные системы и т.п.)

Функции безопасности виртуальной среды:

- разграничение доступа к информации пользователей, обрабатывающейся в ВМ/контейнерах
- ФБ вытекающие из требований СЗИ к среде ИТ:
  - поддержание доменов безопасности для выполнения функция безопасности;
  - изоляция доменов

В случае, когда часть ФБ выполняется системой виртуализации, **необходима сертификация**

ЭЛВИС-ПЛЮС

СЕРТИФИКАЦИЯ ПЛАТФОРМ ВИРТУАЛИЗАЦИИ

VMware vSphere

- **ПК VMware vSphere 4** (ESX 4.0 Update 1, VMware vCenter Server 4.0 Update) - СВТ 5 (АС 1Г и ИСПДн К2);
- НДВ нет

Microsoft Hyper-V

- **Windows Server 2008 R2** – сертификация на НДВ завершена, продолжается экспертиза результатов, ожидается получение сертификата на класс К1;
- **Windows Server 2012** - планируется сертификация во ФСТЭК;

Parallels Virtuozzo

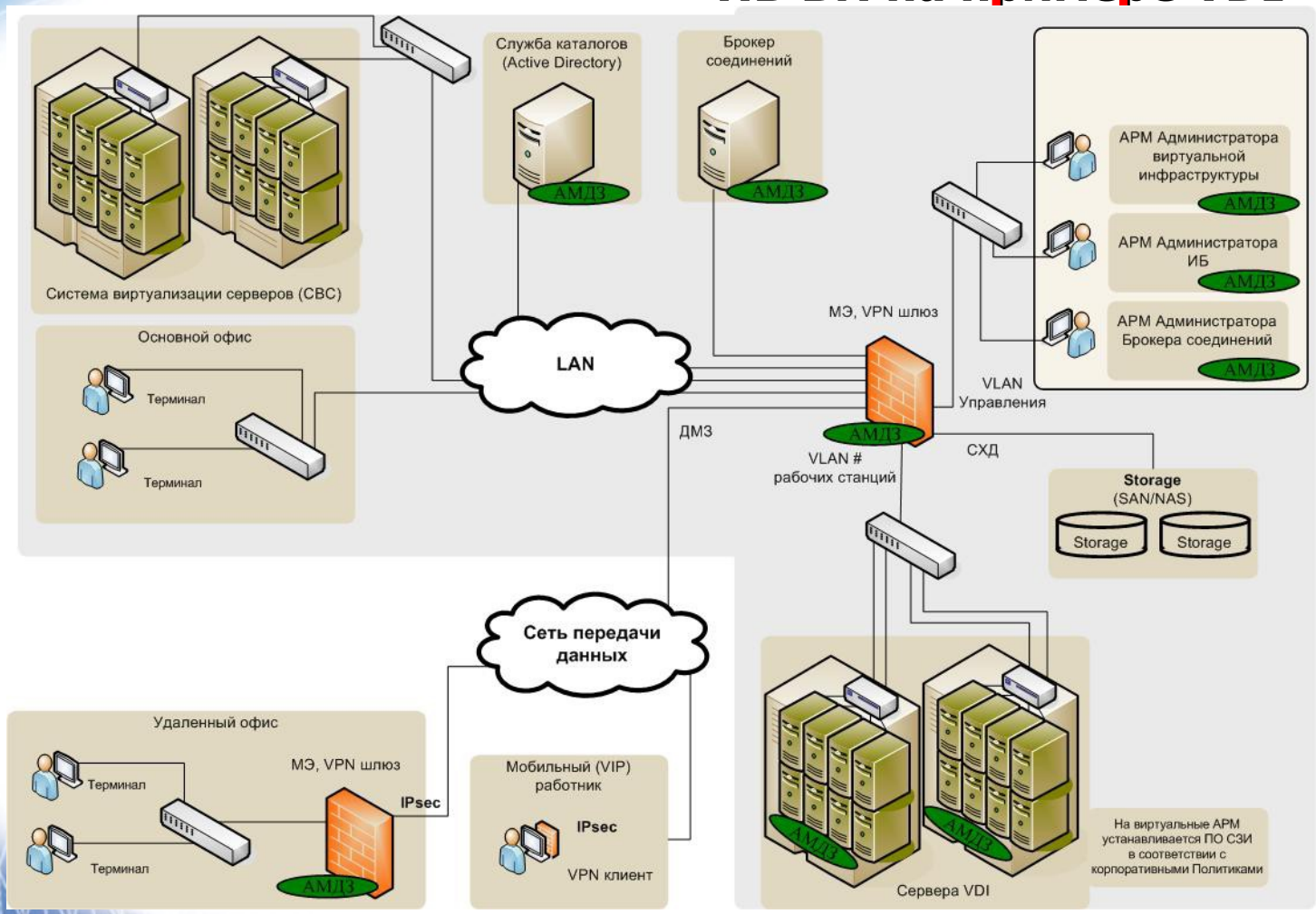
- **PVCfW** – ведутся работы по сертификации во ФСТЭК – НДВ 4, (АС 1Г и ИСПДн К1);
- **ПК Parallels VDI** (с наложенными СЗИ) - ведутся работы по сертификации во ФСТЭК – ОУД2, НДВ 4, (АС 1Г и ИСПДн К1);

