Частное облако: требования заказчика и возможности продуктов

Александр Шибаев
sav@cbr.ru

Результаты внедрения систем виртуальных серверов и терминального доступа в Банке России

Реализация проекта виртуализации серверов позволила:

- сократить времени на внедрение автоматизированных систем (подготовка технической базы АС сокращена с 4-5 месяцев до 2-3- дней);
- повысить надежности за счет свойств виртуальной среды и резервирования;
- повысить эффективное использование вычислительных ресурсов (с 1-5% до 50-80%);
- снизить затраты на администрирование комплекса серверов;
- по мере роста потребностей проводить модернизацию СКСД, а не АС;
- экономить площади ВЦ (около 100 виртуальных серверов и рабочих станций – 1 стойка);
- снизить требования к системам инженерного обеспечения.

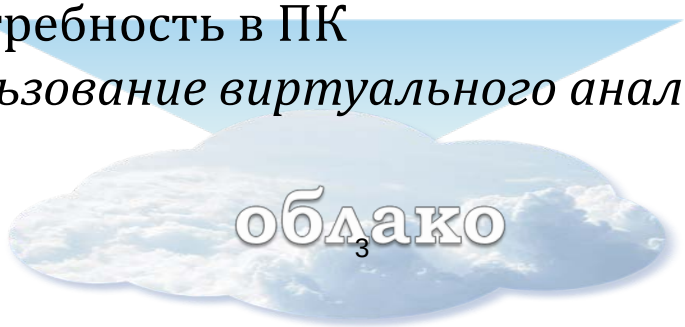
Реализация проекта терминального доступа позволила :

- отказаться от серверного оборудования в РКЦ (в ИС);
- снизить трудоемкость администрирования типовых программных комплексов;
- сократить время на внедрение ППК;
- снизить стоимость АРМ ТУ.

Как развиваться дальше?

Вопросы, требующие решения

- повышение управляемости виртуальной инфраструктурой - *в виртуальной* среде *десятки серверов*
- автоматизация процессов администрирования - *снижение нагрузки на системных администраторов и зависимости от администраторов*
- обеспечение информационной безопасности в виртуальной среде – *вход в виртуальную среду защищен, но внутренней защиты нет*
- обеспечение оперативной масштабируемости – *виртуальный сервер может быть загружен неравномерно от 5% до 95% - ресурсы или не используются или не хватает*
- как уменьшить потребность в ПК *использование виртуального аналога терминала*



Облачные вычисления

Определение Национального института стандартов и технологий США

пять основных характеристик

- динамическое выделение ресурсов
- сетевой доступ (корпоративные сети)
- оперативная эластичность (масштабируемость)
- поддержание качества оказываемой услуги за счет автоматического перераспределения ресурсов
- измеряемое качество оказываемых услуг

три сервисные модели

- ПО как услуга (SaaS)
- платформа как услуга (PaaS)
- инфраструктура как услуга (IaaS)

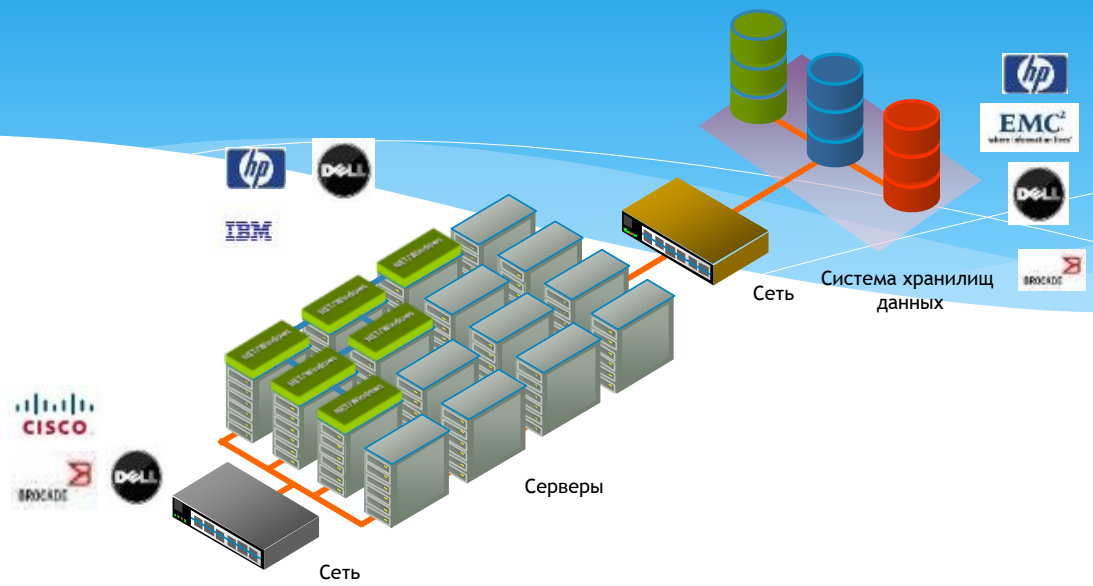
три модели развертывания

- частные облака
- публичные облака
- гибридные облака

Облако = ЦОД +виртуализация+ «Cloud» ПО

Комплекс технических средств

1



Комплекс программных средств

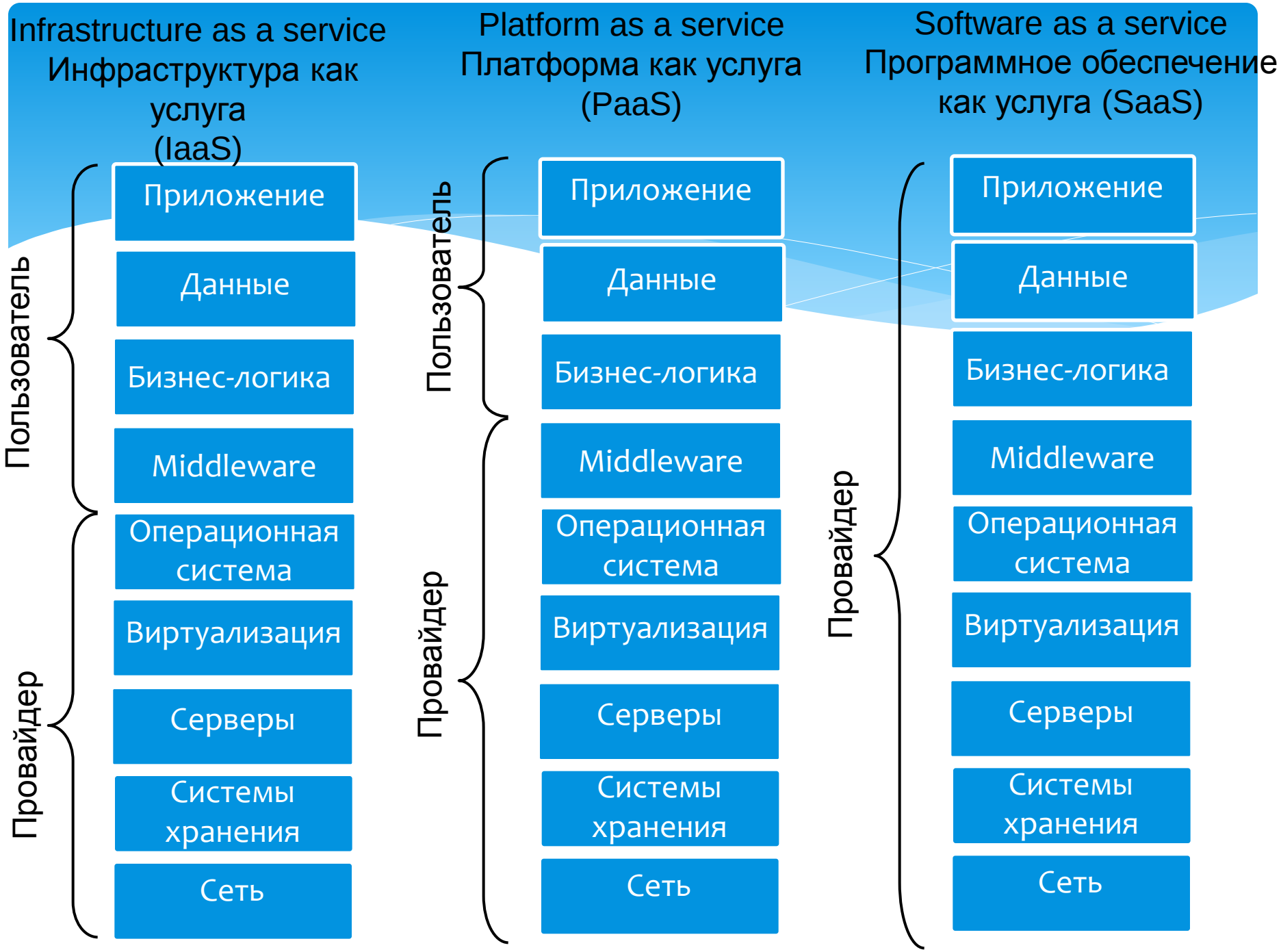
2 ПО гипервизора — Гостевые ОС

3 ПО контроллера инфраструктуры (облачного контроллера)

