



Код безопасности



конференция
РусКрипто

Технологии виртуализации и информационная безопасность

Денис Полянский
ООО «Код Безопасности»

**Все знают преимущества
виртуализации...
но не ее риски!**

Известные преимущества виртуализации

- ❏ Сокращение затрат на закупку и обслуживание физических серверов;
- ❏ Оптимизация использования вычислительных мощностей;
- ❏ Увеличение энергоэффективности;
- ❏ Обеспечение непрерывности работы за счет механизмов кластеризации и аварийного восстановления.



Российский рынок виртуализации 2014

Развивающийся

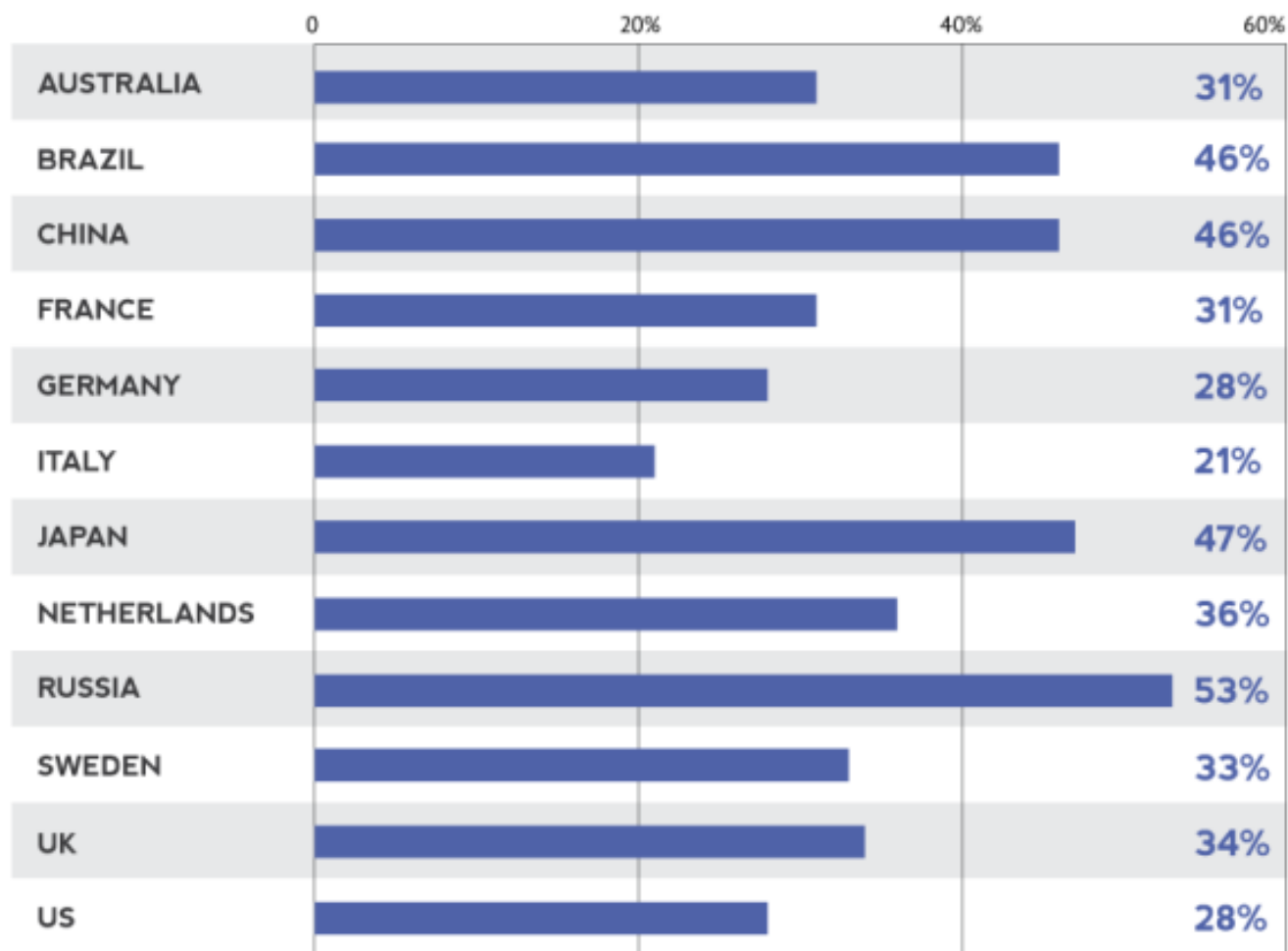


Развитой



Россия -лидер

▶ PERCENT OF ORGANIZATIONAL IT BUDGETS DEVOTED TO CLOUD IN EACH COUNTRY (INCLUDING SOFTWARE, SERVICES, STAFF, RESOURCES, TRAINING, ETC.):



Виртуализация – не только преимущества

46%

компаний остановили или замедлили внедрение виртуализации из-за вопросов безопасности*.



* - опрос Ponemon Institute

Виртуализация

Обычный компьютер



Управление виртуальной инфраструктурой

Сервер виртуализации



Традиционные угрозы

- Нарушение работы оборудования.
- Угрозы хостовой системе.
- Атаки\сетевые угрозы.
- Угрозы вредоносного ПО.



Традиционно-специфические угрозы

- Вредоносное ПО.
- Уязвимости платформы.



- **2012 г. MORCUT.**

Первый троян, заражающий шаблоны VM



Security Advisories & Certifications

Advisories

Certifications

Guides

Security Advisories are the official notification of security-related vulnerabilities and issues impacting VMware products. Security Advisories outline complete information on how to protect impacted systems. Each advisory contains a detailed description of the security vulnerability, affected systems, threat severity, risk mitigation techniques for fixing the vulnerability and securing the system. Third-party certifications such as Common Criteria and FIPS provide independent validation of the security of VMware products. These are listed along with links to the official certificate or report. Security Hardening Guides provide prescriptive guidance for customers on how to deploy VMware products in a secure manner and also provide script examples and other information to help with security automation.

