

Особенности применения СКЗИ в средах виртуализации

Николай Смирнов,
директор по продуктам, ИнфоТеКС

Постановка задачи

ДАНО:

СКЗИ, соответствующее требованиям высоких (КС2+) классов безопасности, имеют исполнение в виде Программно-Аппаратных комплексов

Программно-Аппаратный комплекс это:

- Вычислительная платформа общего или специального назначения
- Элементы доверия платформы
- Доверенная среда функционирования СКЗИ

Постановка задачи

Проблема:

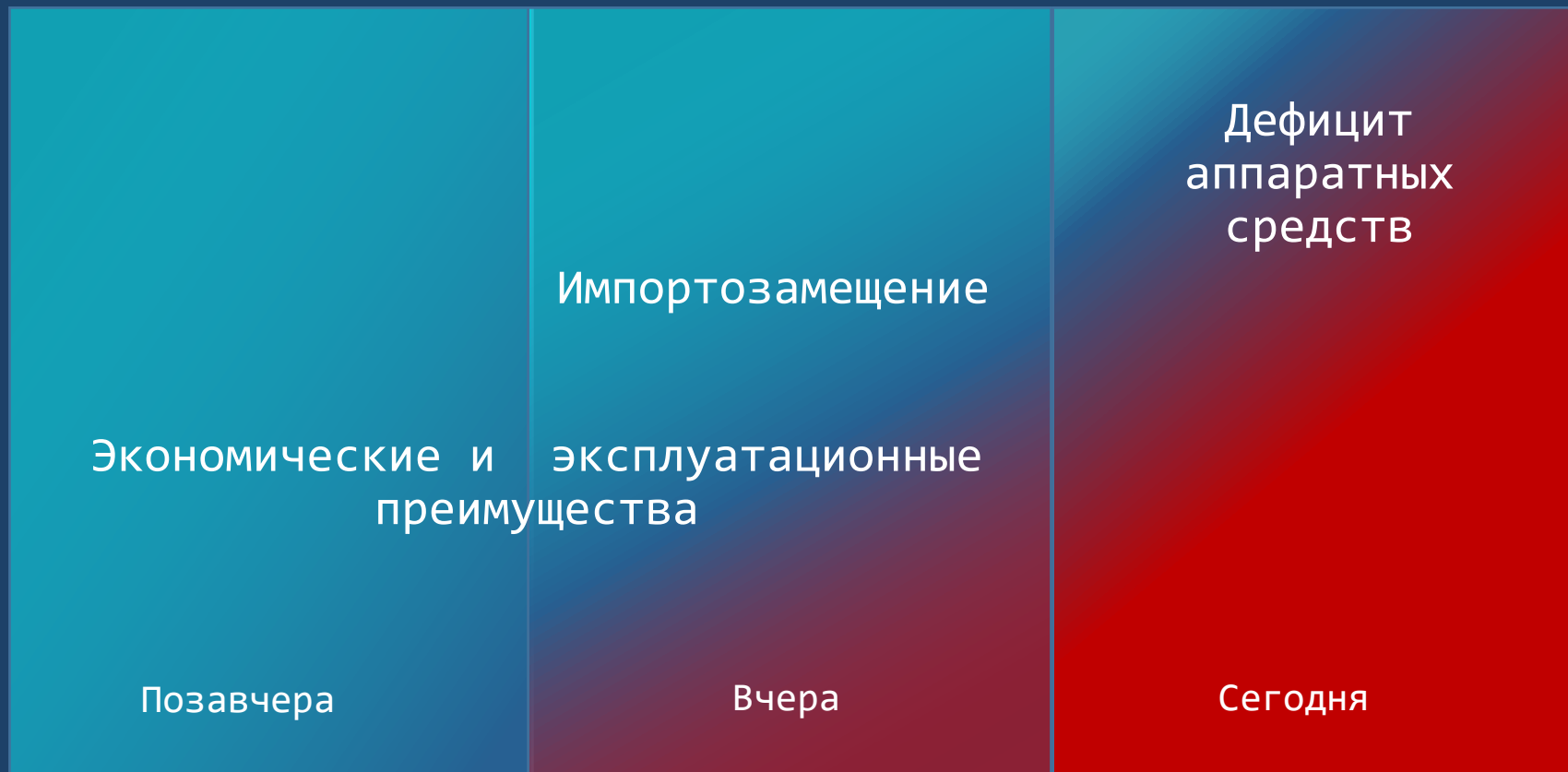
- Неопределенности импортозамещения
- Дефицит микроэлектроники
- Геополитические активности (разрушение цепочек поставок)