4 ПО управления | ПО мониторинга | ПО принятия решений

5 ПО портала самообслуживания

6 ПО брокера соединений


Infrastructure as a service
Инфраструктура как услуга (IaaS)
Platform as a service
Платформа как услуга (PaaS)
Software as a service
Программное обеспечение как услуга (SaaS)
Пользователь
Провайдер
Приложение
Данные
Бизнес-логика
Middleware
Операционная система
Виртуализация
Серверы
Системы хранения
Сеть

ПОСТАВЩИКИ ОБЛАЧНЫХ РЕШЕНИЙ

СРАВНЕНИЕ ОБЛАЧНЫХ РЕШЕНИЙ (2011 Г.)

	HP CSA	BMC BladeLogic	DELL VIS	Vmware vCloud Director	IBM CloudBurst
Поддержка компонент сторонних разработчиков		✓	✓		
Интегрированное решение	✓			✓	✓
Быстрое и удобное создание сервисов					
Управление жизненным циклом приложений	✓	✓	✓		
Контроль потребляемых сервисов	✓	✓		✓	✓
Решение для частного «облака»	✓	✓	✓	✓	✓
Инсталляция приложений	✓	✓	✓		✓
Конфигурирование серверов	✓	Нет управления СХД	Не интегрированное решение	✓	✓

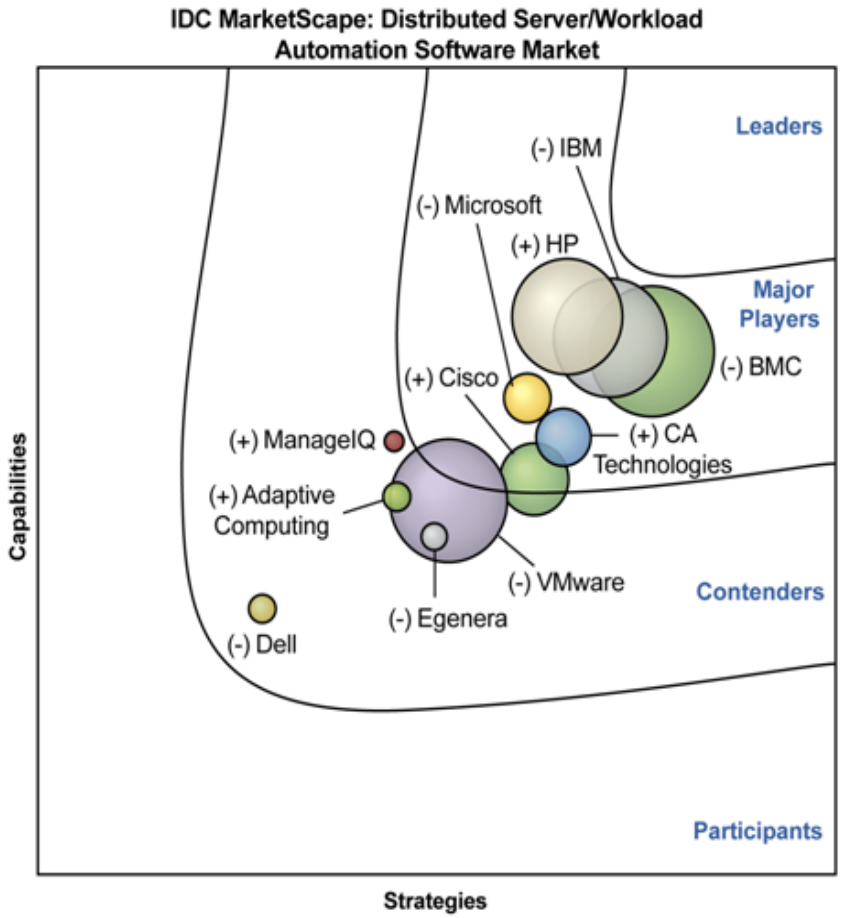
ПОСТАВЩИКИ ОБЛАЧНЫХ РЕШЕНИЙ

HP CSA	BMC BladeLogic	DELL VIS	Vmware vCloud Director	IBM CloudBurst

СРАВНЕНИЕ ОБЛАЧНЫХ РЕШЕНИЙ (2012 Г.)

	HP Cloud System	IBM Pure Flex +SmartCloud	VCE Vblock + vCloud	NetApp-Cisco FlexPod+ Cloud SW	Cisco IA for Cloud+ UCS	Oracle Exalogic	Dell VIS
Experience	✓	new/ uproven	✓	limited	limited	limited	limited
Hybrid Delivery	✓	✓	✓	limited	✓	✓	✓
Open and Extensible	✓	limited heterogeneous	rigid configs	✓	✓	closed	✓
Converged Infrastructure	✓	✓	✓	✓	no storage	✓	limited

АНАЛИЗ IDC



SOURCE: IDC MarketScape: Worldwide Distributed Server/Workload Automation Software 2012 Vendor Analysis, by Mary Johnston Turner, Doc # 236186, July 2012.
http://idcdocserv.com/236186E_HP

* Additional Notes: IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of ICT suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. The Capabilities score measures vendor product, go-to-market and business execution in the short-term. The Strategy score measures alignment of vendor strategies with customer requirements in a 3-5-year timeframe. Vendor market share is represented by the size of the circles. Vendor year-over-year growth rate relative to the given market is indicated by a plus, neutral or minus next to the vendor name.

КВАДРАНТ GARTNER (10.11.2012)

Категории: лидеры (Leaders), провидцы (Visionaries), претенденты (Challengers) и нишевые игроки (Niche Players).

Лидер	Amazon Web Services, Terremark, Savvis (CenturyLink), CSC, Dimension Data
Провидец	Tier 3, Rackspace, Virtustream
Претендент	Joyent, Bluelock, GoGrid
Нишевой Игрок	SoftLayer, OVH, Fujitsu, Dell

Макет облачной инфраструктуры

Система обработки и хранения данных в составе:

- 3-х серверов виртуализации (HP BL460)
- сервера управления (HP DL360)
- системы хранения данных (EMC CLARiiON)

Комплекс программного обеспечения управления и автоматизации администрирования виртуальных серверов:

- средства виртуализации (VMWare ESXi, VMWare View, vCenter)
- средства контроля и управления виртуальной инфраструктурой (HP CSA, Operations Orchestration, Server Automation)

Программное обеспечение для работы виртуальных машин

(WEB-серверы, СУБД, домен контроллер и др.)

Специализированные программные средства для обеспечения информационной безопасности в виртуальной среде:

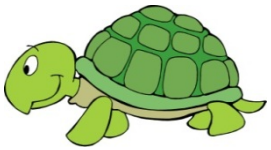
- централизованной антивирусной защиты
- централизованного контроля и управления ИБ, разграничение доступа, разделение полномочий и др.

Угрозы информационной безопасности в облаке

Атаки между виртуальными машинами

Спящие виртуальные машины

Разные уровни безопасности для данных



Обычный антивирус

Угрозы облачной среды

Первичный перечень угроз, сформированный ГУБиЗИ:

У1 -Отсутствие защиты гипервизора.

У2 -Отсутствие контроля действий пользователей и вносимых ими изменений в конфигурацию виртуальной среды.

У3 -Отсутствие требуемого уровня защиты виртуальных машин, долгое время находящихся в выключенном состоянии.

У4 -Несанкционированный сетевой доступ внутри виртуальной инфраструктуры

У5 -Получение несанкционированного доступа к системе управления виртуальной среды.

У6 -Несанкционированный доступ к виртуальным машинам.

У7 -Внедрение вредоносного ПО при работе пользователей на персональном виртуальном компьютере.

У8 -Несанкционированное изменение виртуальных машин в выключенном состоянии.

У9 -Угроза компрометации образов виртуальных машин.

