Код Безопасности

конференция РусКрипто

Технологии виртуализации и информационная безопасность

Денис Полянский
ООО «Код Безопасности»

FORRESTER®

Все знают преимущества виртуализации...

но не ее риски!

Код Безопасности

Известные преимущества виртуализации

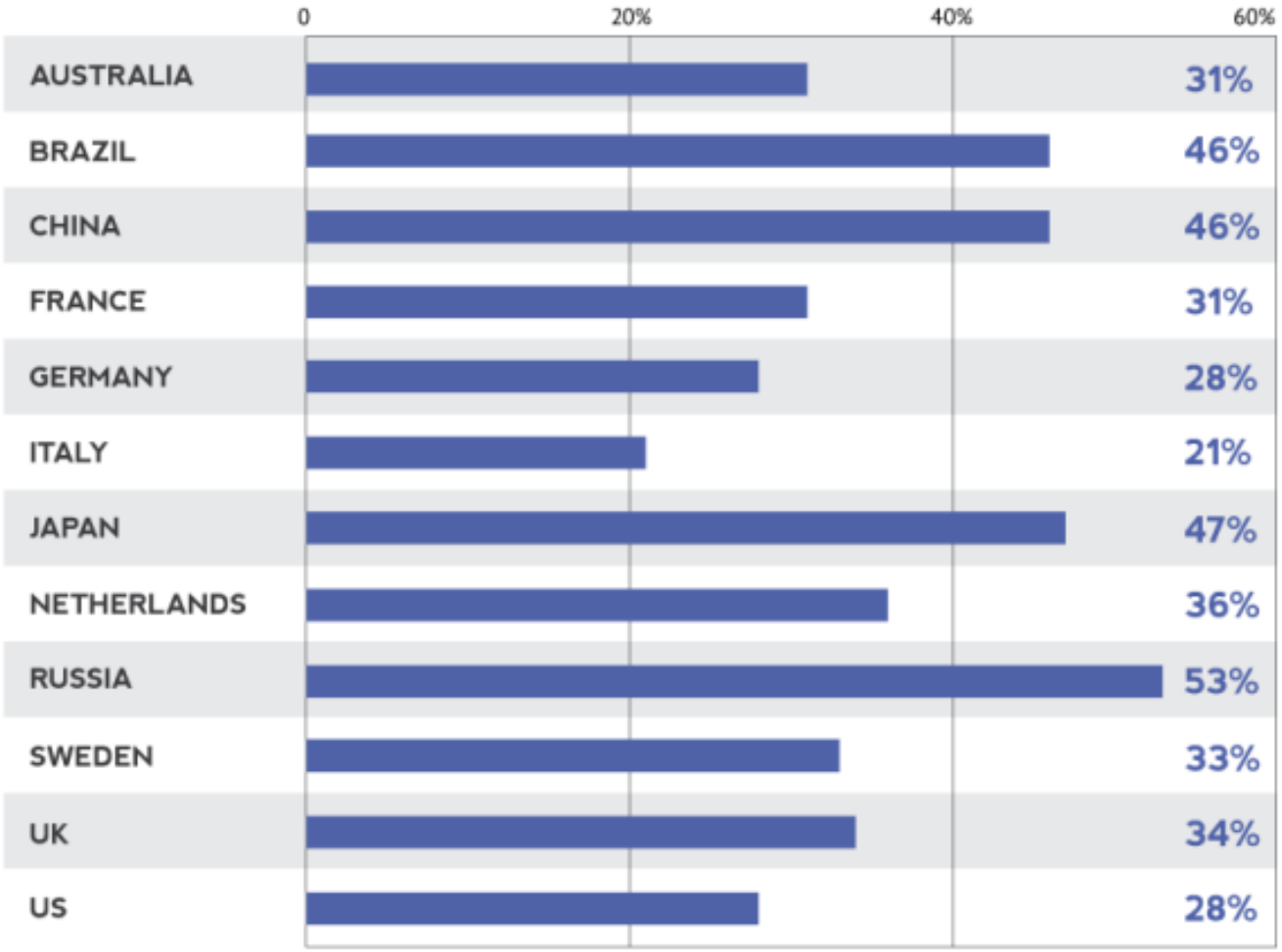
- Сокращение затрат на закупку и обслуживание физических серверов;
- Оптимизация использования вычислительных мощностей;
- Увеличение энергоэффективности;
- Обеспечение непрерывности работы за счет механизмов кластеризации и аварийного восстановления.

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.):



