# «Технологическое управление в защищенных центрах обработки данных»

**Запольских Сергей Владимирович**
Кандидат технических наук
Руководитель департамента разработки АСЗИ
АО «ФИНТЕХ»

# Основные задачи технологического управления в защищенных ЦОД

- Применение порталов технологического управления в ЦОД для автоматизации деятельности администраторов информационной безопасности и системы
- Применение руководящих указаний по конструированию, определяющих регламенты, форматы и протоколы технологического управления. Разработка на их основе отраслевых и общероссийских стандартов
- Применение репозитория доверенного ПО: дистрибутивы ПО, контейнеры и образы ВМ с ПО, инфраструктурные и функциональные сервисы (клиент-серверное ПО) в унифицированном формате
- Мониторинг состояния технических средств и программного обеспечения
- Автоматизация управления средствами защиты информации от НСД
- Автоматизация управления конфигурациями ЦОД: развертывание требуемой топологии физических и виртуальных хостов, установка ОС и ПО (включая СКЗИ); обновление ПО на физических и виртуальных хостах; управление режимами работы ЦОД (боевой/технологический)
- Интеграция средств криптографической защиты информации в среду виртуализации
- Интеграция со средствами администрирования частных виртуальных сетей
- Интеграция со средствами антивирусной защиты
- Интеграция со средствами обнаружения атак (СОА), ГосСОПКА
- Обеспечение кроссплатформенности в части: операционных систем; среды виртуализации; аппаратных средств

# Архитектура портала технологического управления

Управление пользователями.
Управление правами по работе с внешними носителями информации.
Разработка правил разграничения доступа, генерация и применение политик безопасности.
Управление подсистемами:
- идентификации и аутентификации;
- контроля целостности;
- замкнутой программной среды;
- регистрации событий безопасности;
- антивирусной защиты;
- управления доступом;
- контроля внешних устройств;
- печати;
- самотестирования.

Мониторинг событий безопасности.

Контроль разрешенных клиент-серверных TCP/HTTP-соединений на основе данных о доступе пользователей к сервисам

Применение шаблонов и моделей оценки состояния технических и программных средств (ТС и ПО), программно-аппаратных комплексов (ПАК), автоматизированных и информационных систем (АИС).
Мониторинг состоянии АИС, ПАК, ТС и ПО

Ведение IP-плана, подсетей, частных виртуальных сетей.
Подготовка данных для сценариев управления конфигурациями.
Управление конфигурациями в ЦОД и на удаленных объектах:
- развертывание ПО (установка, обновление, удаление);
- развертывание ВМ (с гостевыми ОС) и контейнеров с ПО;
- развертывание частных виртуальных сетей, настройка СКЗИ;
- настройка СЗИ от НСД;
- установка и настройка клиентов СОА, АВЗ

Дистрибутивы ПО, образы ВМ и контейнеров с ПО, метаданные инфраструктурных и функциональных сервисов (шаблоны хостов, ссылки на дистрибутивы ПО, образы ВМ и контейнера с ПО, шаблоны сценариев управления и политик безопасности)

Инвентаризация АИС, ПАК и технических средств.
Ведение схем и таблиц подключений ТС

**Портал технологического управления**

- **Сервер безопасности**
- **Сервер управления доступом к сервисам**
- **Сервер контроля и диагностирования**
- **Сервер управления конфигурациями**
- **Репозитории ПО**
- **Подсистема инвентаризации**

**Сервер управления доступом (IPA)**
**Сервер антивирусной защиты**
**Сервер СОА**
**Система управления ViPNet Prime**

**Физический/виртуальный хост**
Диспетчер агента безопасности
Клиент СУДС

**Сервер контроля и управления функционированием (zabbix, …)**

**Система управления конфигурациями (ansible, …)**
**Менеджер среды виртуализации (ovirt, proxmox, opennebula, openstack)**
**Менеджер контейнеризации (podman, docker)**