August 29, 2013

VMSA-2013-0011

VMware ESXi and ESX address an NFC Protocol Unhandled Exception

August 22, 2013

VMSA-2013-0010

VMware Workstation host privilege escalation vulnerability

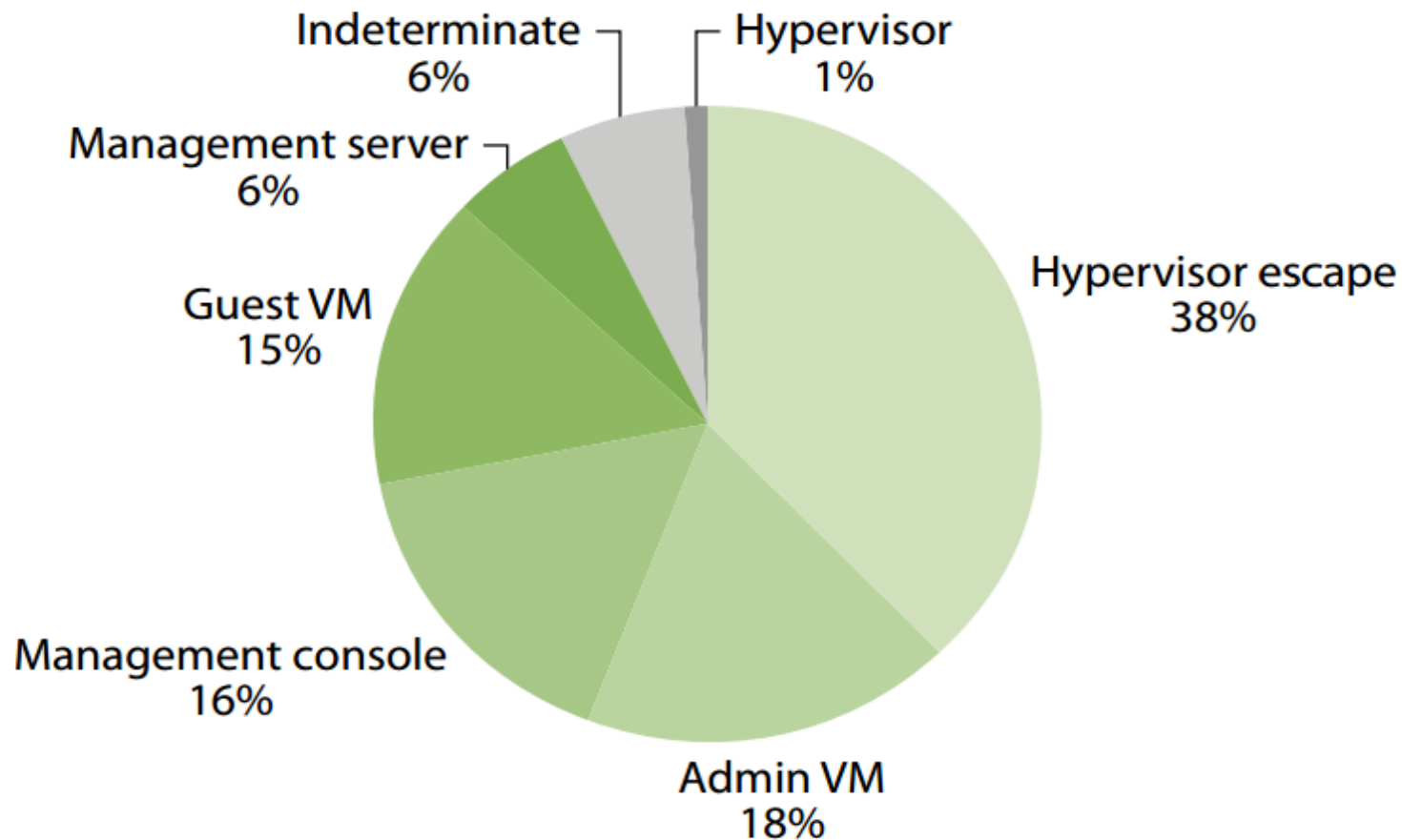
July 31, 2013

VMSA-2013-0009

VMware ESX and ESXi updates to third party libraries

Уязвимости платформы

Distribution of virtualization system vulnerabilities



* Forrester Research, Inc

Уязвимости платформы

Банк данных угроз безопасности информации



Федеральная служба по техническому и экспортному контролю
ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»



Угрозы **Уязвимости** Документы Обратная связь Новости сайта ФСТЭК России

Главная / Список уязвимостей

ФИЛЬТРАЦИЯ

Контекстный поиск по названию уязвимости

vmware|

Производитель ПО

Выберите производителя ПО

Тип ПО

Выберите тип ПО

Программное обеспечение

Выберите программное обеспечение

Аппаратная платформа

Выберите платформу

Версия ПО

Выберите версию ПО

Статус уязвимости

Выберите статус уязвимости

Доп. параметры

Диапазон дат

с по

Класс уязвимости

Выберите класс уязвимости

Уровень опасности

Выводить по: 10, 20, 50, 100

Элементы с 1 по 6 из 6

2015-00723	Уязвимость программного обеспечения VMware Workstation, позволяющая злоумышленнику нарушить доступность защищаемой информации VMware Inc. VMware Workstation от 9.0.0 до 9.0.1	17.01.2014
2015-00722	Уязвимость программного обеспечения VMware Player, позволяющая злоумышленнику нарушить доступность защищаемой информации VMware Inc. VMware Player от 5.0.0 до 5.0.1	17.01.2014
2014-00322	Уязвимость гипервизора VMware ESXi, позволяющая злоумышленнику повысить свои привилегии в гостевой операционной системе или вызвать отказ в обслуживании VMware Inc. VMware ESXi 5.5	31.05.2014
2014-00019	Уязвимость программного обеспечения управления виртуальной инфраструктурой VMware vCenter Server, позволяющая злоумышленнику препятствовать входу других пользователей в систему VMware Inc. VMware vCenter Server от 5.0 до 5.5 включительно	06.02.2013
2014-00006	Уязвимость гипервизора VMware ESXi, позволяющая злоумышленнику повысить привилегии или вызвать отказ в обслуживании VMware Inc. VMware ESXi 4.1	16.03.2012
2014-00005	Уязвимость гипервизора VMware Workstation, позволяющая злоумышленнику получить контроль над выполнением утилиты «vmgrip» VMware Inc. VMware Workstation 6.5	04.04.2011

[Скачать сведения об уязвимостях](#)

Угрозы

Уязвимости

Термины

Список каналов (RSS, Atom)

Инфографика

Калькулятор CVSS

НОВЫЕ УЯЗВИМОСТИ

25.02.2015

Уязвимость программного обеспечения Java™ Platform, позволяющая удаленному злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации

25.02.2015

Уязвимость программного обеспечения Java™ Platform, позволяющая удаленному злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации