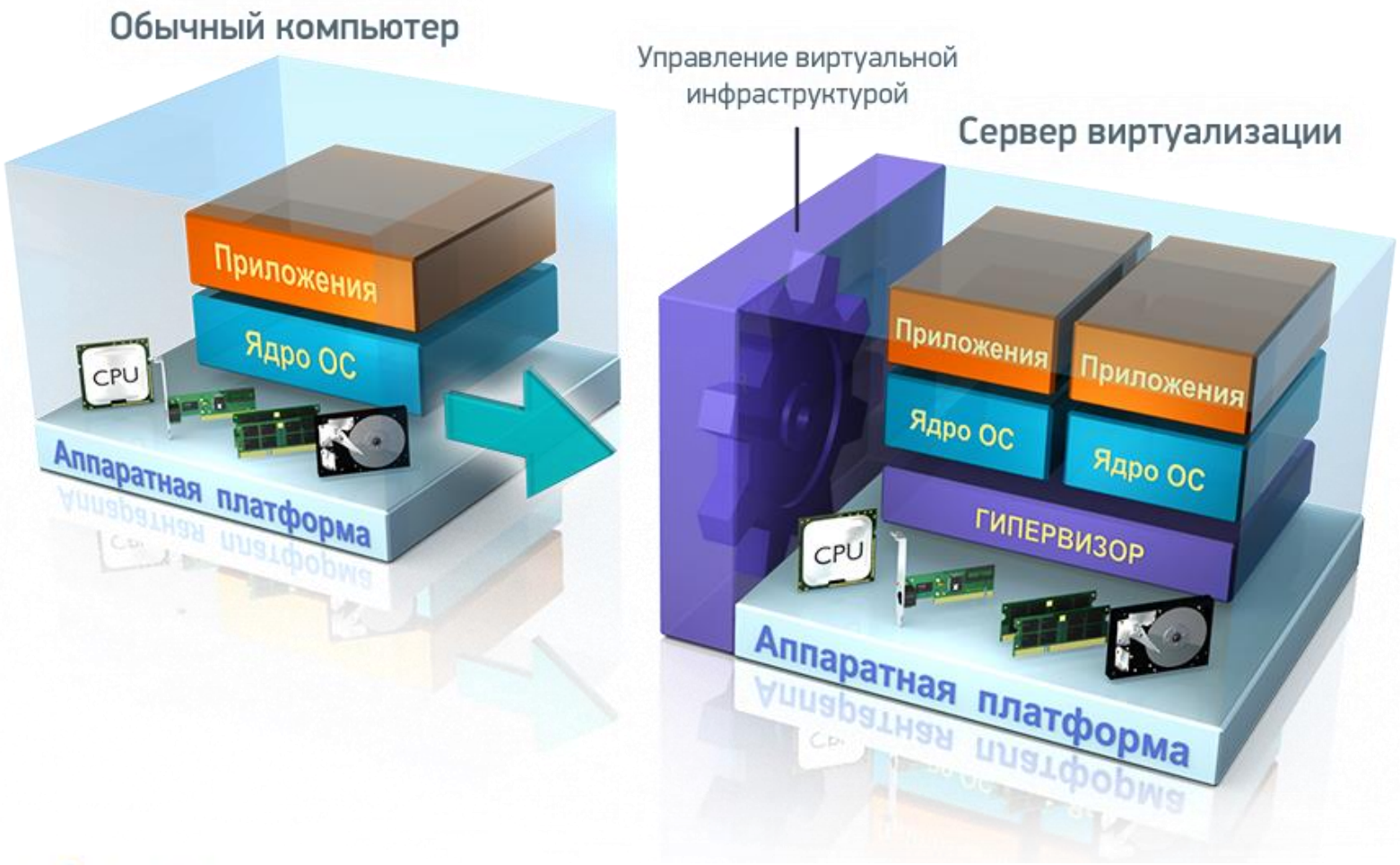
Виртуализация – не только преимущества

46%

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

*- опрос Ponemon Institute

Виртуализация



Традиционные угрозы

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

Традиционно-специфические угрозы

- Вредоносное ПО.
- Уязвимости платформы.

Вредоносное ПО

- **2012 г. MORCUT.**

  Первый троян, заражающий шаблоны BM

Уязвимости платформы

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

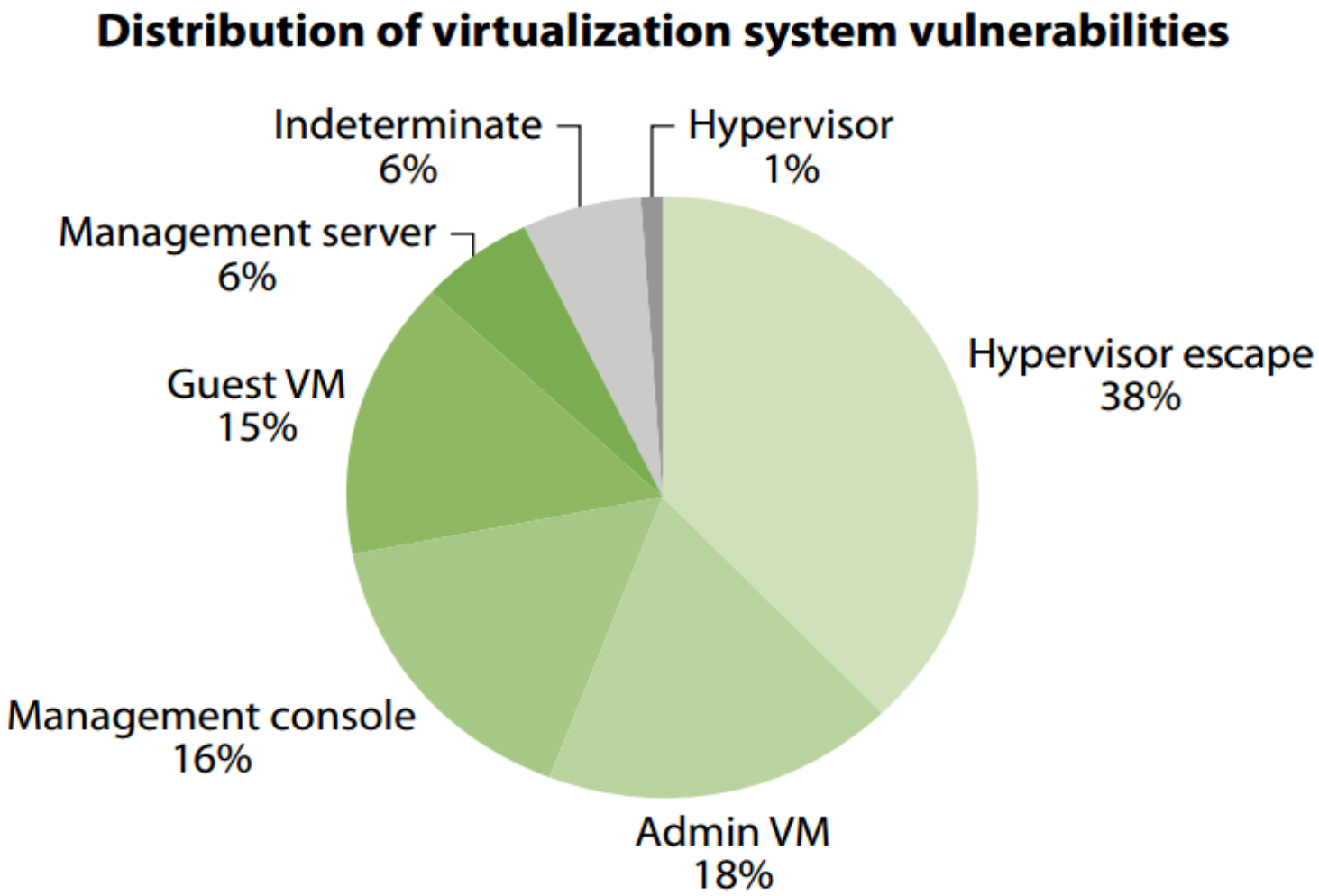
VMware Workstation host privilege escalation vulnerability