Citrix XenDesktop

- Нет данных

ЭЛВИС-ПЛЮС

ПБ ВИ на примере VDI



ЭЛВИС-ПЛЮС

Функции безопасности	VMware View (vSphere)	Hyper-V	Citrix XenDesktop	Parallels Virtuozzo
Аутентификация средств виртуализации, администраторов управления средствами виртуализации и аутентификация терминальных устройств виртуальной инфраструктуры	vGate R2, ПАК «Соболь»; Аккорд-В StoneGate Firewall/VPN; TrustAccess; ПК ЗАСТАВА	Встроенные средства StoneGate Firewall/VPN; TrustAccess; ПК ЗАСТАВА	Встроенные средства StoneGate Firewall/VPN; TrustAccess; ПК ЗАСТАВА	Встроенные средства, Аккорд StoneGate Firewall/VPN; TrustAccess; ПК ЗАСТАВА
Управление доступом к средствам виртуализации	vGate R2 (отдельный сегмент сети управления ВИ), Аккорд-В	Встроенные средства, отдельный сегмент сети управления ВИ, ПАК «Соболь», ПАК Аккорд	Встроенные средства, отдельный сегмент сети управления ВИ	Встроенные средства, отдельный сегмент сети управления ВИ, ПАК «Соболь», ПАК Аккорд
Разграничение доступа к данным, обрабатываемым в виртуальных машинах/контейнерах, или изоляция виртуальных машин/контейнеров	Организационные меры, *Сертификат на НДВ отсутствует*	*Ожидается сертификация Windows Server 2012, в том числе – на отсутствие НДВ*	Нет данных	*В процессе сертификации виртуализатора, в том числе по ФБ «изоляция»*

ЭЛВИС-ПЛЮС

Функции безопасности	VMware View (vSphere)	Hyper-V	Citrix XenDesktop	Parallels Virtuozzo
Управление потоками информации между гостевыми машинами/контейнерами и по периметру виртуальной инфраструктуры	StoneGate SSL VPN Virtual Appliance, TrustAccess, ПК ЗАСТАВА	StoneGate SSL VPN Virtual Appliance, MS ISA Server MS Forefront Threat Management Gateway (TMG) 2010 ПК ЗАСТАВА	ЗАСТАВА, MS ISA Server MS Forefront Threat Management Gateway (TMG) 2010,ПАК Дионис (НПП Фактор-ТС)	ЗАСТАВА, MS ISA Server MS Forefront Threat Management Gateway (TMG) 2010,ПАК Дионис (НПП Фактор-ТС)
Защита каналов передачи данных внутри виртуальной среды	StoneGate SSL VPN Virtual Appliance; ПК «ЗАСТАВА»	StoneGate SSL VPN Virtual Appliance; MS Windows + КриптоПро IPsec; ПК ЗАСТАВА	StoneGate Firewall/VPN; MS Windows + КриптоПро IPsec; ПК ЗАСТАВА	ПК ЗАСТАВА
Доверенная загрузка серверов виртуализации	ЭЗ «Соболь»; Аккорд-АМДЗ	ЭЗ «Соболь», Аккорд-АМДЗ	Нет данных	ЭЗ «Соболь», Аккорд-АМДЗ
Доверенная загрузка виртуальных машин/контейнеров	vGate R2; Аккорд-В	Встроенные средства, ПО ПАК Аккорд	Нет данных	ПО ПАК Аккорд