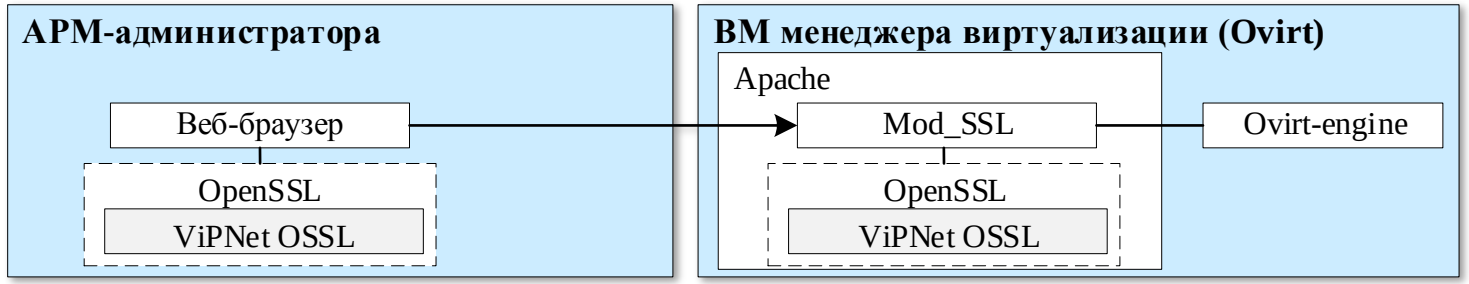
**Физические/ виртуальные хосты**

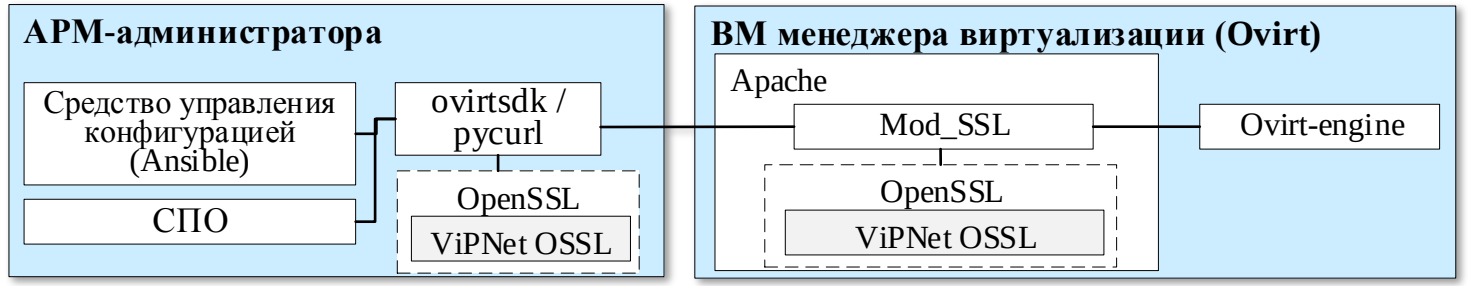
**Защищенная операционная система (подсистемы защиты информации)**
- идентификация и аутентификация
- контроль целостности
- замкнутая программная среда
- регистрация событий безопасности
- антивирусная защиты
- управление доступом
- контроль внешних устройств
- печать
- самотестирование

**Аппаратная платформа (Intel, Эльбрус и т.п.)**

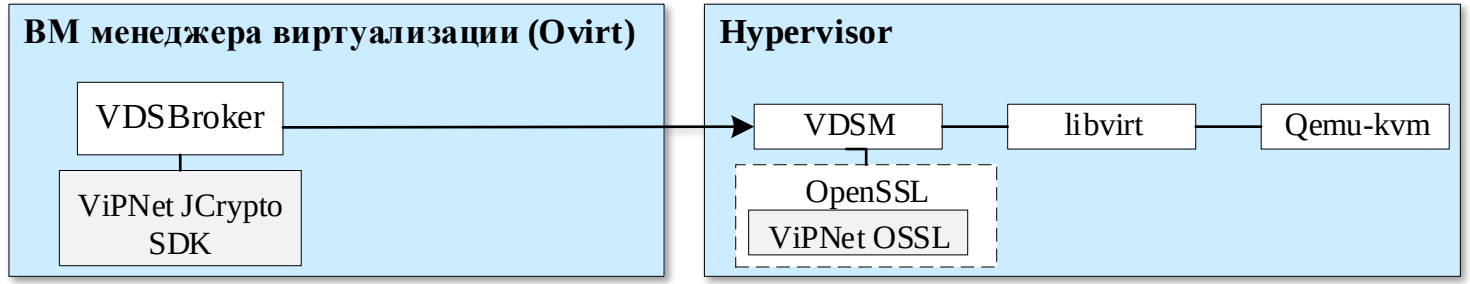
# Задачи интеграции СКЗИ в среду виртуализации ЗОС «СинтезМ»