July 31, 2013

VMSA-2013-0009

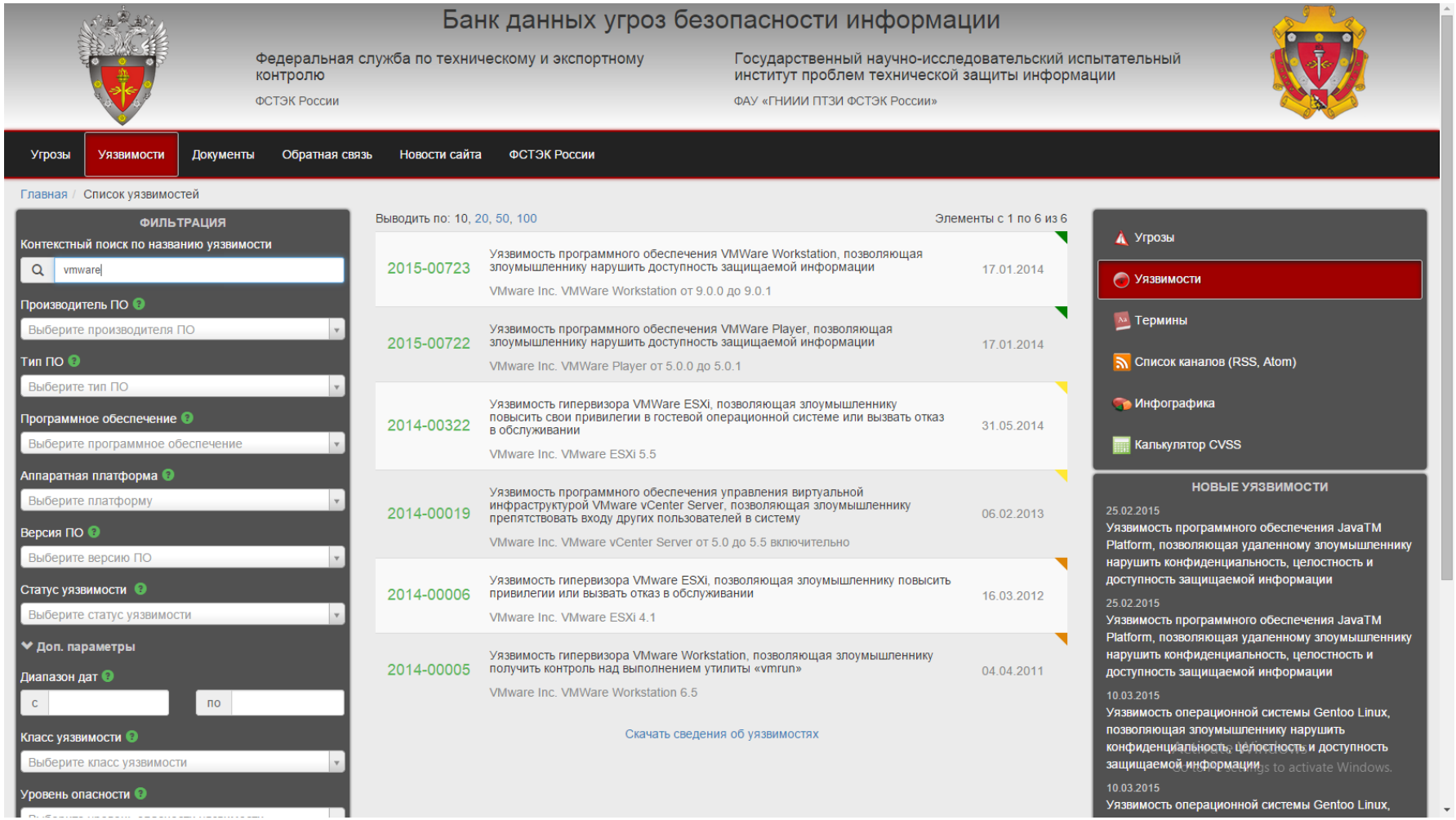
VMware ESX and ESXi updates to third party libraries