10.03.2015

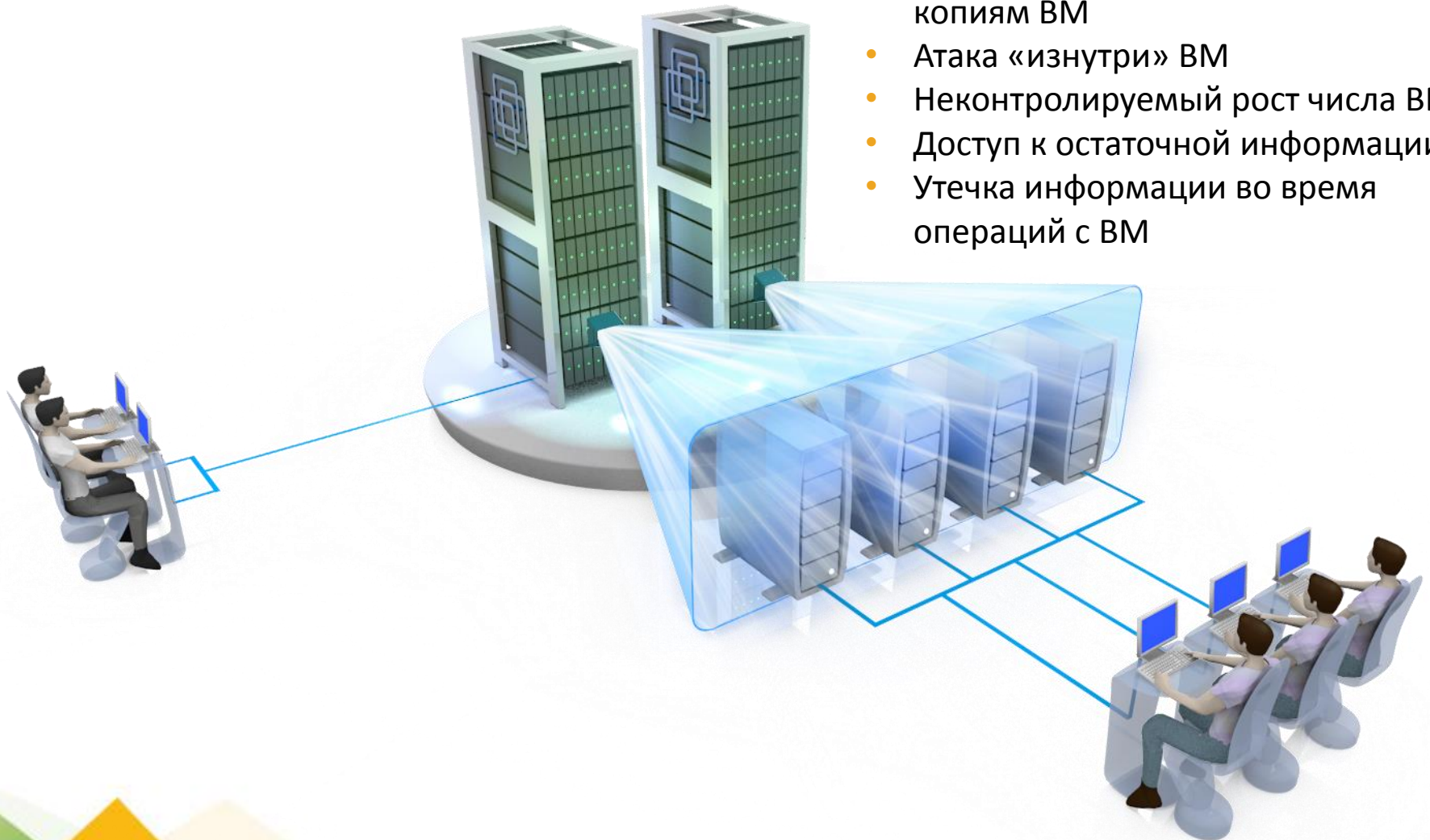
Уязвимость операционной системы Gentoo Linux, позволяющая злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации

10.03.2015

Уязвимость операционной системы Gentoo Linux,

Угрозы виртуальной инфраструктуры

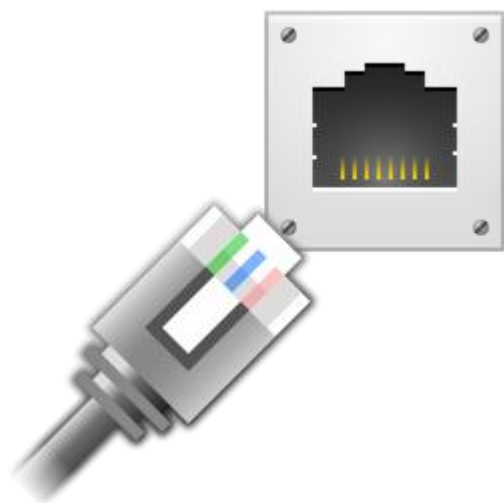
Суперпользователь



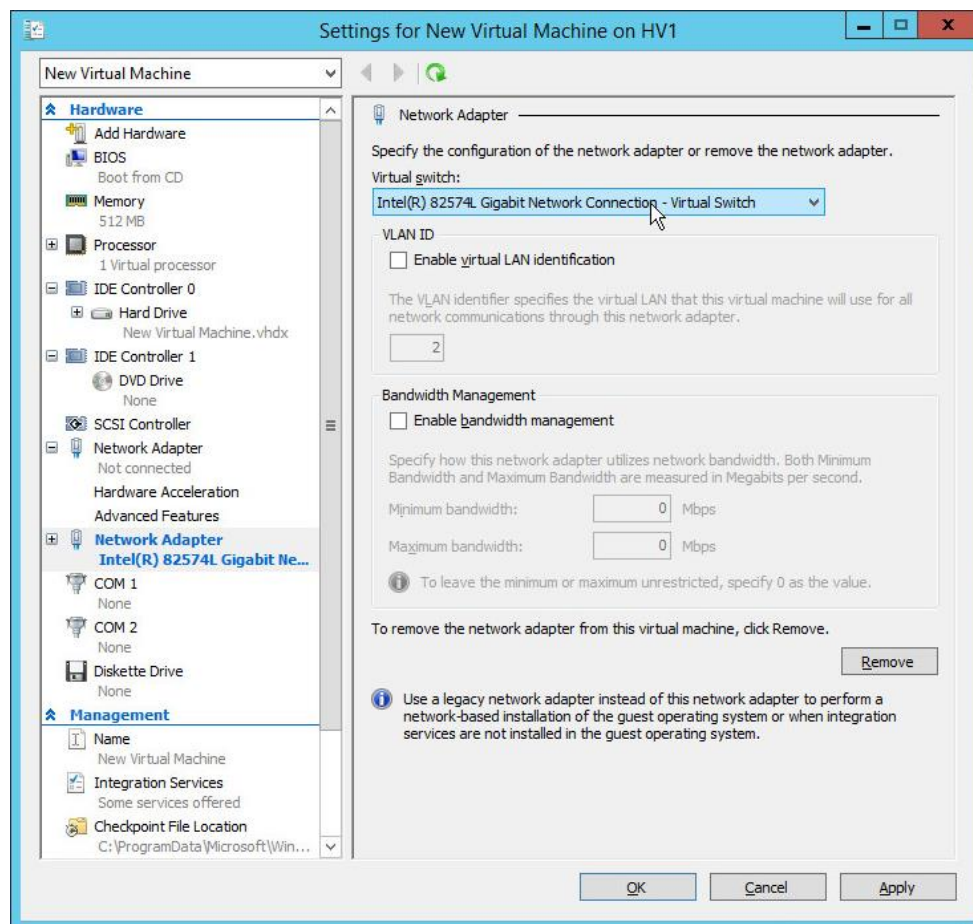
- НСД к снимкам и резервным копиям VM
- Атака «изнутри» VM
- Неконтролируемый рост числа VM
- Доступ к остаточной информации
- Утечка информации во время операций с VM