**1.** Защита команд управления при обращении к веб-порталам менеджера ВМ, в том числе к API

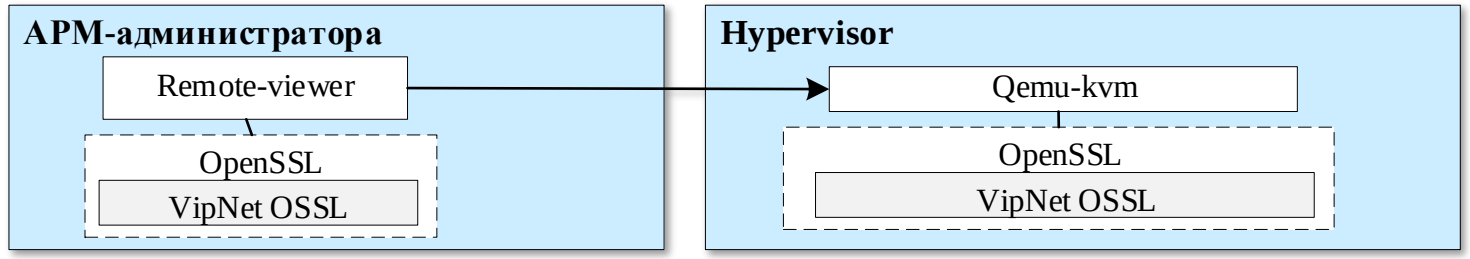


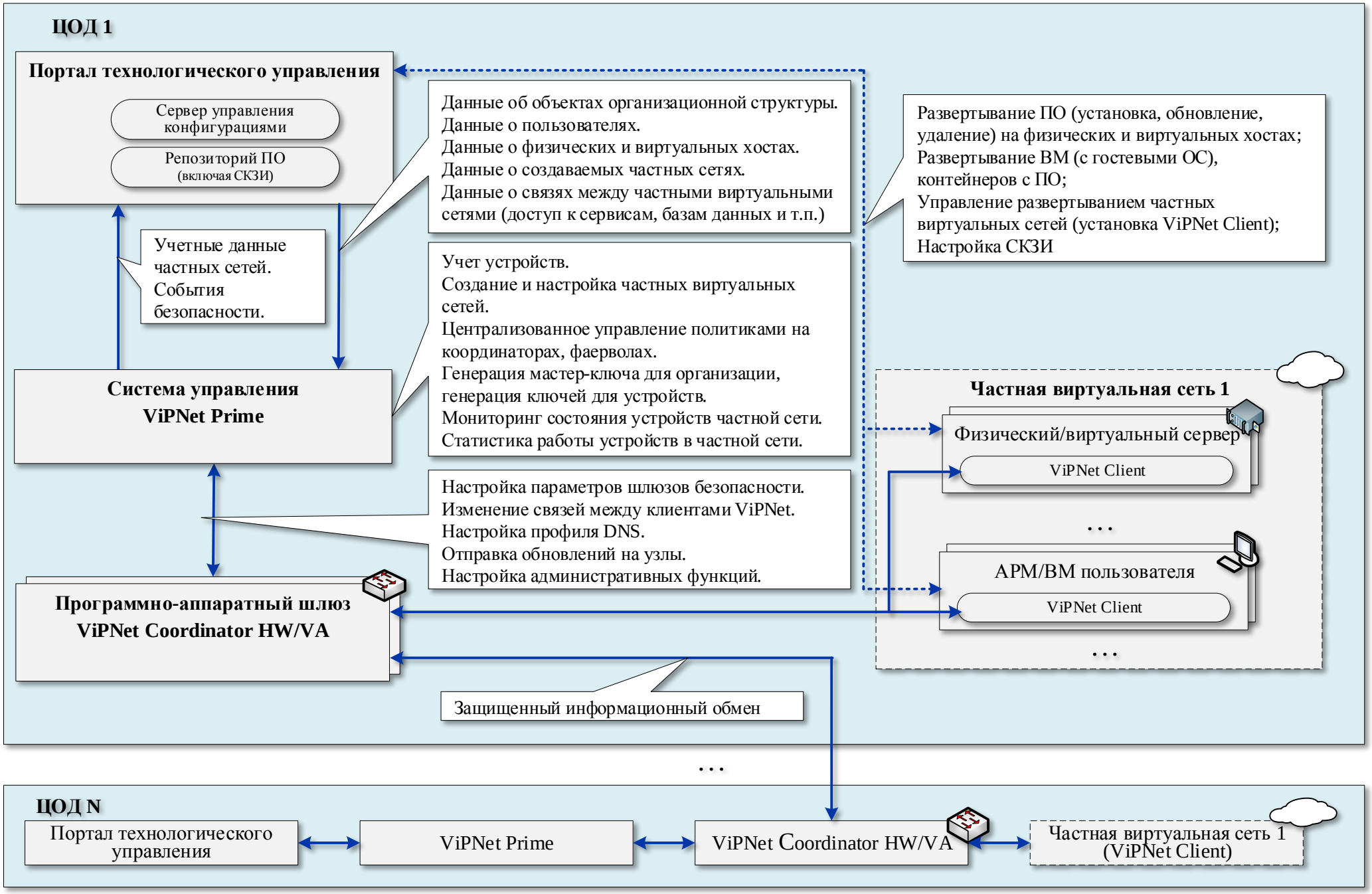

**2.** Взаимная идентификация гипервизора и менеджера ВМ в рамках создания соединения для передачи команд управления от менеджера ВМ гипервизору