Уязвимости платформы



* Forrester Research, Inc

Уязвимости платформы

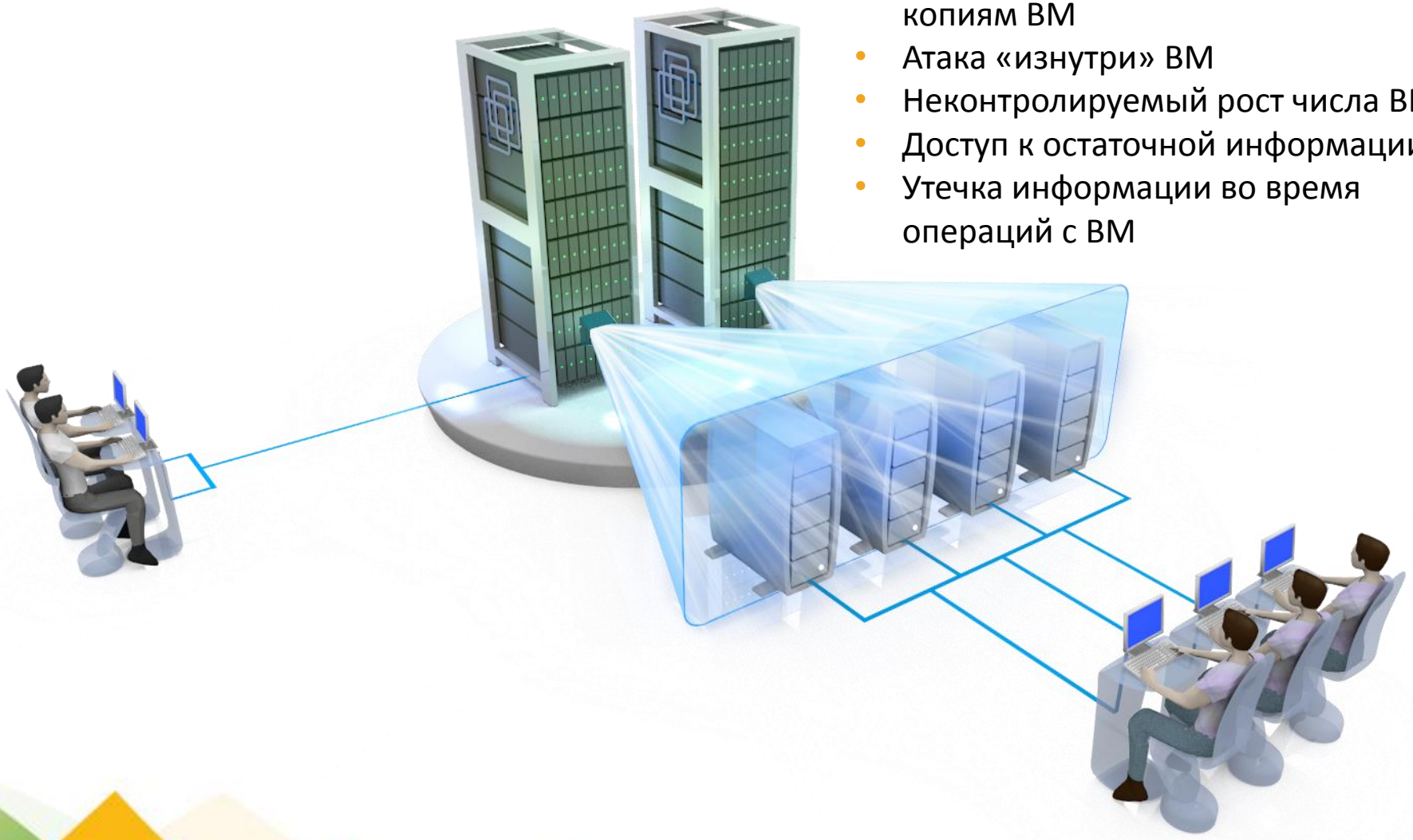


Код Безопасности

Угрозы виртуальной инфраструктуры

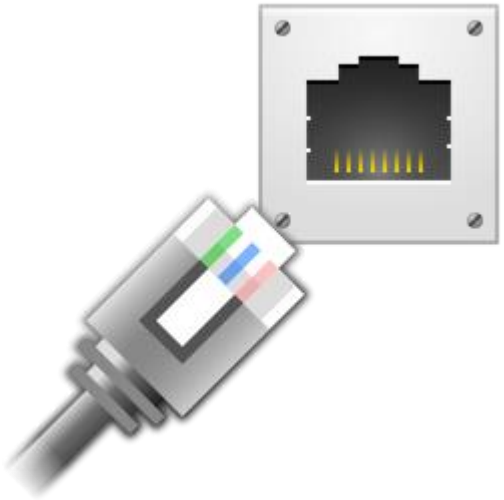
Суперпользователь

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

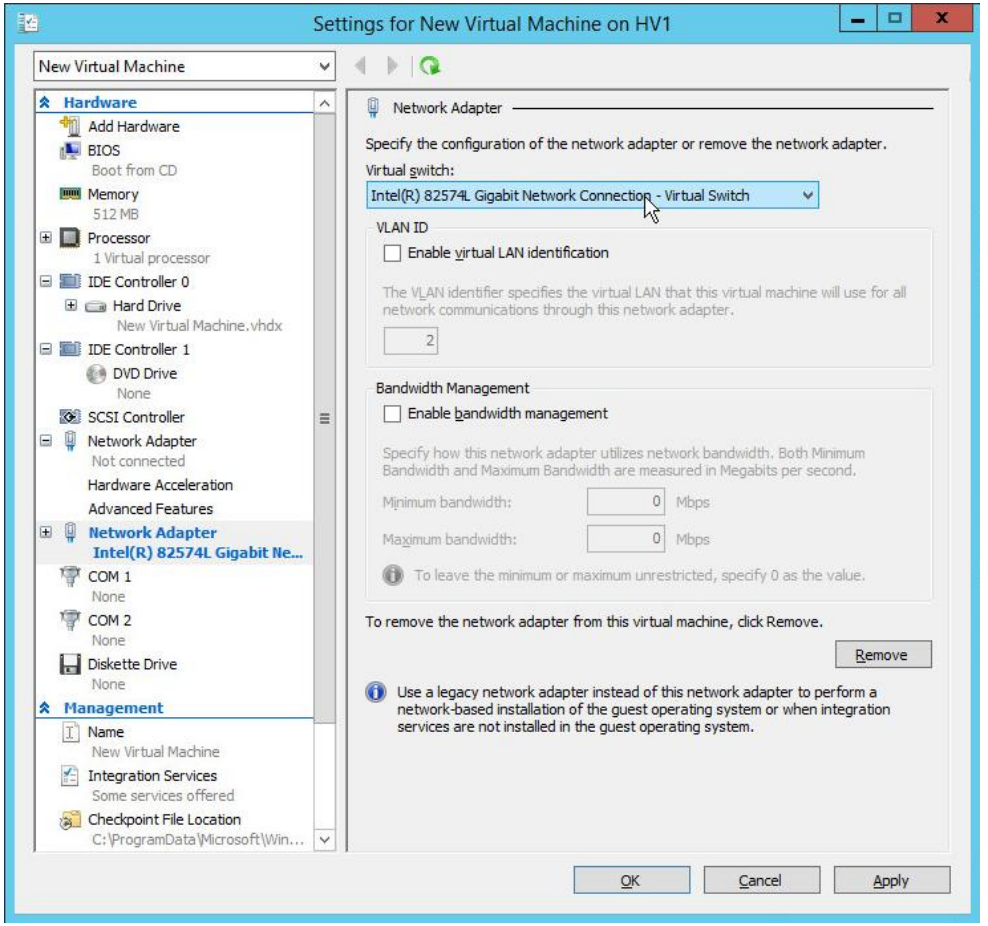


Как подключить ПК к доступной сети?

Физический:



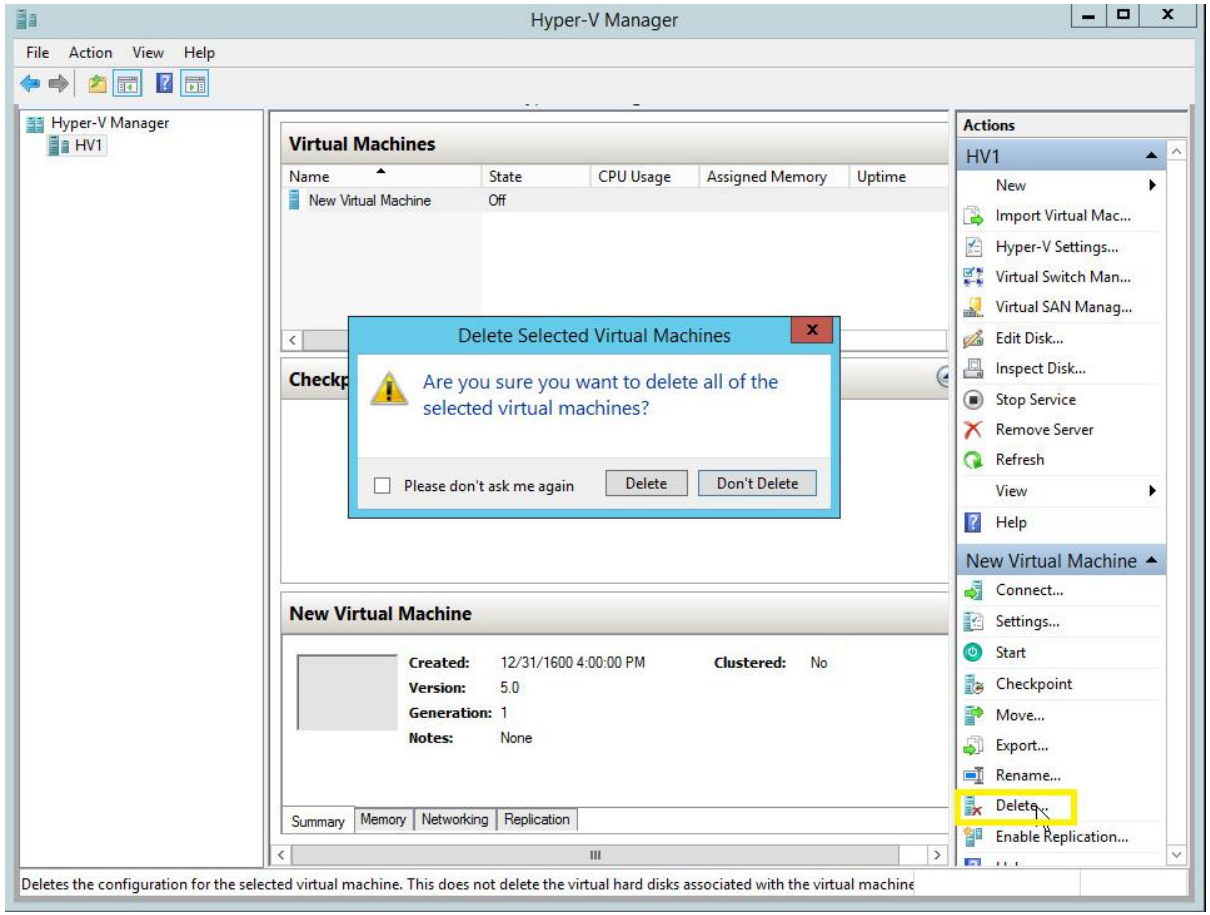
Виртуальный:



Как украсть/перенести/уничтожить ПК?