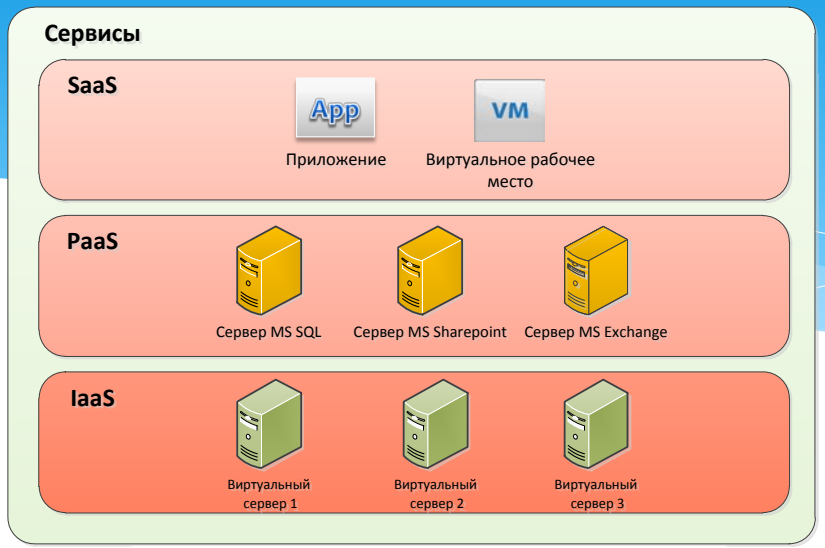
У10 - Угроза перегрузки вычислительных ресурсов при использовании стандартных средств защиты от вредоносного кода.

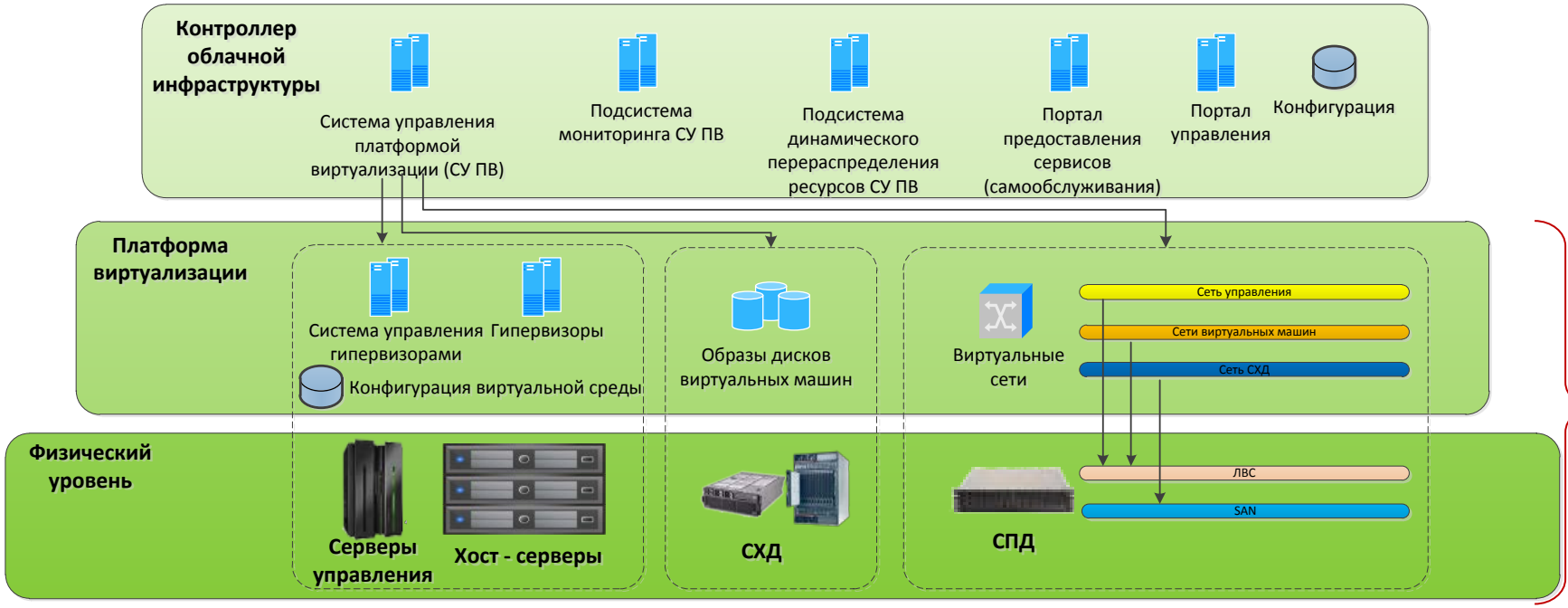
У11 -Отсутствие контроля целостности конфигурационных файлов ВРМ.

У12 -Отсутствие выделенного сегмента управления.

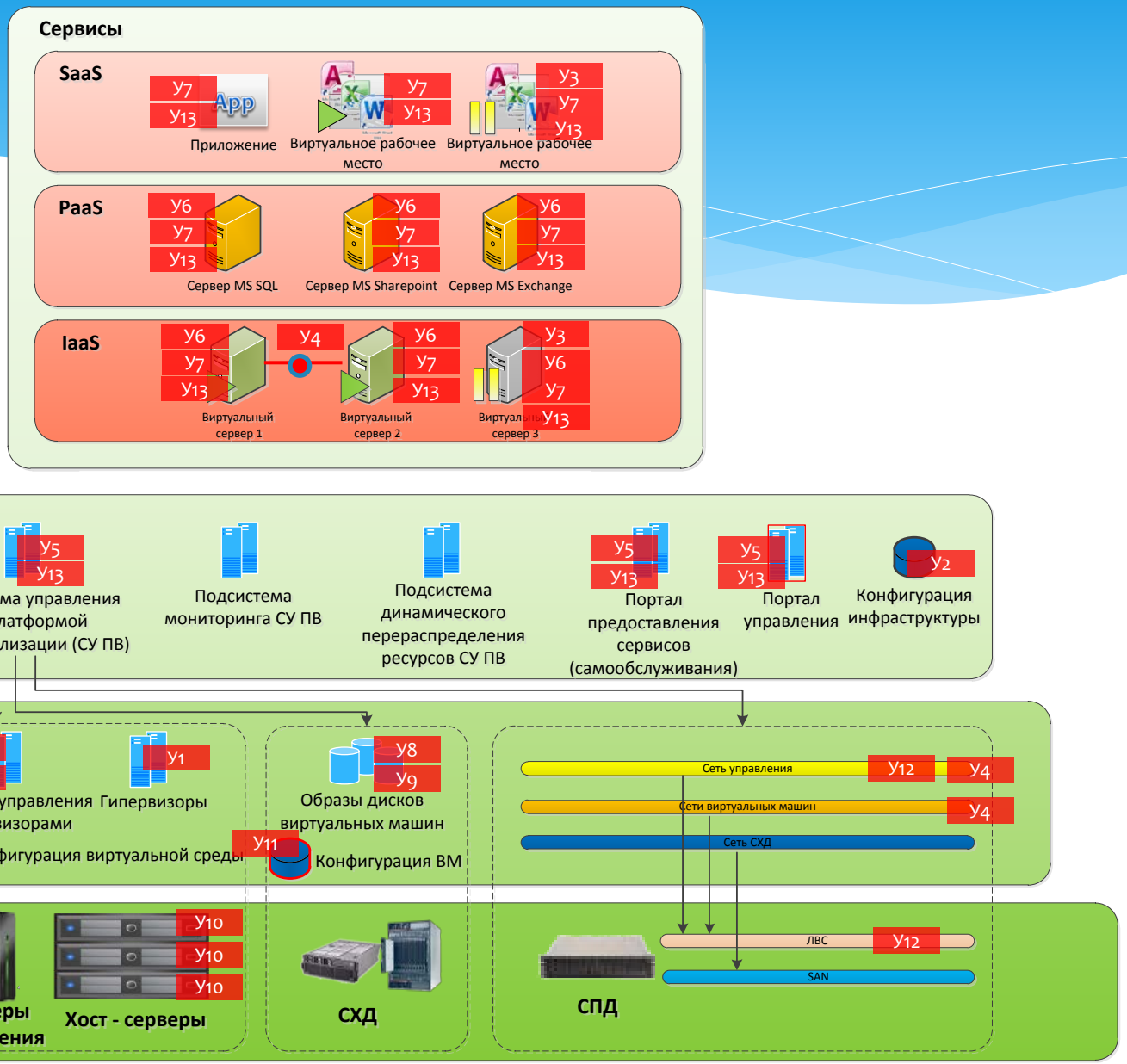
У13 -Отсутствие централизованной идентификации и аутентификации пользователей