Как подключить ПК к доступной сети?

Физический:



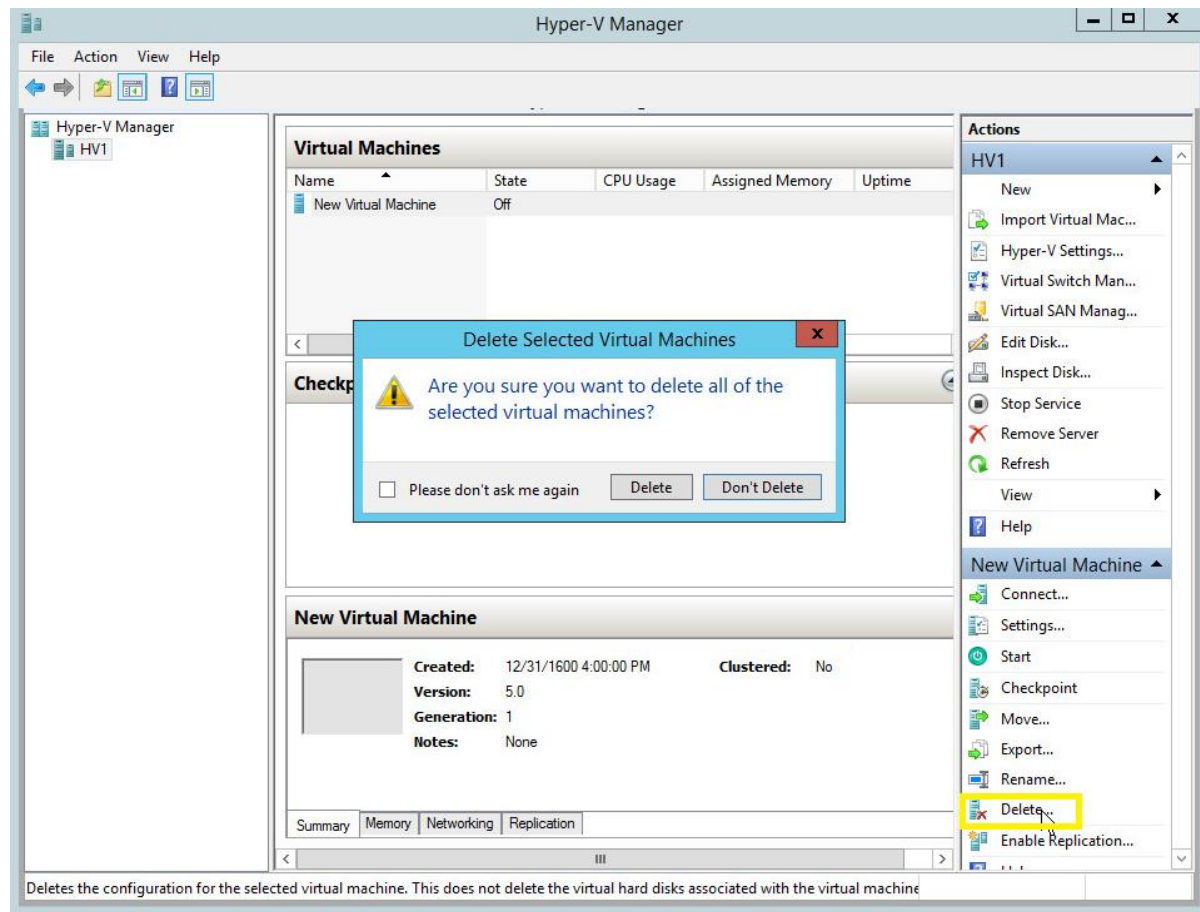
Виртуальный:



Как украсть/перенести/уничтожить ПК?

Физический:

Виртуальный:



Есть прецеденты...

Уволенный ИТ-специалист;

88 серверов;

\$800 000.



SHIONOGI INC.

[Contact Us](#) | [Privacy Policy](#) | [Terms of Use](#)

[HOME](#)

[ABOUT US](#)

[PRODUCTS](#)

[RESPONSIBILITY](#)

[CAREERS](#)

THE SHIONOGI DIFFERENCE

by being a unique global pharmaceutical company driven by a disciplined and performance based culture which values innovation, transparency and speed of execution.

Shionogi Inc.'s mission is "Working to deliver a better life". We develop and commercialize brand name prescription products for niche opportunities within chronic disease markets.