ЭЛВИС-ПЛЮС

Функции безопасности	VMware View (vSphere)	Hyper-V	Citrix XenDesktop	Parallels Virtuozzo
Регистрация и анализ событийбезопасности в виртуальной среде,	vGate R2; vCenter Server, IgniteVM от Confio Software	Встроенные средства, vCenter Server	Встроенные средства (редакция Platinum)	Встроенные средства
Контроль целостности конфигураций элементов виртуальной инфраструктуры	vGate R2; ПАК Аккорд-В	Встроенные средства, ПАК «Соболь», Аккорд, Secure Pack Rus (Крипто-Про)	Встроенные средства, ПАК «Соболь», Аккорд, Secure Pack Rus (Крипто-Про)	Встроенные средства, ПАК «Соболь», Аккорд, Secure Pack Rus (Крипто-Про)
Резервное копирование данных, резервирование технических средств и ПО	CommVault; EMC Avamar; Quest Software vRanger; Symantec Backup;	CommVault; Symantec Backup	CommVault; Symantec Backup	CommVault; Symantec Backup
Распределенное хранение данных и восстановление информации после сбоев	CommVault; EMC Avamar; Quest Software vRanger; Symantec System Recovery	CommVault; Symantec System Recovery	CommVault Symantec System Recovery	CommVault Symantec System Recovery

ЭЛВИС-ПЛЮС

СЕРТИФИКАТЫ СЗИ ВИ

StoneGate Firewall/VPN: МЭ2, НДВ4 (АС 1Г и ИСПДн К1)
StoneGate SSL VPN Virtual Appliance: МЭ2, НДВ4 (АС 1Г и ИСПДн К1)
TrustAccess: МЭ2, НДВ4 (АС 1Г и ИСПДн К1)
ПАК Дионис (НПП Фактор-ТС): МЭ2, НДВ2 (АС 1Б и ИСПДн К1)
ЗАСТАВА: МЭ2, НДВ4 (АС 1Г и ИСПДн К1)
MS ISA Server 2006: МЭ4/3(с ограничениями) АС 1Г

«Аккорд-В.»: СВТ5, НДВ4 (АС 1Г и ИСПДн К1)
vGate R2: СВТ5, НДВ4 (АС 1Г и ИСПДн К1)

Microsoft

КРИПТО ПРО

Код Безопасности
ГК «Информзащита»

АПР ОКБ

STONESOFT

ФАКТОР

ЭЛВИС-ПЛЮС

ЭЛВИС-ПЛЮС

ПРОЧИЕ ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИБ ВИ

- **Безопасность ключевой информации**
- **Мониторинг**
- **Отказоустойчивость**
- **Прочие наложенные СЗИ** *(согласно концепции СОИБ и политикам ИБ)*
  - Подсистема защиты СХД (SAN/NAS)
  - Антивирусные системы
  - Система обнаружения вторжений (IDS)
  - Защита сетевого трафика / каналов связи
  - Обеспечение безопасности активов службы каталогов
  - Предотвращение утечек конфиденциальной информации (DLP)

ЭЛВИС-ПЛЮС

ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННОЙ ВИ

Этапы

- Разработка требований к ВИ (в том числе – СЗИ)
- Разработка Эскизного проекта
- Разработка Макета, утверждение решения
- Развертывание тестового сегмента / Тестовая эксплуатация
- Доработка по результатам ТЭ
- Разработка Типового проекта (Системный проект)
- Развертывание сегментов ВИ
- Опытная эксплуатация
- Приемо-сдаточные испытания

ЭЛВИС-ПЛЮС

Спасибо за внимание !

124498, МОСКВА, Зеленоград,
проезд 4806, д. 5, стр. 23
тел. (495) 276-0211,
факс (499) 731-2403
info@elvis.ru
www.elvis.ru