Принципиальная схема облачной инфраструктуры





Угрозы облачной среды



Выбранные решения по информационной безопасности

- Отсутствие защиты гипервизора
- Отсутствие контроля действий пользователей и вносимых ими изменений в конфигурацию виртуальной среды
- Контроль целостности

HyTrust HTA

vGate

- Отсутствие требуемого уровня защиты виртуальных машин, долгое время находящихся в выключенном состоянии
- Отсутствие межсетевых экранов в виртуальной среде
- Опасность перегрузки системы при использовании стандартных средств защиты от вредоносного кода
- Защита от вредоносного кода
- Контроль целостности на уровне гипервизора
- Дедупликация антивирусных проверок

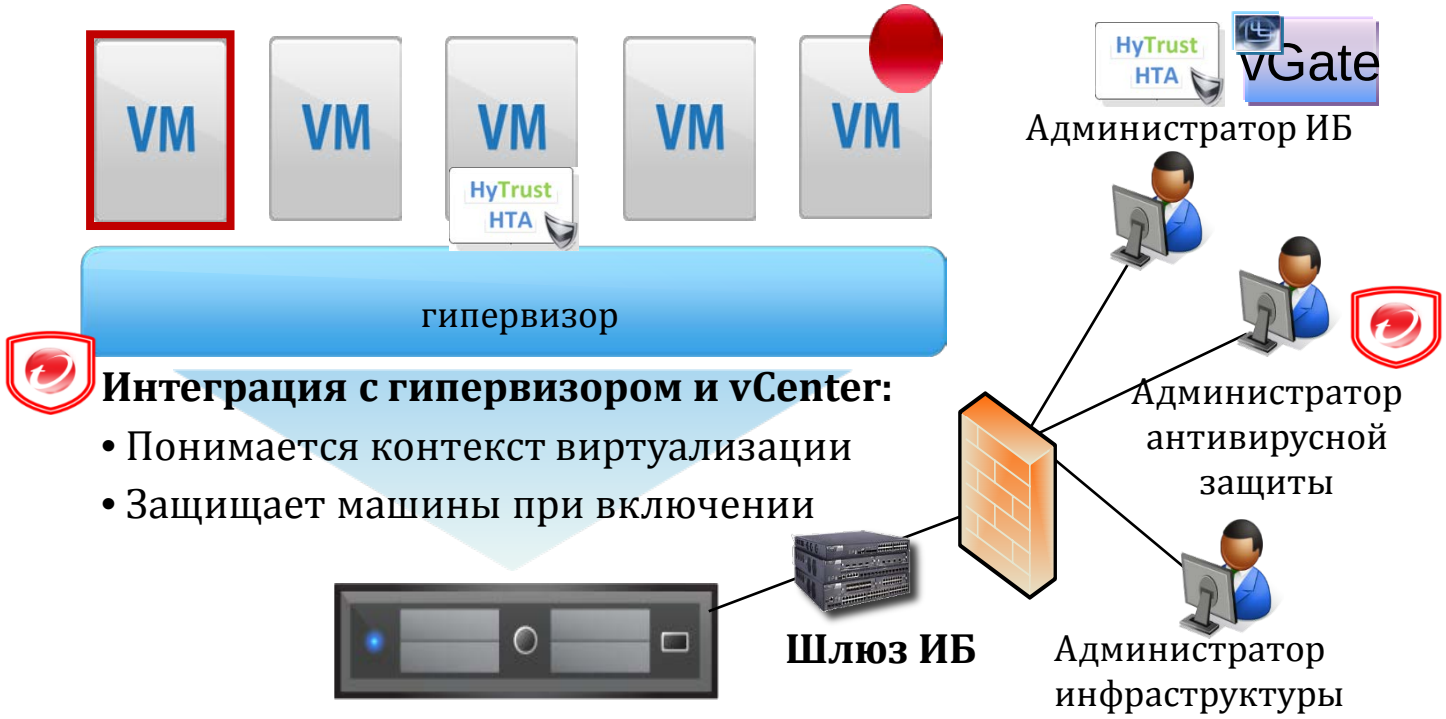
Trend Micro Deep Security

Касперский

Информационная безопасность макета облака

Virtual Appliance:
- AV, IDS/IPS, FW
- высокая эффективность
- управляемость

Агенты безопасности:
- Дополнительные модули защиты
- Мобильность для перемещения в облаке



Интеграция с гипервизором и vCenter:
- Понимается контекст виртуализации
- Защищает машины при включении

Выбранные решения по обеспечению информационной безопасности. Парирование угроз

Несанкционированный доступ к элементам виртуальной среды и файлам конфигурации

У1
У2
У5
У8
У9
У11

HyTrust HTA

vGate

ЕСК

У6
У13

Неавторизованный доступ

Внедрение вредоносного кода и несанкционированное сетевое взаимодействие

У3
У4
У7
У10
У12

Trend Micro Deep Security

Аппаратный межсетевой экран

У12

Решение «HyTrust - HTA»

«HyTrust HTA» позволяет:

- контролировать все соединения пользователей с виртуальной инфраструктурой
- интегрироваться с Microsoft Active Directory
- использовать RSA SecurID
- передавать привилегии администратора другой учетной записи на ограниченное время
- организовывать политики доступа с помощью меток
- централизованно хранить журналы событий
- обследовать хосты ESX / ESXi на предмет соблюдения требований безопасности (C.I.S., PCI DSS, VMware Best Practices, созданные вручную шаблоны)
- функционировать в режиме основного шлюза для серверов VMware ESX и VMware vCenter

Решение «Код безопасности - vGate»

ПО «vGate» обеспечивает:

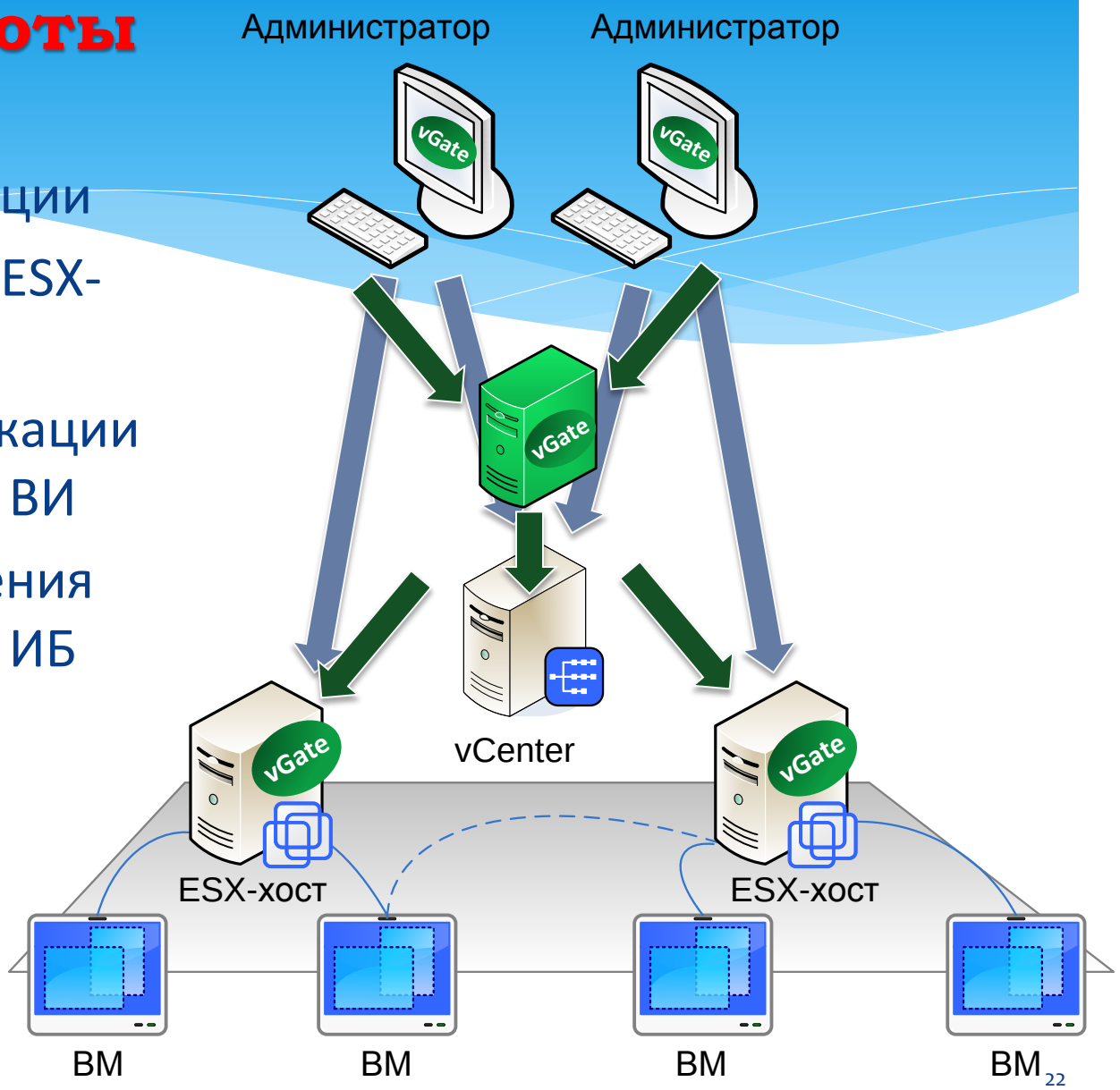
- усиленную аутентификацию администраторов виртуальной инфраструктуры и администраторов информационной безопасности
- мандатное управление доступом
- защиту ESX-серверов от НСД
- контроль целостности конфигурации виртуальных машин и доверенную загрузку
- регистрацию событий, связанных с информационной безопасностью
- контроль целостности и доверенную загрузку ESX-серверов
- контроль целостности и защита от НСД компонентов СЗИ
- централизованное управление и мониторинг