[Read More >](#)





Федеральная служба по техническому и экспортному контролю
ФСТЭК России

Банк данных угроз безопасности информации

Государственный научно-исследовательский испытательный институт проблем технической защиты информации
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»



[Угрозы](#) [Уязвимости](#) [Документы](#) [Обратная связь](#) [Новости сайта](#) [ФСТЭК России](#)

[Главная](#) / [Список угроз](#)

ФИЛЬТРАЦИЯ

Контекстный поиск по названию угрозы

Источник угрозы

Последствия реализации угрозы:

Нарушение конфиденциальности

Нарушение целостности

Нарушение доступности

Выводить по: 10, 20, 50, 100

Элементы с 1 по 10 из 16

- УБИ. 010** Угроза выхода процесса за пределы виртуальной машины
- УБИ. 044** Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
- УБИ. 046** Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
- УБИ. 048** Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин
- УБИ. 052** Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения
- УБИ. 058** Угроза неконтролируемого роста числа виртуальных машин
- УБИ. 073** Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
- УБИ. 075** Угроза несанкционированного доступа к виртуальным каналам передачи
- УБИ. 076** Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
- УБИ. 077** Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение

<< < 1 2 > >>

- Угрозы**
- Уязвимости
- Термины
- Список каналов (RSS, Atom)
- Инфографика
- Калькулятор CVSS

НОВЫЕ УЯЗВИМОСТИ

- 25.02.2015
Уязвимость программного обеспечения JavaTM Platform, позволяющая удаленному злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации
- 25.02.2015
Уязвимость программного обеспечения JavaTM Platform, позволяющая удаленному злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации
- 10.03.2015
Уязвимость операционной системы Gentoo Linux, позволяющая злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации
- 10.03.2015
Уязвимость операционной системы Gentoo Linux,

Как аттестовать инфраструктуру на соответствие требованиям регулятора?

1. Приказ **ФСТЭК №21 от 18.02.2013** «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности **персональных данных** при их обработке в информационных системах персональных данных»
2. Приказ **ФСТЭК №17 от 12.02.2013** «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
3. Приказ **ФСТЭК №31 от 14.03.2014** «Об утверждении Требований к обеспечению защиты информации в **автоматизированных системах управления производственными и технологическими процессами** на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

10 мер безопасности

+

Проект требований к СЗСВ

Требования регуляторов

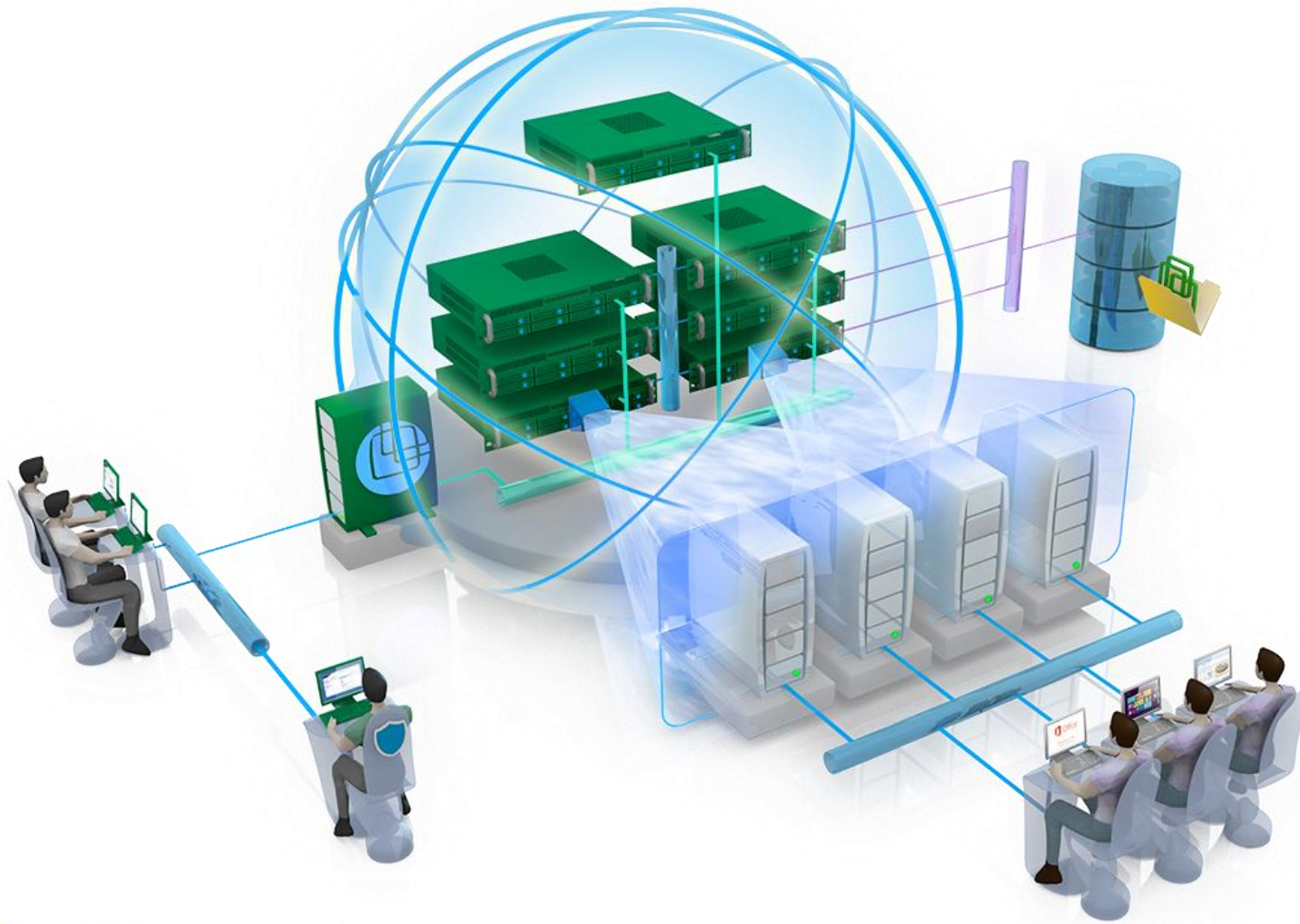
- ✓ Идентификация и аутентификация субъектов и объектов доступа в ВИ;
- ✓ Управление доступом в виртуальной инфраструктуре;
- ✓ Регистрация событий;
- ✓ Управление потоками информации между компонентами ВИ и по периметру ВИ;
- ✓ Доверенная загрузка серверов виртуализации, VM и т.д.;
- ✓ Управление перемещением VM и обрабатываемых на них данных;
- ✓ Контроль целостности виртуальной инфраструктуры и ее конфигураций;
- ✓ Резервное копирование данных, технических средств и т.д.;
- ✓ Антивирусная защита в ВИ;
- ✓ Разбиение ВИ на сегменты