Физический:

Виртуальный:

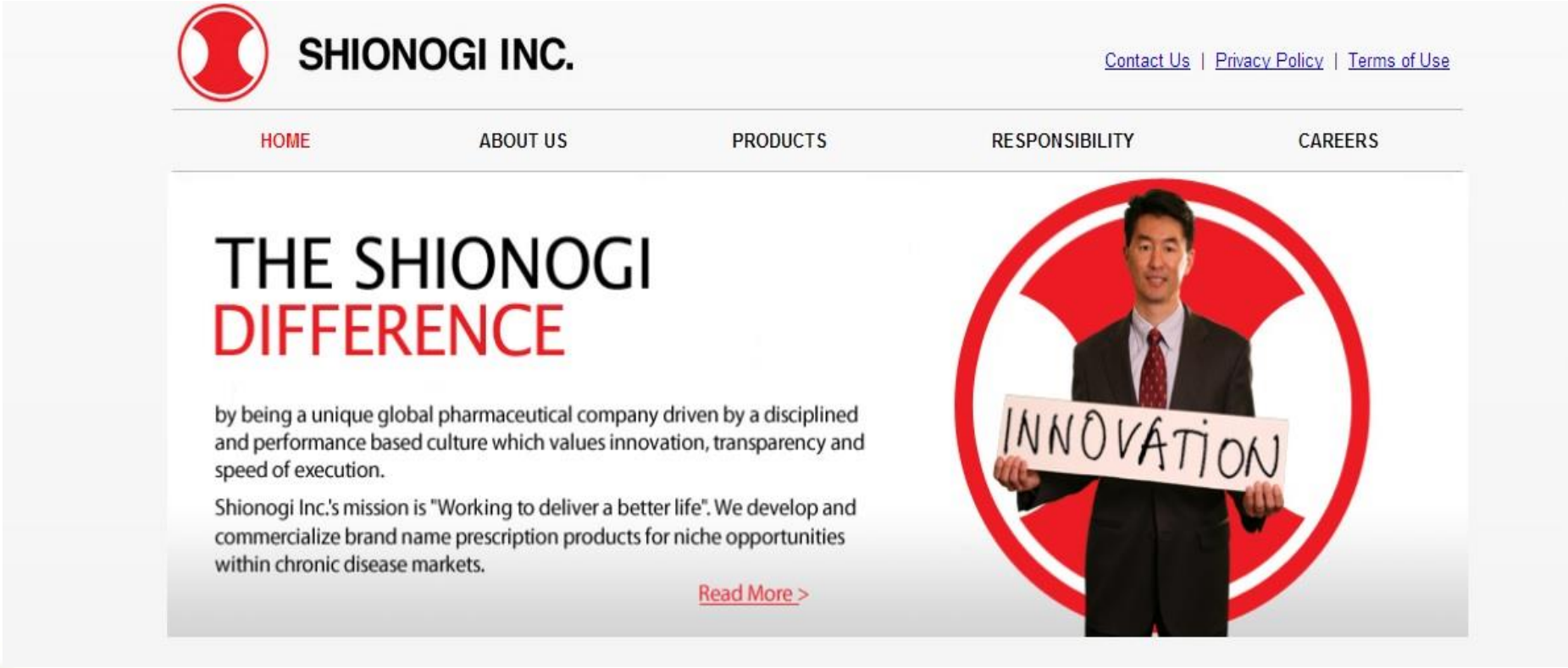


Есть прецеденты…

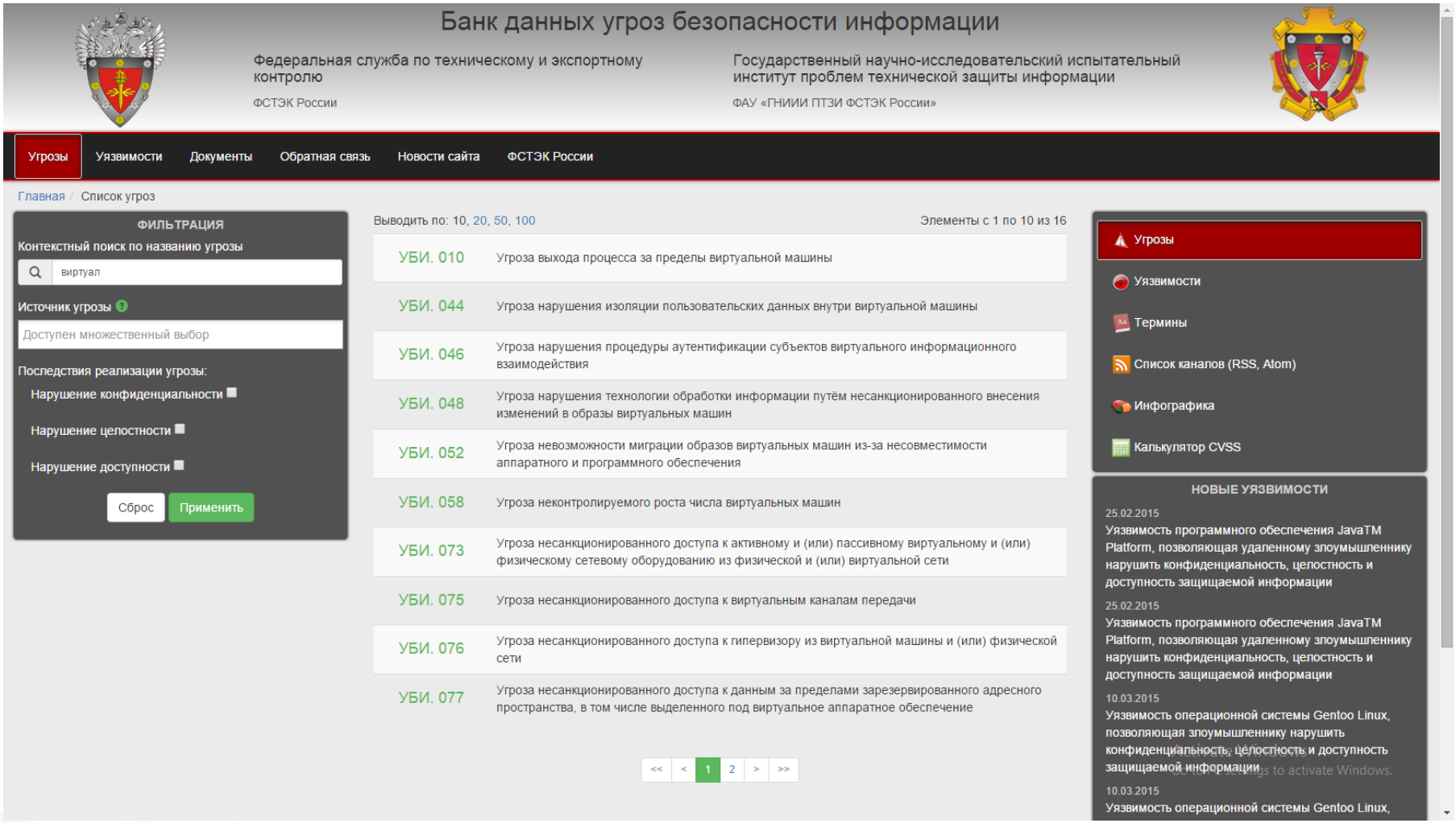
Уволенный ИТ-специалист;

88 серверов;

$800 000.