Сертификат ФСТЭК России (СВТ 5, НДВ 4) позволяет применять продукт в автоматизированных системах уровня защищенности до класса 1Г включительно и в информационных системах персональных данных (ИСПДн) до класса К1 включительно.

Сертификат ФСТЭК России (ТУ, НДВ2) позволяет применять продукт в автоматизированных системах уровня защищенности до класса 1Б включительно и в информационных системах персональных данных (ИСПДн) до класса К1 включительно.

Принцип работы

- Сервер авторизации
- Модули защиты ESX-серверов
- Агент аутентификации администратора ВИ
- Консоль управления администратора ИБ



Решение «Trend Micro - Deep Security»

Функции ПО Deep Security:

- защита виртуальных машин на уровне гипервизора
- защита виртуальных сред от вредоносных программ
- обнаружение и предотвращение вторжений
- контроль целостности
- защита веб-приложений
- управление сетевым доступом на уровне приложений
- межсетевое экранирование
- централизованный сбор журналов информационной безопасности

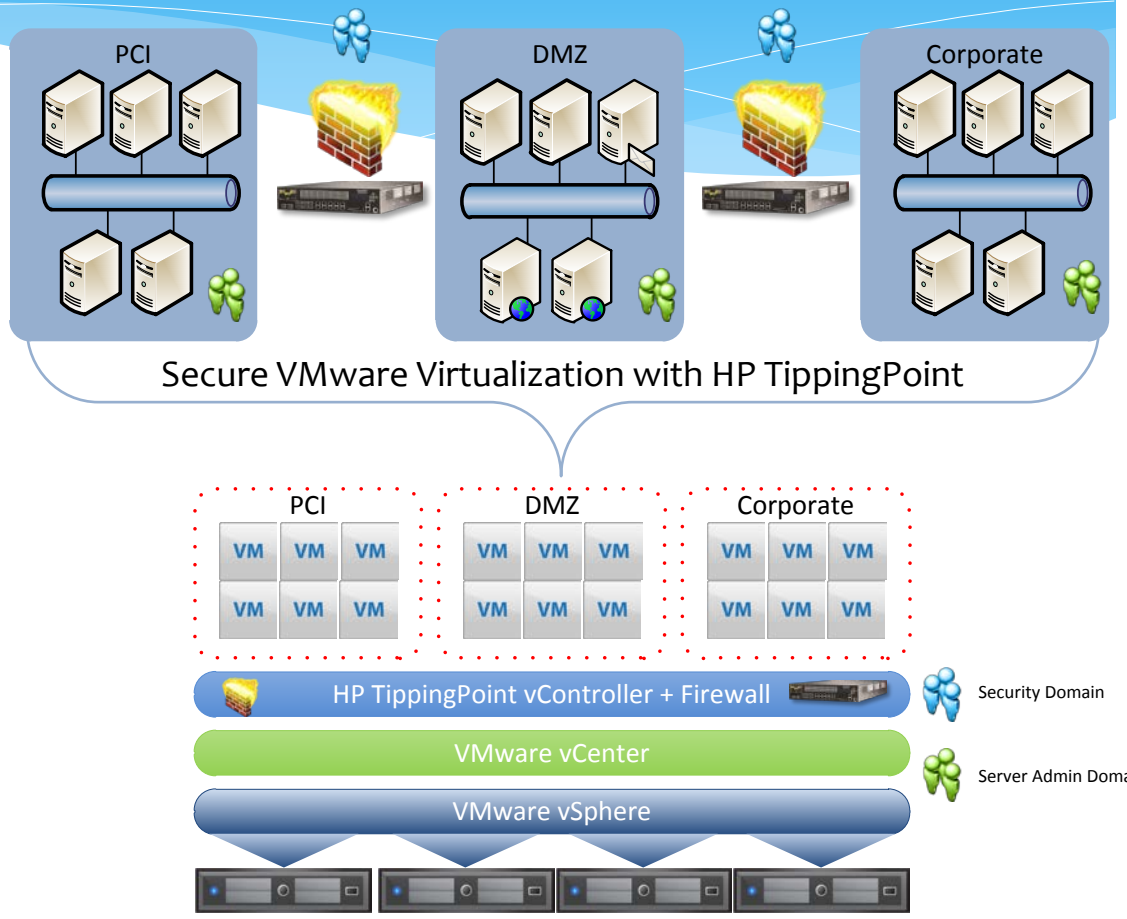
Сертификат ФСТЭК России (ТУ, НДВ4) позволяет применять продукт в автоматизированных системах уровня защищенности до класса 1Г включительно и в информационных системах персональных данных (ИСПДн) до класса К1 включительно.

Решение «Trend Micro - Deep Security»

ПО «Trend Micro Deep Security» является комплексной платформой реализации механизмов защиты информации на виртуальных серверах и рабочих станциях в составе «облачной» инфраструктуры

Межсетевое экранирование в виртуальной среде

- IPS protection для виртуальных сегментов
- Создание виртуальных сетевых сегментов
- Права определяются на основе правил для данного сегмента



Роли администраторов

Администратор облачной инфраструктуры

- управление виртуальной инфраструктурой
- управление процессом предоставления «облачных» сервисов

HP CSA **VMware vCenter** **ЕСК**

Администратор информационной безопасности (распределение прав доступа)

- управление правами доступа к элементам облачной среды
- контроль действий пользователей

HyTrust HTA **vGate** **ЕСК**

Администратор ИБ по управлению СЗ от ВВК и межсетевым взаимодействием

- управление политиками антивирусной защиты, сервисами безопасности
- контроль вирусной активности
- управление политиками межсетевого взаимодействия

Trend Micro Deep Security **Межсетевой экран**

Администратор сервисов (автоматизированных систем)