Методы и рекомендации

Разделение инфраструктур



Архитектура



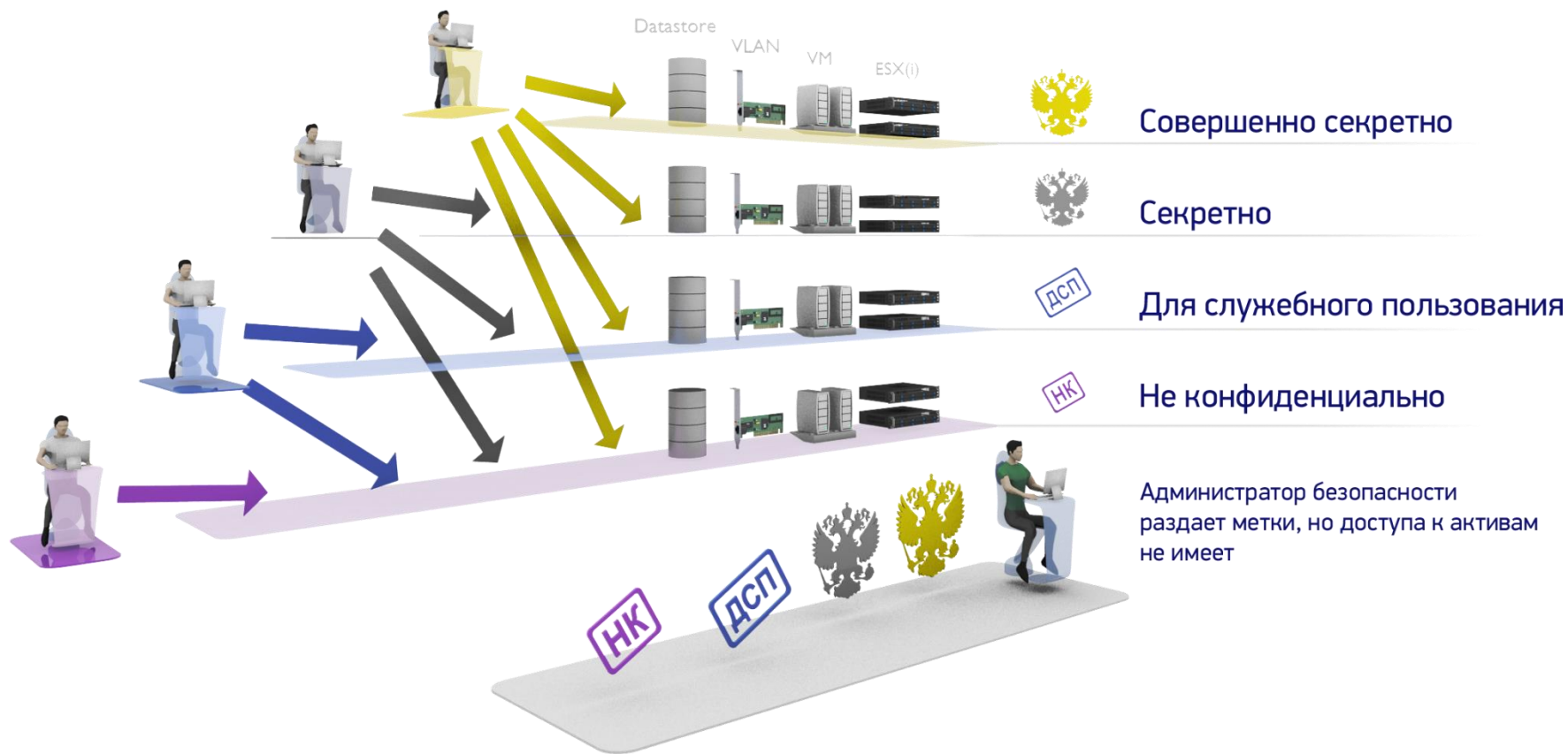
Разделение ролей



Различные способы разграничения доступа



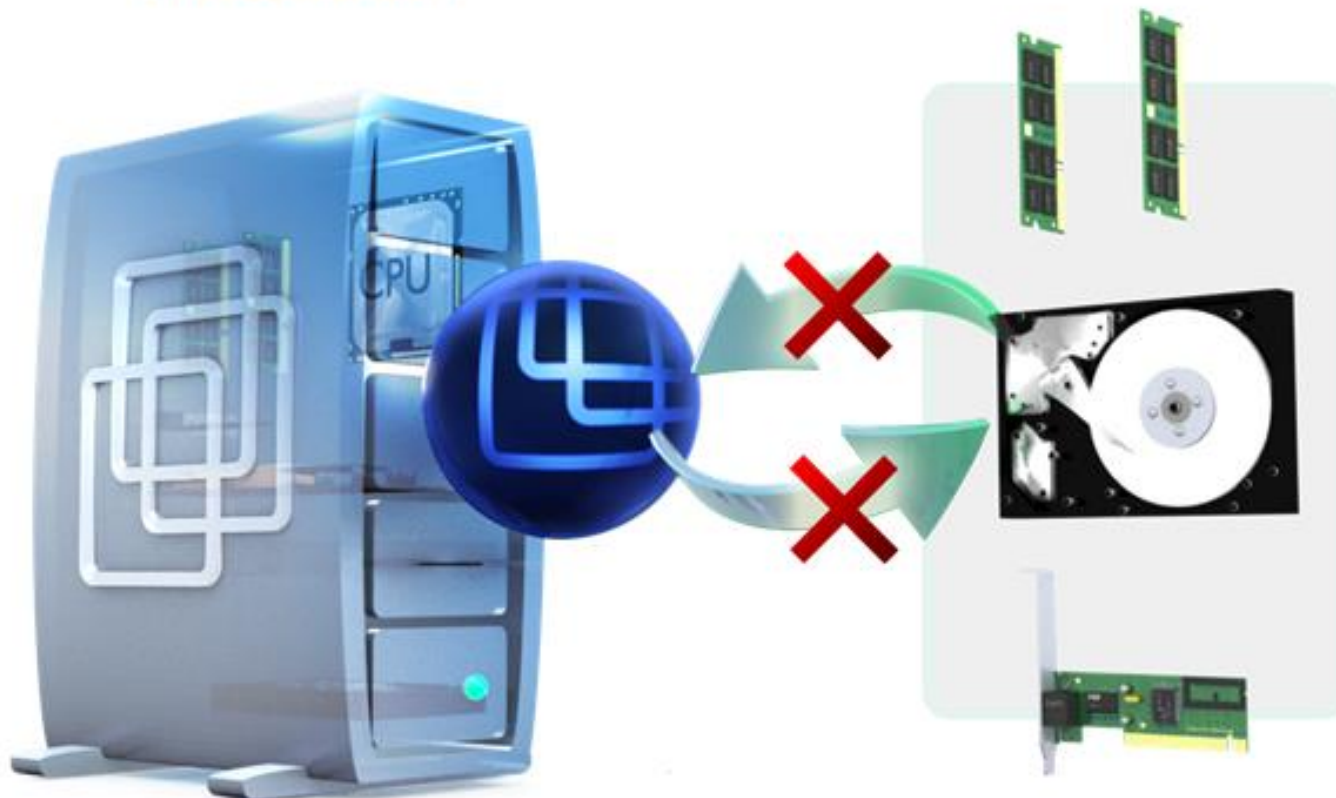
Различные способы разграничения доступа



Контроль целостности виртуальных машин и доверенная загрузка

Виртуальная машина
(virtual machine)