ФСТЭК



Код Безопасности

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

Код безопасности

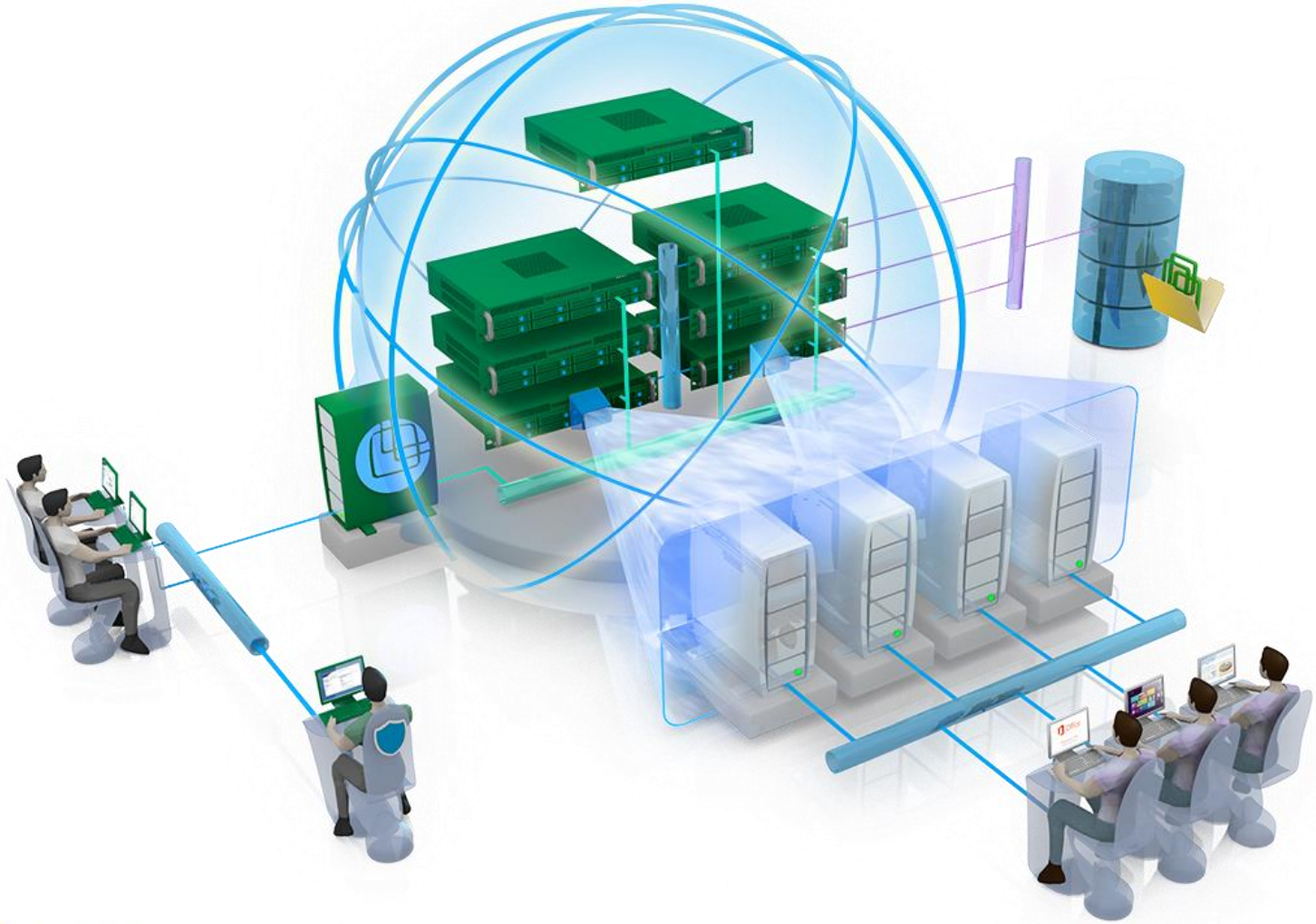
Требования регуляторов

- 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, ВМ и т.д.;
- Управление перемещением ВМ 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