Что делать?

Кто виноват?

Системы виртуализации

Потребность в системах виртуализации



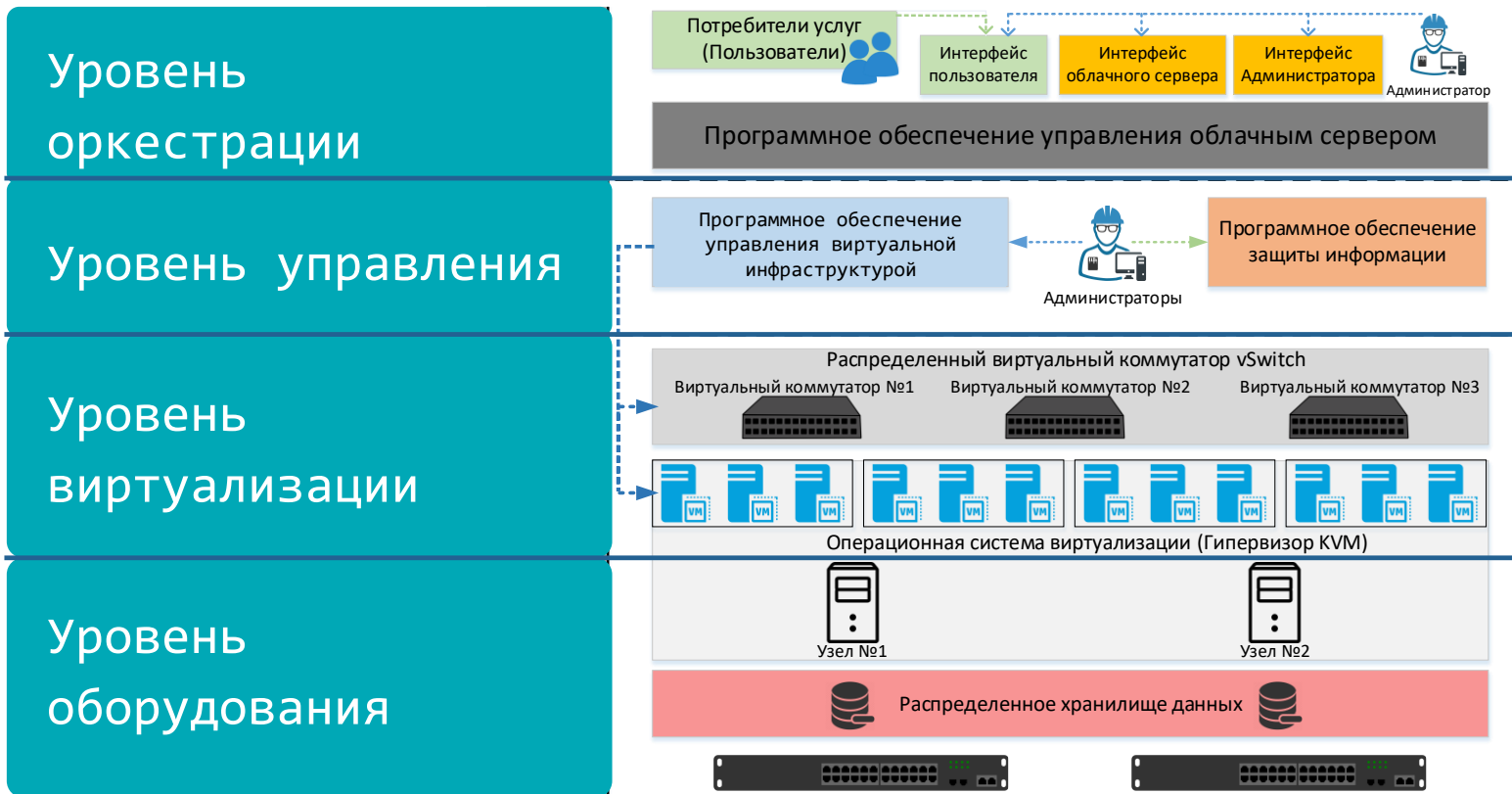
Игроки рынка систем виртуализации

- VMware
 - Oracle
 - Microsoft
 - Open Source
- «Р-Виртуализация»
 - «Брест»
 - «Sharx»
 - «ХОСТ»
 - «Zvirt»
 - «ROSA»
 - «СКАЛА-Р»
 - «ТИОНИКС»
 - «Горизонт-ВС»

Вчера

Сегодня

Типовая архитектура



Нормативные документы

- ГОСТ Р 56938-2016
- ТК 362 Проект стандарта по защите в облачных средах
- Рекомендации Банка России РС БР ИББС-2.8-2015
- Приказы ФСТЭК России 17, 21, 31 и чуть-чуть 239

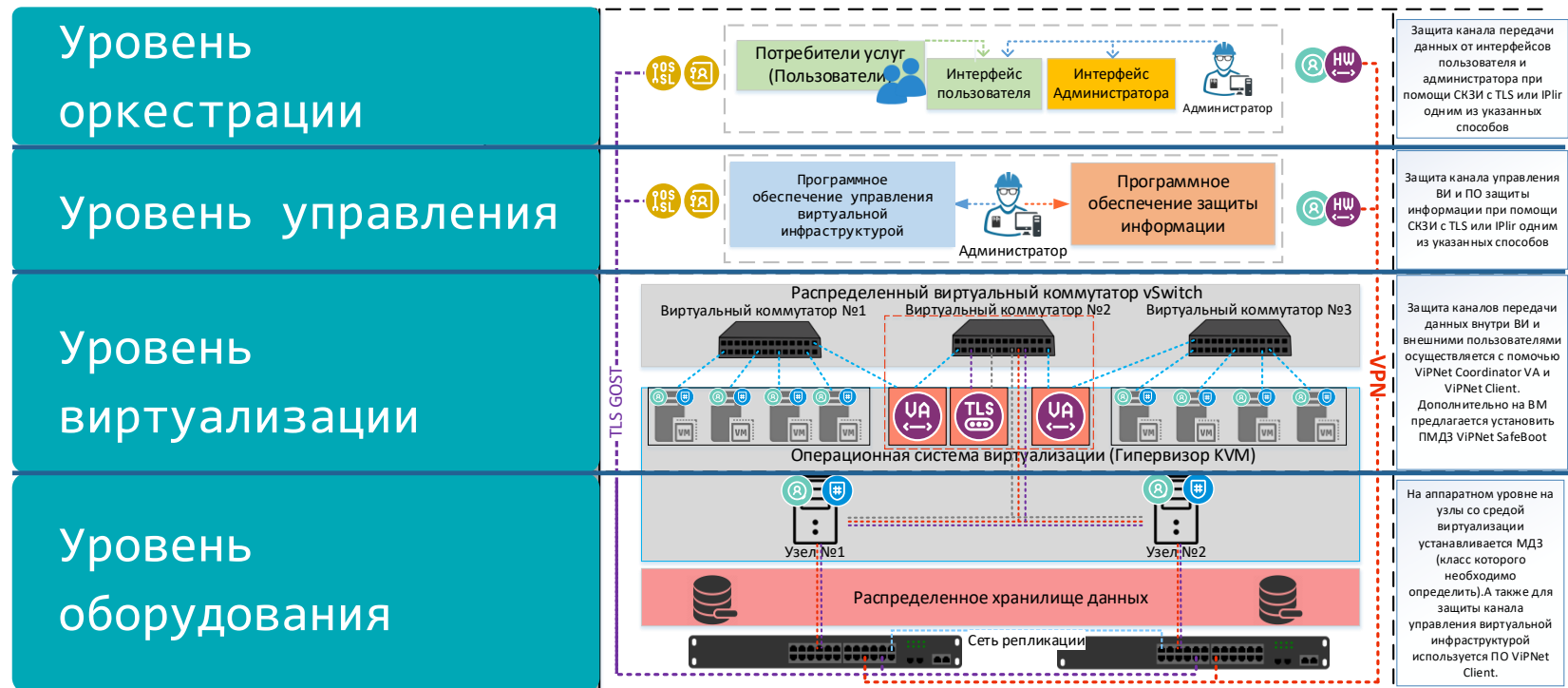
- угрозы атаки на активное и/или пассивное виртуальное и/или физическое сетевое оборудование из физической и/или виртуальной сети
- угрозы атаки на виртуальные каналы передачи информации
- угрозы атаки на гипервизор из виртуальной машины и/или физической сети
- угрозы атаки на защищаемые виртуальные устройства из виртуальной и/или физической сети
- угрозы атаки на защищаемые виртуальные машины из виртуальной и/или физической сети
- угрозы атаки на систему хранения данных из виртуальной и/или физической сети
- угрозы выхода процесса за пределы виртуальной машины
- угрозы несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
- угрозы нарушения изоляции пользовательских данных внутри виртуальной машины
- угрозы нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
- угрозы перехвата управления гипервизором
- угрозы перехвата управления средой виртуализации
- [...]