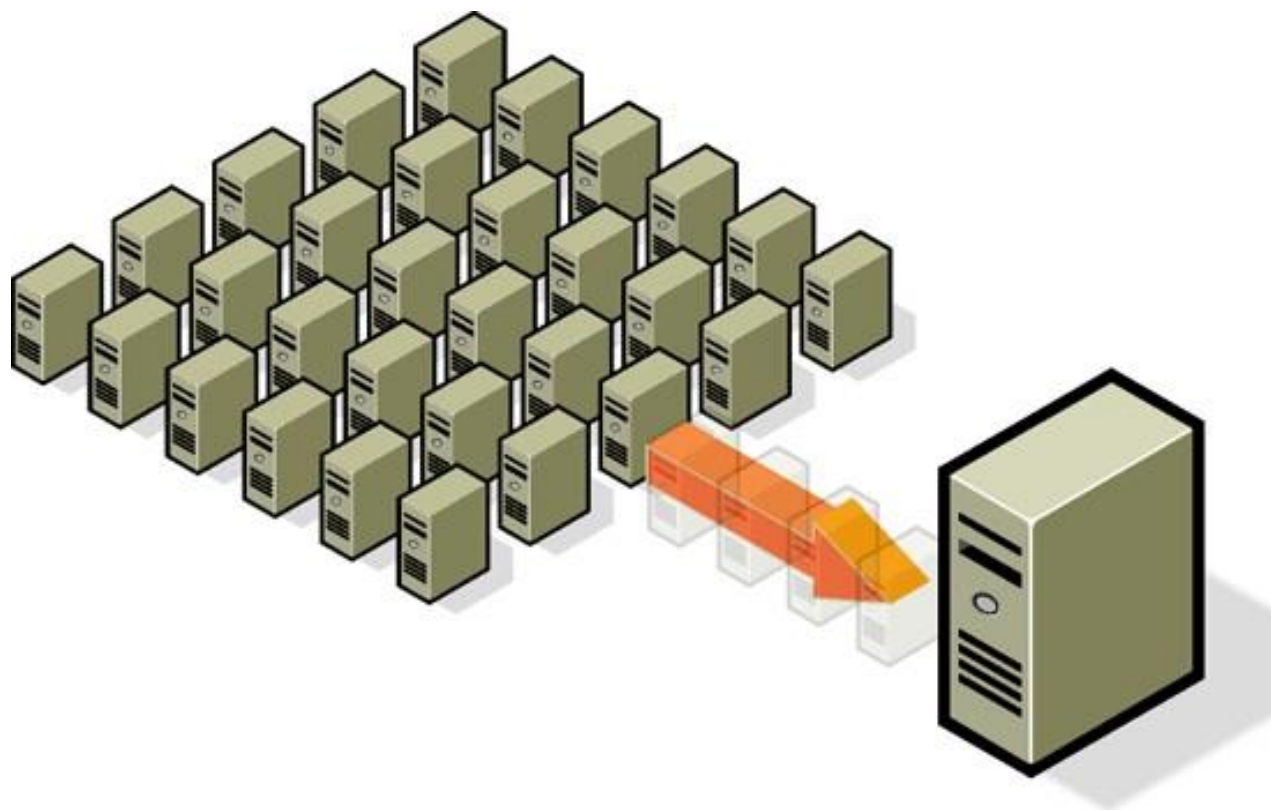
Аппаратные составляющие



Шифрование

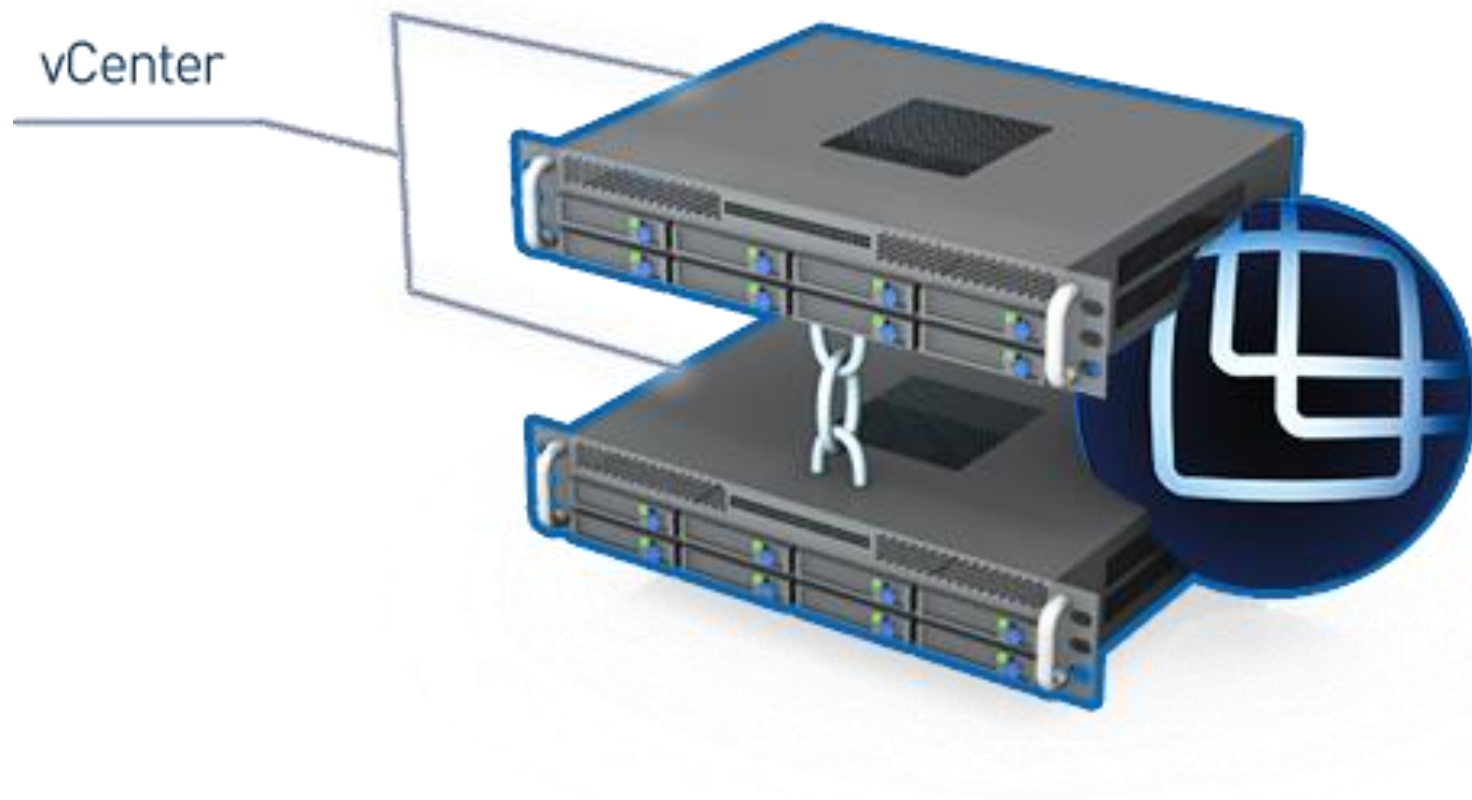


Разграничение запуска (сегментация)



Отказоустойчивость

vCenter Linked Mode



Аудит событий безопасности

The screenshot displays the vGate security console interface. On the left, a navigation pane lists various system components and their configuration options. The main area shows the 'Аудит' (Audit) section with a list of events and a detailed view of a selected event.

Аудит

Фильтрация событий

Типы событий

- Успех
- Уведомление
- Предупреждение
- Ошибка

Список событий:

Тип	Время
Успех	25-06-2014 12:22:02
Успех	25-06-2014 12:22:02
Успех	25-03-2014 12:22:02
Успех	25-03-2014 12:22:02
Успех	24-03-2014 12:22:02
Предупреждение	24-03-2014 12:22:02
Предупреждение	24-03-2014 12:22:02
Уведомление	24-03-2014 12:22:02
Уведомление	24-03-2014 12:22:02
Уведомление	24-03-2014 12:20:02
Уведомление	24-02-2014 17:15:58

Свойства события

Дата: 24-03-2014 12:22:02

Тип: Предупреждение

Компьютер: QWE

Код: 67117061

Компонент: Служба аутентификации

Категория: Аутентификация

Описание:

Аутентификация завершилась неудачно.
Пользователь: admin@VGATE
SID: <недоступно>
Адрес: 172.28.1.2
Причина: неверный пароль

Копировать Закрывать

Всего объектов: 152

Категория
Аутентификация
Аутентификация
Политики
Политики
Аутентификация
Аутентификация
Аутентификация
Служба
Служба
Общее

Настройки
Очистить
Сохранить
Свойства
Включить
Отключить
Обновить

Best Practices

Соответствие виртуальных инфраструктур требованиям стандартов и best practices :

- PCI DSS;
- VMware Security Hardening Best Practices;
- CIS VMware ESX Server Benchmarks 4;
- СТО БР ИББС;
- РД АС;
- ИСПДн.

Политики безопасности

Список наборов политик: безопасности: Всего объектов: 3

Имя	Описание
Стандарт	Стандартный набор политик
Супер	Усиленная безопасность
PCI DSS	Набор политик PCI DSS
✗ vGate	Набор настроек безопасности vGate для VMware ES...
✗ CIS 1.0	CIS VMware ESX Server 3.x Benchmark v1.0
✓ PCI DSS	PCI DSS. Requirements and Security Assessment Proc...
✓ VMware	VMware Infrastructure 3 Security Hardening
✗ CIS 1.2	CIS Security Configuration Benchmark for VMware ESX...
✗ АС 1Г	Автоматизированные системы класса 1Г
✗ АС 1В	Автоматизированные системы класса 1В
✗ АС 1Б	Автоматизированные системы класса 1Б
✓ СТО БР ИСПДн-Д	Стандарт Банка России для ИСПДн-Д