- управление конфигурацией сервисов
- предоставление сервисов пользователям

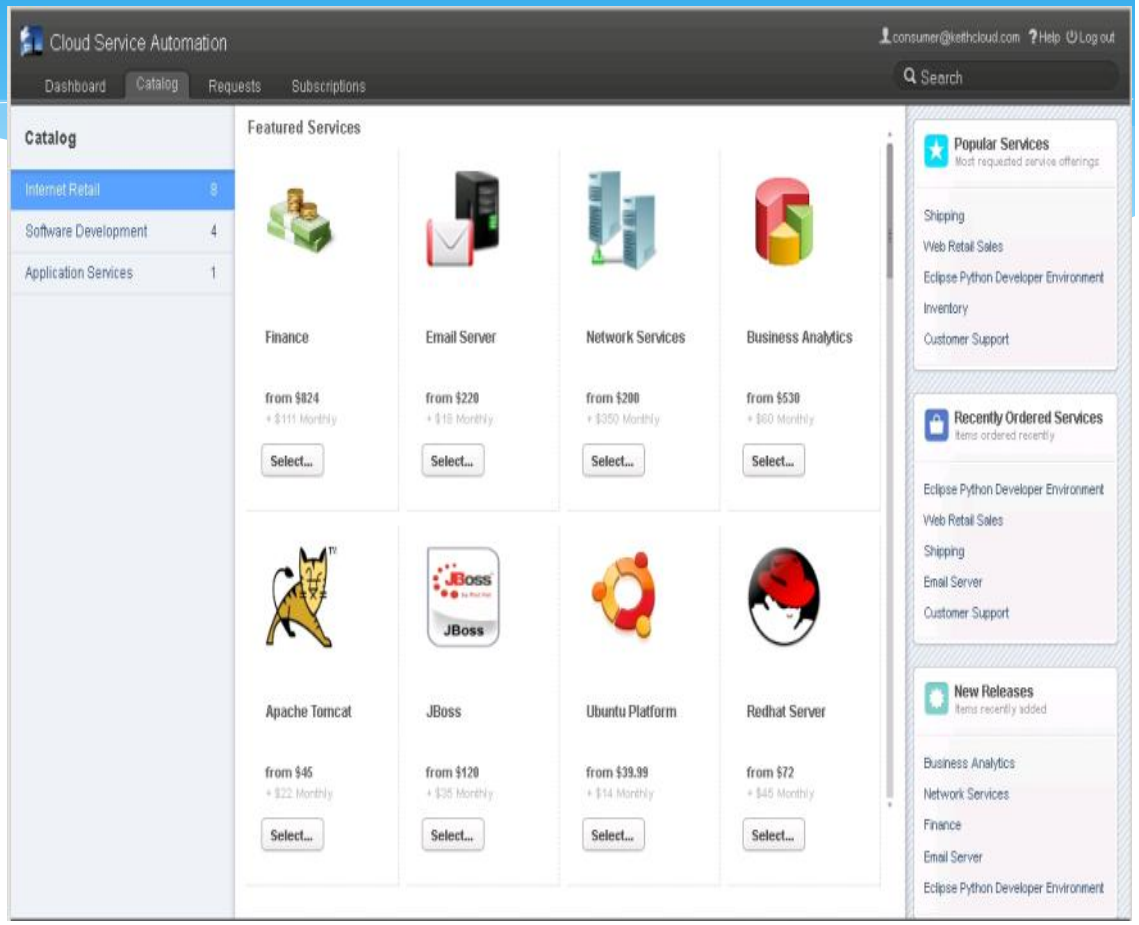
VMware View **HP Портал самообслуживания**

Пользователь

Портал пользователя

- Услуги
  - IaaS, PaaS
  - Внутренние или внешние ресурсы
  - Физическая и виртуальная инфраструктуры
  - Любые корпоративные услуги
- Каталог
  - Просмотр и поиск услуг
  - Подробная документация
  - Формирование цены
- Заказ
  - Конфигурация и заказ услуг
  - Доступ и изменение услуг
  - Расписание

- **Заказ услуг, доступ, модификация**



cloudsecurityalliance.org

Состав Безопасность как услуга:

- Управления идентификацией доступа
- Data Loss Prevention
- Web Security
- Email Security
- Оценка безопасности
- Вторжения (обнаружения, предотвращение)
- Информационная безопасность и Event Manager
- Шифрование
- Непрерывность бизнеса и аварийное восстановление
- Сетевая безопасность

Информационная безопасность как сервис

Что нужно делать:

- Проектировать виртуальную среду:
  - Принципы защиты: агентская защита, безагентская;
  - сетевая топология с учетом ИБ
  - размещение хранилищ данных и управление доступа к ним
  - характеристики каналов и производительность серверов
  - принципы управления системами
- Сформировать пул сервисов ИБ
- Не забыть про аутентификацию на всех уровнях:
  - Гипервизор, среда управления, хранилище, сетевые устройства, в том числе виртуальные, операционные системы, СУБД, приложения, среды автоматизации развертывания и среды обслуживания облачной инфраструктуры
- Выбрать средства защиты соразмерные рискам
- Привязать сервисы ИБ к приложениям

Составные части сервиса ИБ на макете

Что реализовано:

- Базовый уровень: HyTrast, vGate, DeepSecurity, Kaspersky
- Единый мониторинг – ArcSight
- Авторизация – RSA, AD
- Контроль целостности – DeepSecurity

Что требуется :

- Добавить интегрированное решение «внешний-внутренний МСЭ»
- Привязать приложения к сервисам ИБ

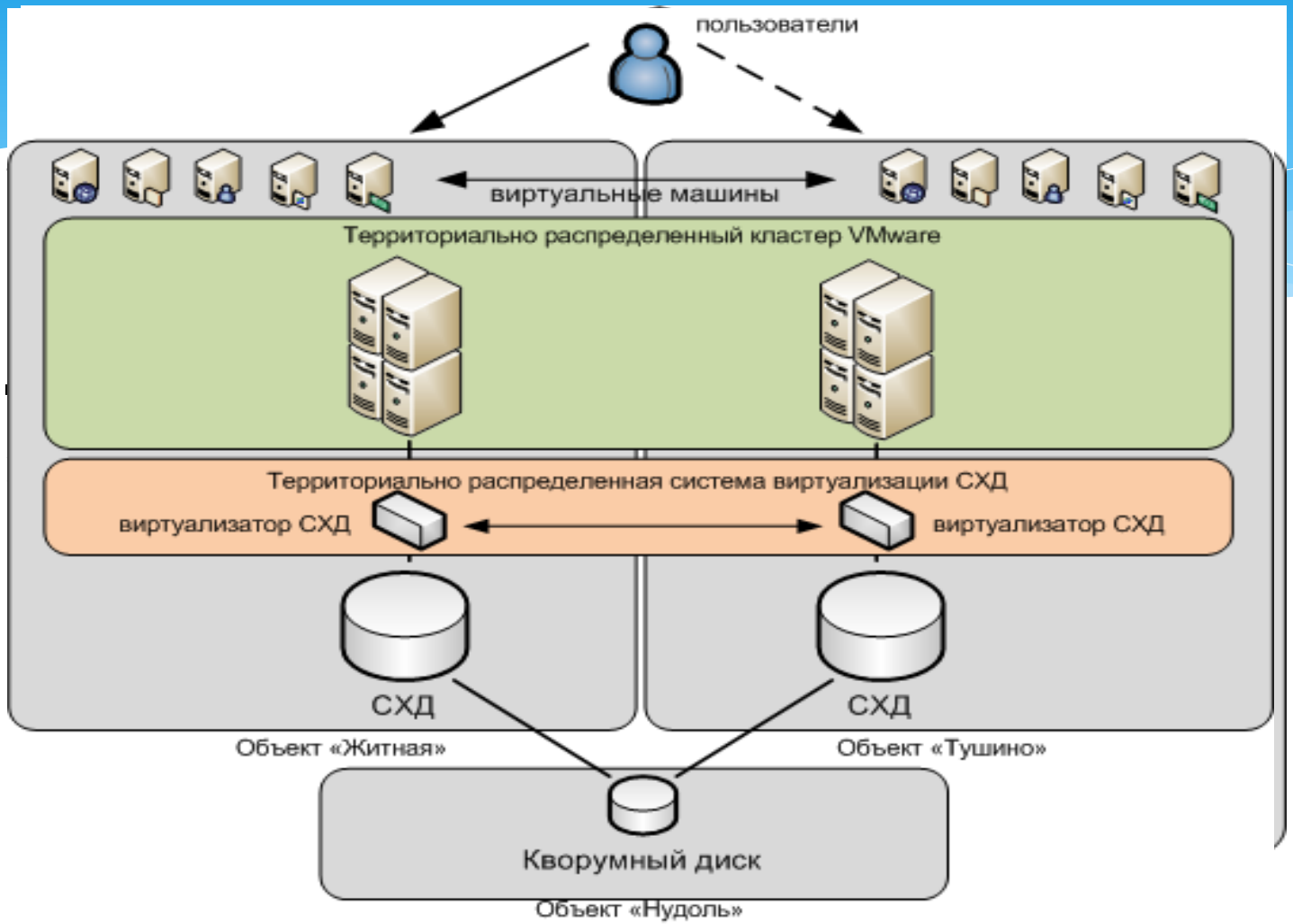
Преимущества:

- Высокая степень зрелости решений (составных частей)
- Соответствие идеологии SIEM