Меры

- Идентификация и аутентификация (ЗСВ.1)
- Управление доступом (ЗСВ.2)
- Регистрация событий ИБ (ЗСВ.3)
- Управление потоками информации между компонентами ВИ (ЗСВ.4)
- Доверенная загрузка (ЗСВ.5)
- Управление перемещением ВМ и обрабатываемых на них данных (ЗСВ.6)
- Контроль целостности (ЗСВ.7)
- Резервное копирование данных (ЗСВ.8)
- Антивирусная защита (ЗСВ.9)
- Сегментирование виртуальной инфраструктуры (ЗСВ.10)

Гипотеза

Гипотеза



- канал управления ВИ, защищаемый при помощи TLS GOST
- канал управления ВИ, защищаемый при помощи VPN
- канал передачи данных внутри ВИ, защищаемый при помощи VPN
- открытый канал управления ВИ, после расшифровки TLS Gateway
- ПО, обеспечивающее доверенную загрузку ВМ и Хоста, класс определяется отдельно

- ПО VIP Net Client
- VIP Net TLS Gateway VA
- VIP Net Coordinator VA
- VIP Net Coordinator HW

- ПО VIP Net OSSL
- ПО VIP Net PKI Client

Результат

Результаты проверки гипотезы

- Основные положения согласованы
 - Определена ролевая модель для доверенной ВИ
 - Определен список требований к уровню виртуализации
 - Определен список требований к узлу виртуальной инфраструктуры в комплексе
 - Определена модель доверенной загрузки комплекса с контролем целостности

The background of the slide is a photograph of a server room with rows of server racks. Overlaid on this image are various semi-transparent digital graphics: a large globe on the right, several bar charts and line graphs, and two circular progress indicators. The left indicator shows '72%' and the right one shows '82%'. The overall color scheme is light blue and white, giving it a high-tech, data-driven appearance.

Что дальше?

Будущее

- Доказательство теоремы существования
- Завершение согласования концепции
- Решение задачи доверия в комплексе*



Обсуждение,
вопросы и ответы