✗ СТО БР ИСПДн-Б	Стандарт Банка России для ИСПДн-Б
✗ СТО БР ИСПДн-И	Стандарт Банка России для ИСПДн-И
✗ СТО БР ИСПДн-С	Стандарт Банка России для ИСПДн-С
✗ ИСПДн К1	Информационные системы персональных данных К...
✗ ИСПДн К2	Информационные системы персональных данных К...
✗ ИСПДн К3	Информационные системы персональных данных К...

+ Добавить
✗ Удалить
✎ Изменить
✎ Переименовать

Специальные! сертифицированные средства защиты

**СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

**ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00**

**СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2383**

Выдан 12 июля 2011 г.
Действителен до 12 июля 2014 г.

Настоящий сертификат удостоверяет, что средство защиты информации «Gate-S R2», разработанное и производимое ООО «Код Безопасности» в соответствии с техническими условиями RU.88338853.501410.013 ТУ, функционирующее в средах операционных систем, указанных в формуляре RU.88338853.501410.013 30, является программным средством защиты от несанкционированного доступа к информации, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 2 уровню контроля и техническим условиям, а также может использоваться для создания автоматизированных систем до класса защищенности ИБ включительно и для защиты информации в информационных системах персональных данных до 1 класса включительно при выполнении ограничений по применению, указанных в технических условиях.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «Научно-Производственное Объединение «Эшелон» (аттестат аккредитации от 03.06.2009 № СЗИ RU.2321.Б011.033) – техническое заключение от 13.05.2011, и экспертного заключения от 29.06.2011 органа по сертификации ОАО «Безопасность информационных технологий и компонентов» (аттестат аккредитации от 21.11.2008 № СЗИ RU.1190.А98.011).

Заявитель: ООО «Код Безопасности»
Адрес: 127018, г. Москва, ул. Сушевский вал, д. 47, стр. 2, пом. 1
Телефон: (495) 980-2345

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанных в настоящем сертификате руководящего документа и техническим условиям осуществляется испытательной лабораторией ЗАО «Научно-Производственное Объединение «Эшелон».

НАЧАЛЬНИК 2 УПРАВЛЕНИЯ ФСТЭК РОССИИ


А.Куй



Настоящий сертификат внесен в Федеральный реестр сертифицированных средств защиты информации
12 июля 2011 г.

СПАСИБО!

Денис Полянский

www.securitycode.ru



Код безопасности