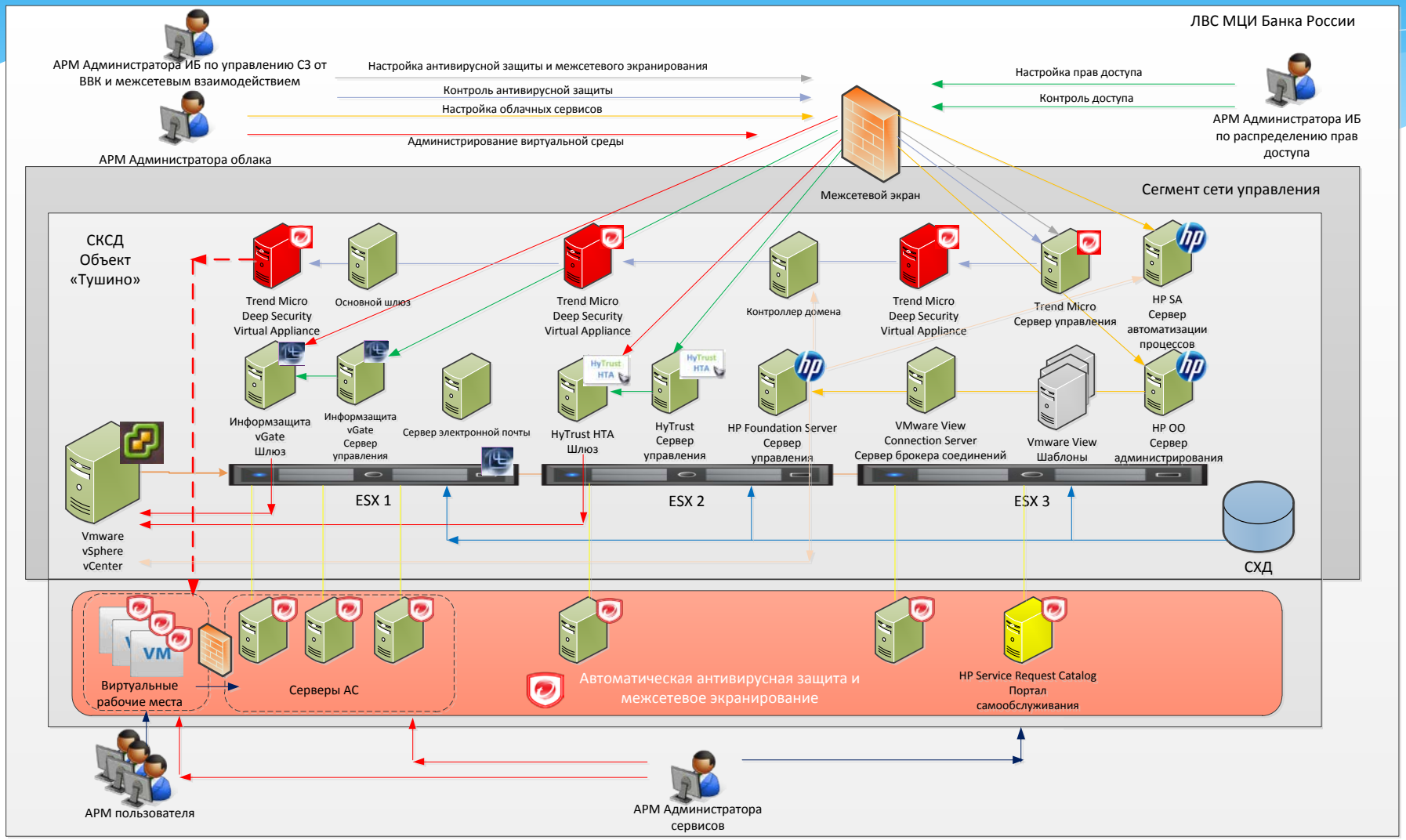
Что требуется для перехода к сервису ИБ

- **Проект виртуальной инфраструктуры с требованиями по ИБ приложений**
- **Перераспределить роли администраторов:**
  - Усилить роль администраторов ИБ, дав им инструмент (консоль) контроля
  - Администратор облачной инфраструктуры, администратор ИБ облачной инфраструктуры, администратор защиты виртуальных машин – равноправные участники бизнес процесса
  - Администратор ИБ облачной инфраструктуры должен обладать высокой квалификацией, позволяющей разбирать инциденты ИБ
- **Использовать зрелые решения по ИБ**
- **Выработать требования по безопасности облачных виртуальных инфраструктур**