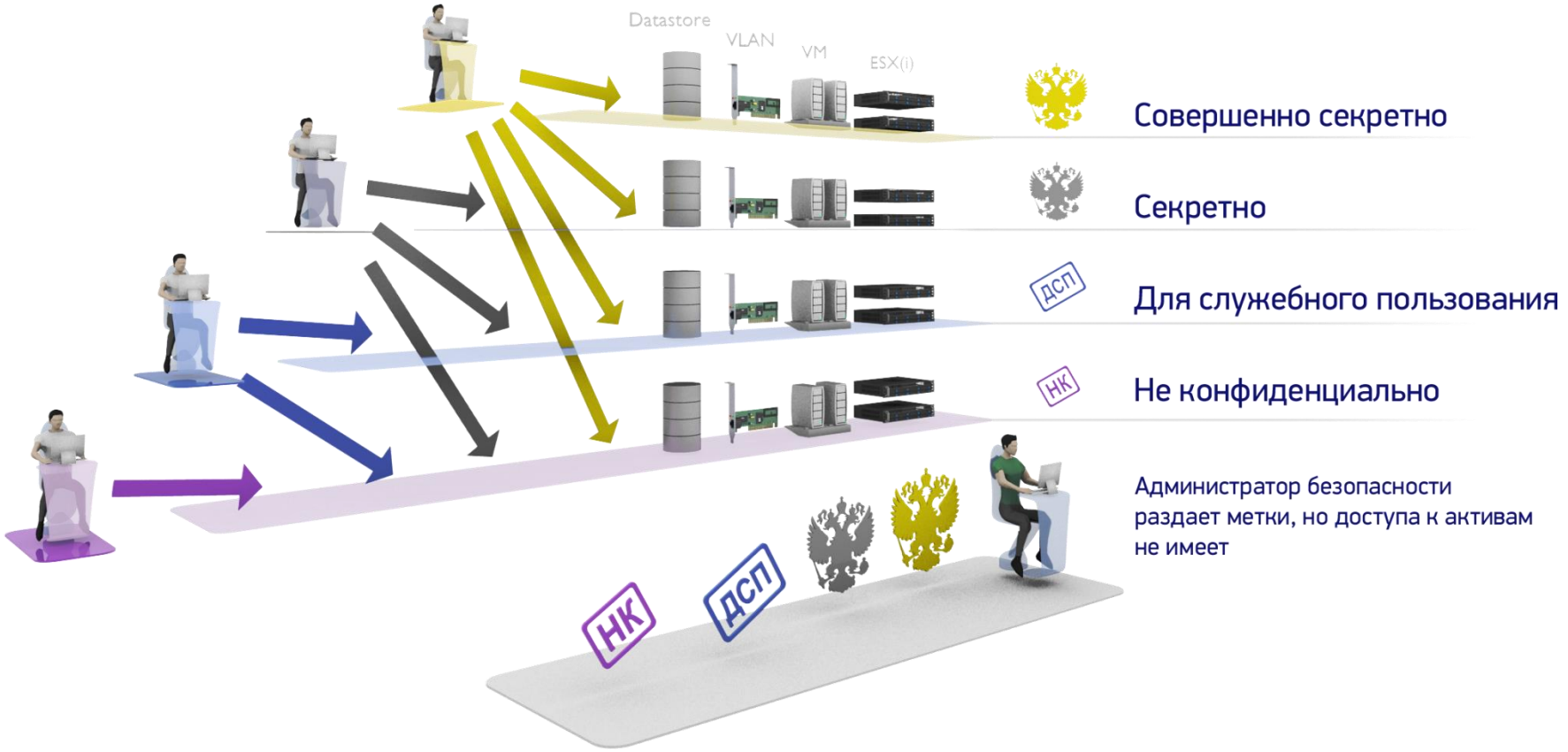
Архитектура



Разделение ролей

Различные способы разграничения доступа

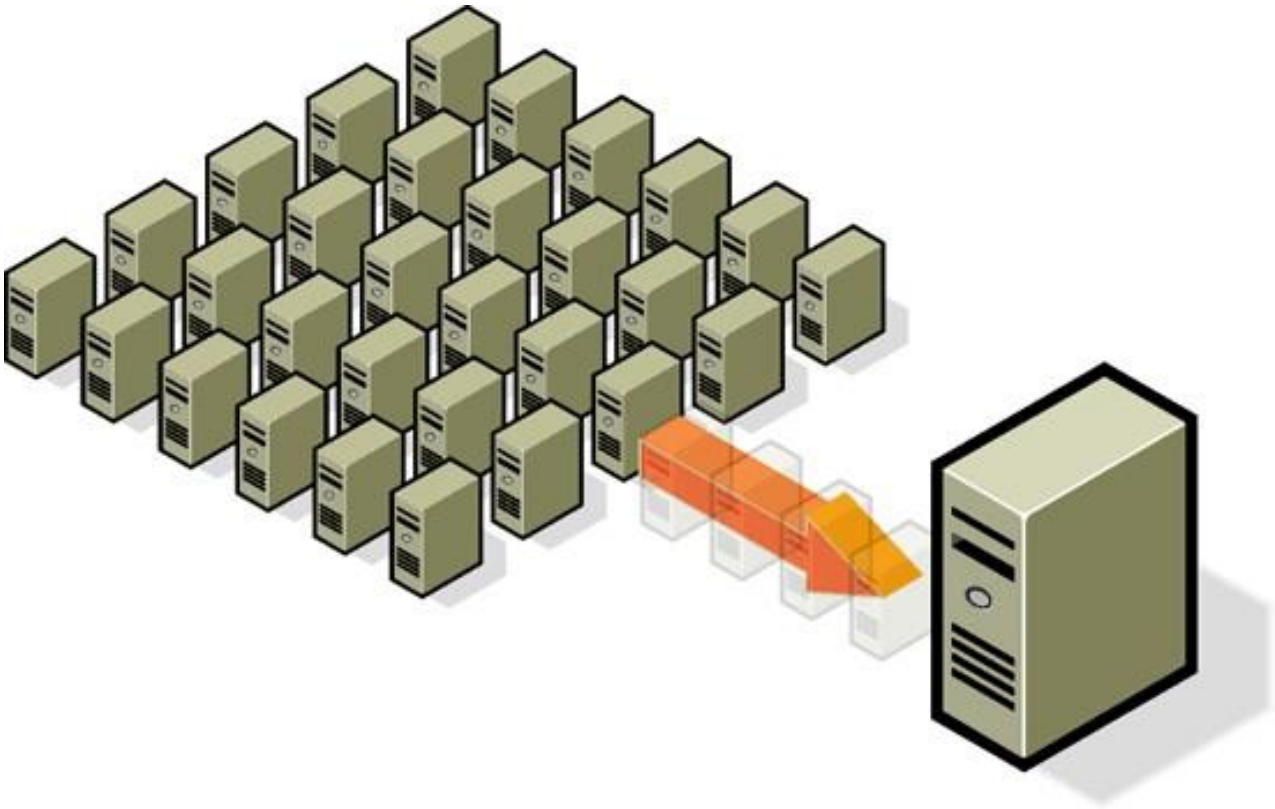
Различные способы разграничения доступа



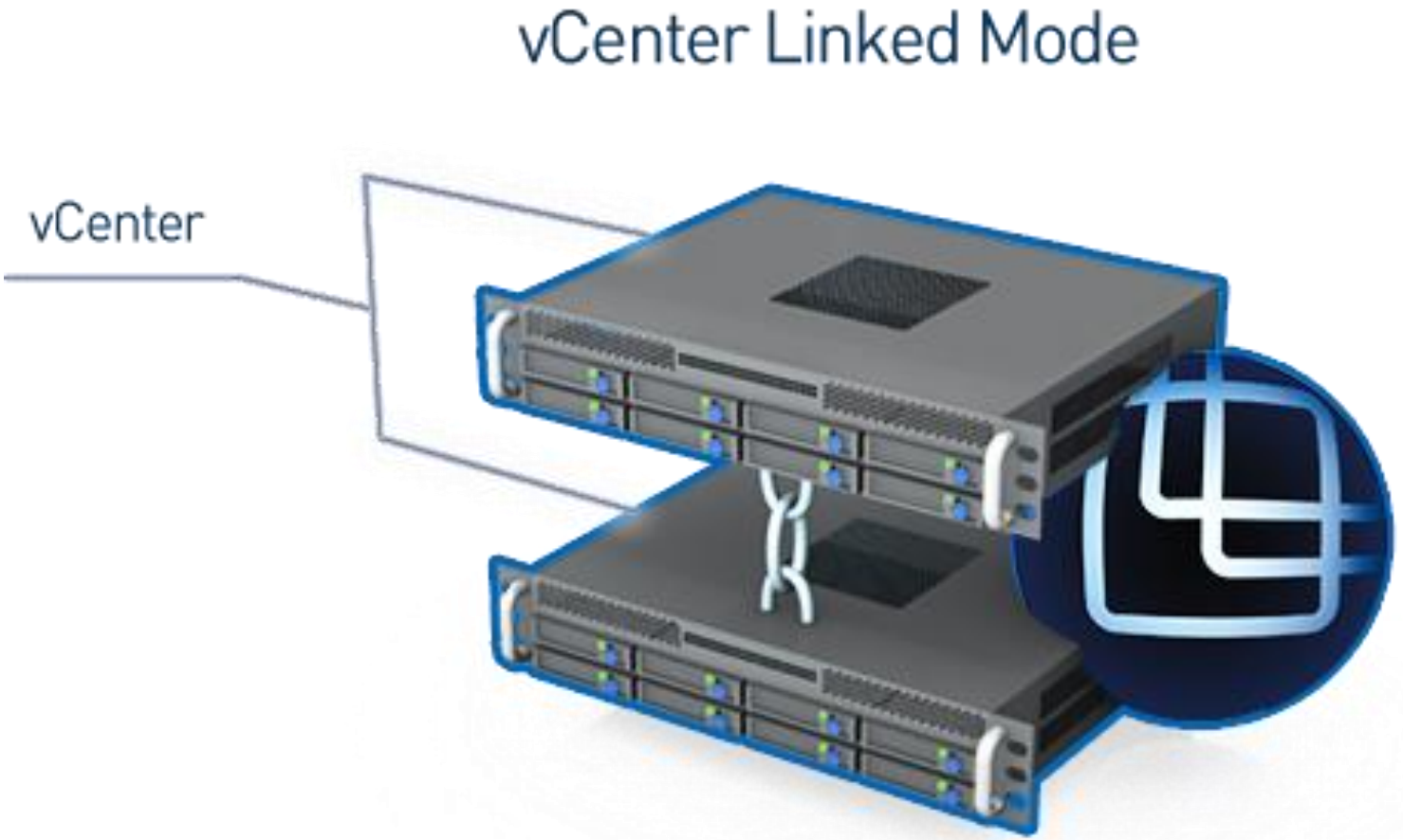
Контроль целостности виртуальных машин и доверенная загрузка