Существующая реализация макета ЦОД для частного облака

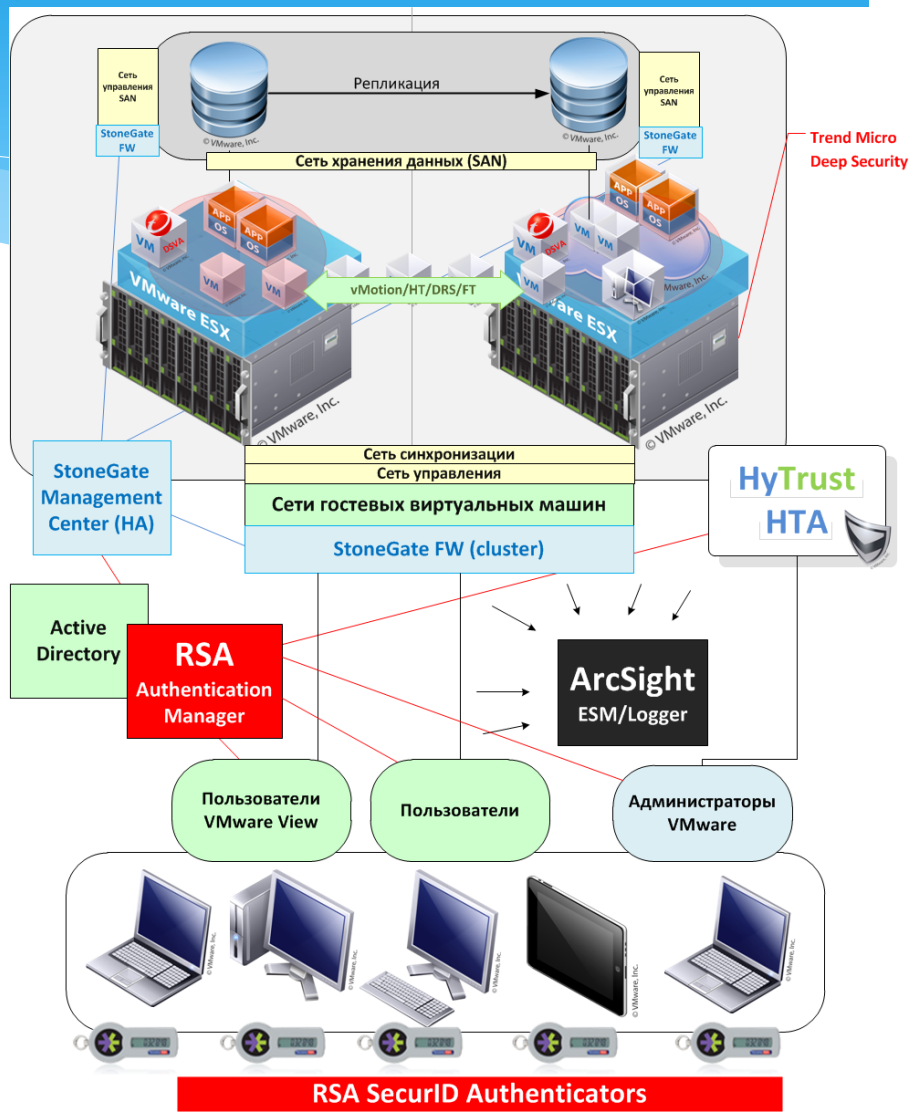


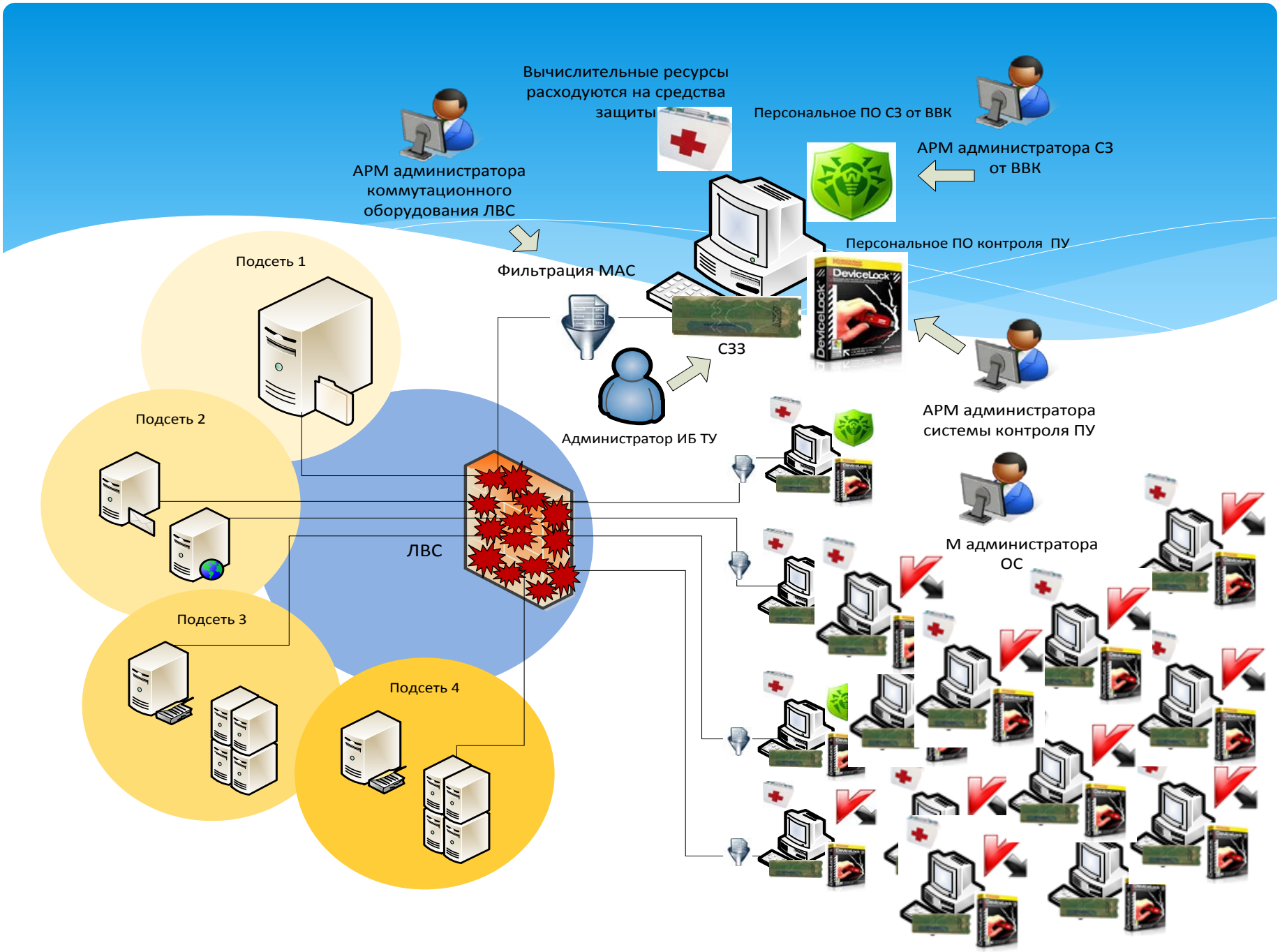
Макет облачной инфраструктуры

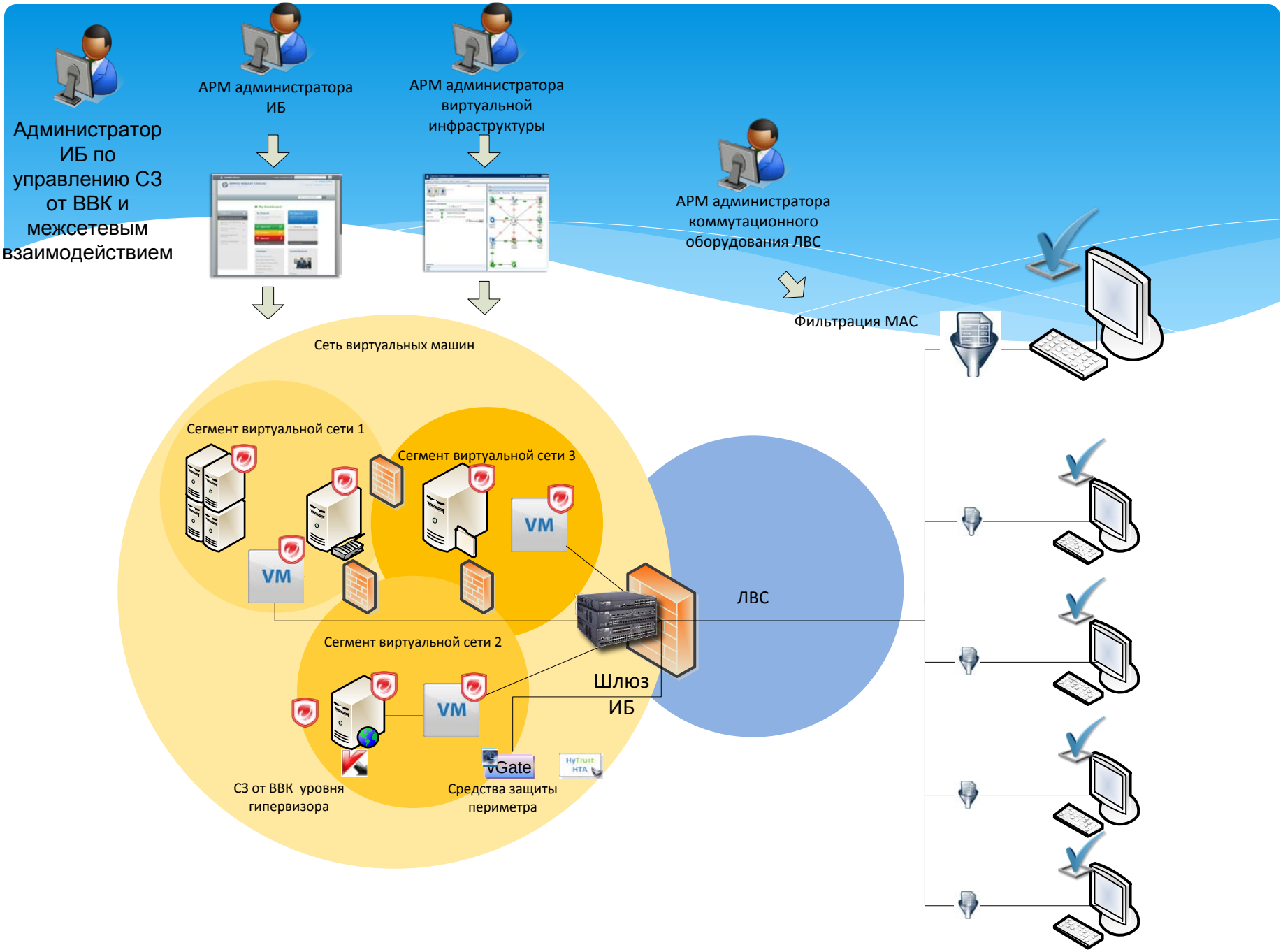


Комплексное перспективное решение по защите

- Управление доступом к среде виртуализации
  - **HyTrust, vGate**
- Базовая защита виртуальной среды
  - **TrendMicro Deep Security, Kaspersky**
- Защищенная сетевая среда
  - **Cisco Nexus/ VSG / ASA 1000v, TippingPoint, StoneGate FW**
- Унифицированная среда усиленной аутентификации
  - **RSA SecurID**
- Управление инцидентами ИБ в виртуальной среде
  - **Продукты HP ArcSight**
- Периметр виртуальной среды
  - **Продукты StoneSoft, TippingPoint**




Вычислительные ресурсы расходуются на средства защиты
Персональное ПО СЗ от ВВК
АРМ администратора СЗ от ВВК
АРМ администратора коммутационного оборудования ЛВС
Фильтрация MAC
Персональное ПО контроля ПУ
DeviceLock
СЗЗ
Администратор ИБ ТУ
АРМ администратора системы контроля ПУ
М администратора ОС
Подсеть 1
Подсеть 2
Подсеть 3
Подсеть 4
ЛВС


Администратор ИБ по управлению СЗ от ВВК и межсетевым взаимодействием
АРМ администратора ИБ
АРМ администратора виртуальной инфраструктуры
АРМ администратора коммутационного оборудования ЛВС
Фильтрация MAC
Сеть виртуальных машин
Сегмент виртуальной сети 1
Сегмент виртуальной сети 3
Сегмент виртуальной сети 2
VM
VM
VM
ЛВС
Шлюз ИБ
vGate
СЗ от ВВК уровня гипервизора
Средства защиты периметра

Constant compromise does not mean constant loss

Спасибо за внимание!

Александр Шибаев
sav@cbr.ru