Шифрование

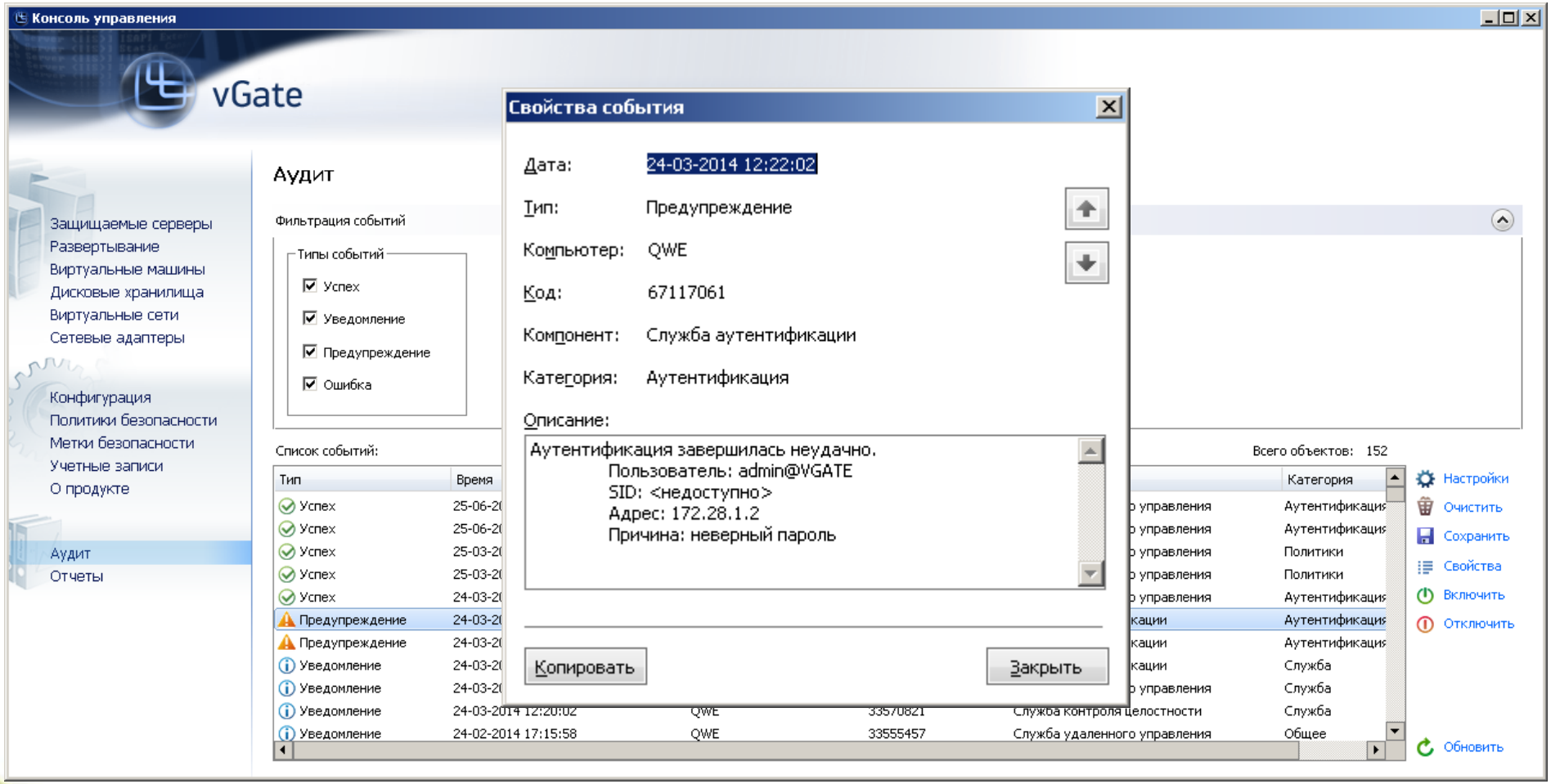
Разграничение запуска (сегментация)



Отказоустойчивость



Аудит событий безопасности

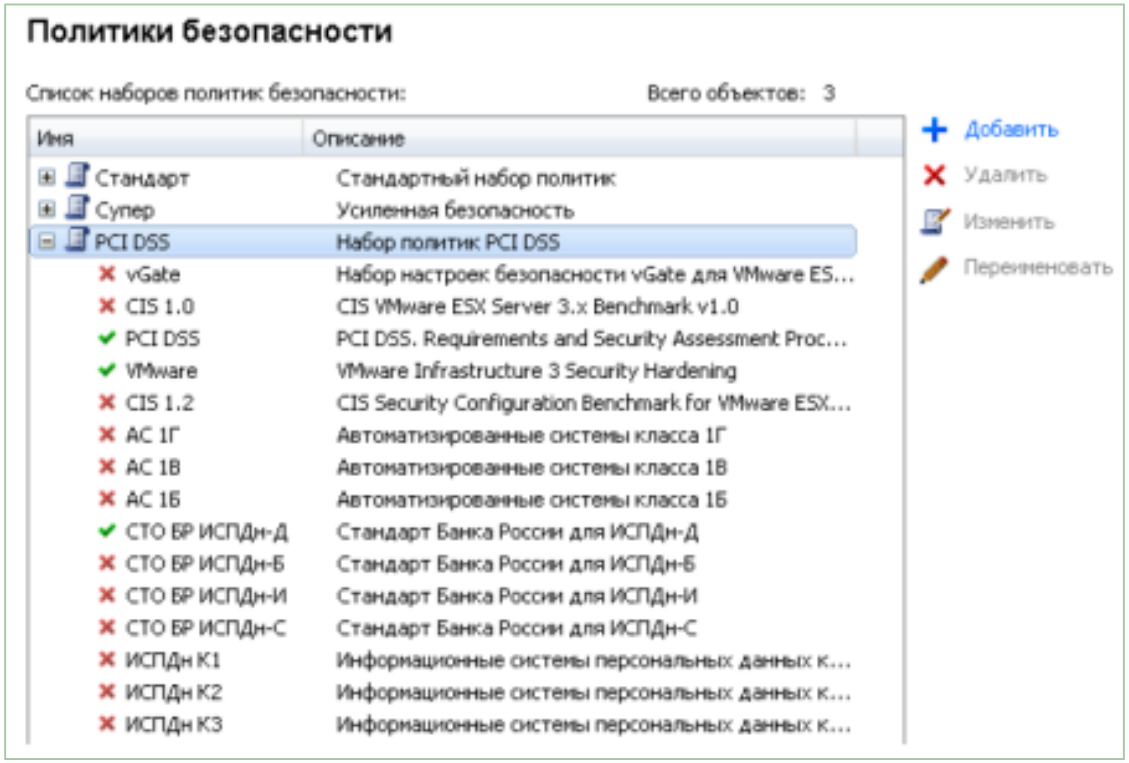


Код Безопасности

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.



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 «vGate-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 1Б включительно и д ля 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.A98.011).

Заявитель: ООО «Код Безопасности»
Адрес: 127018, г. Москва, ул. Сущевский 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.Куц

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

Код Безопасности

СПАСИБО!

Денис Полянский

www.securitycode.ru

Код безопасности