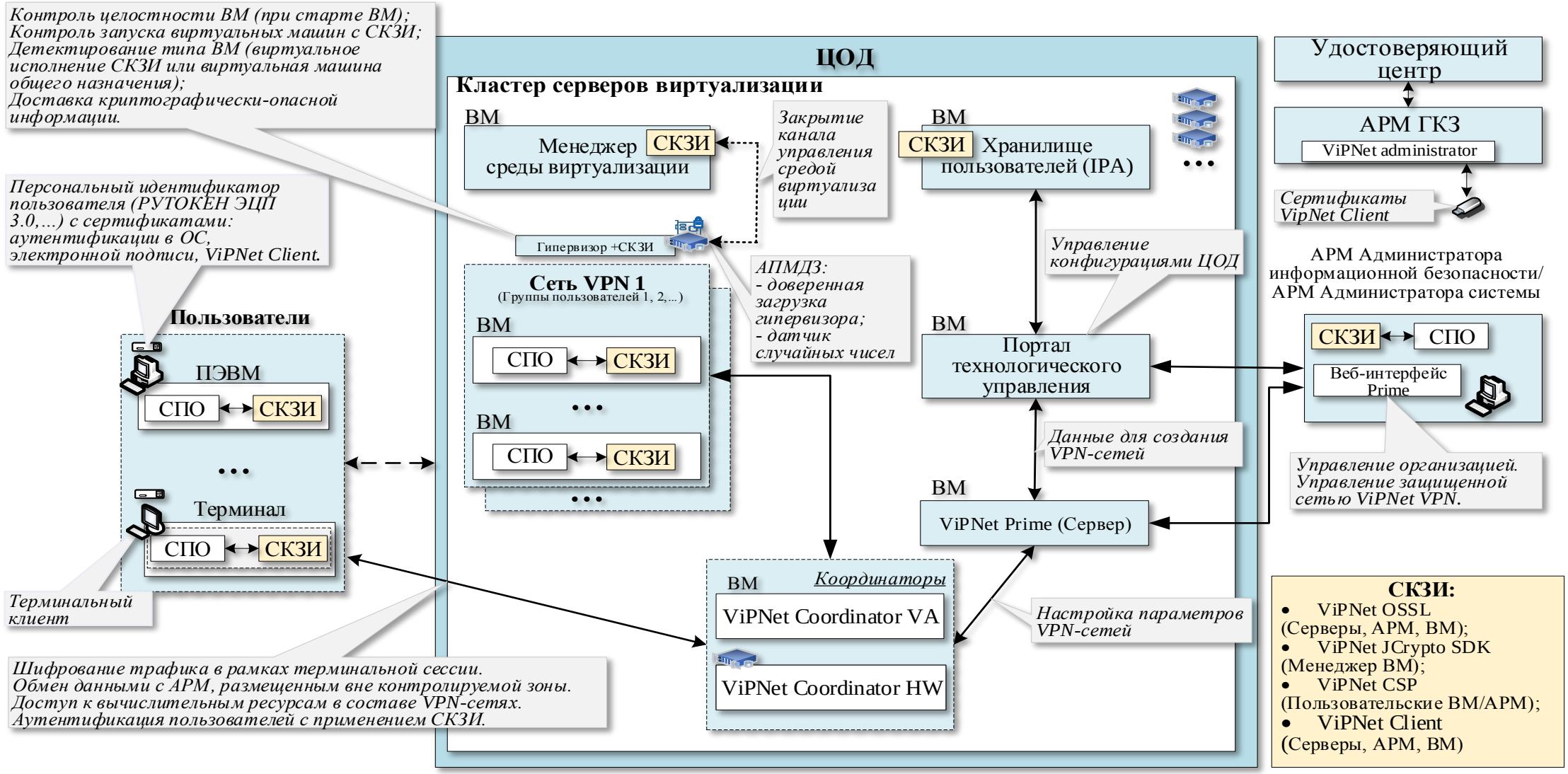

**3.** Защита каналов протокола spice при подключении к ВМ



# Интеграция портала технологического управления с ViPNet Prime



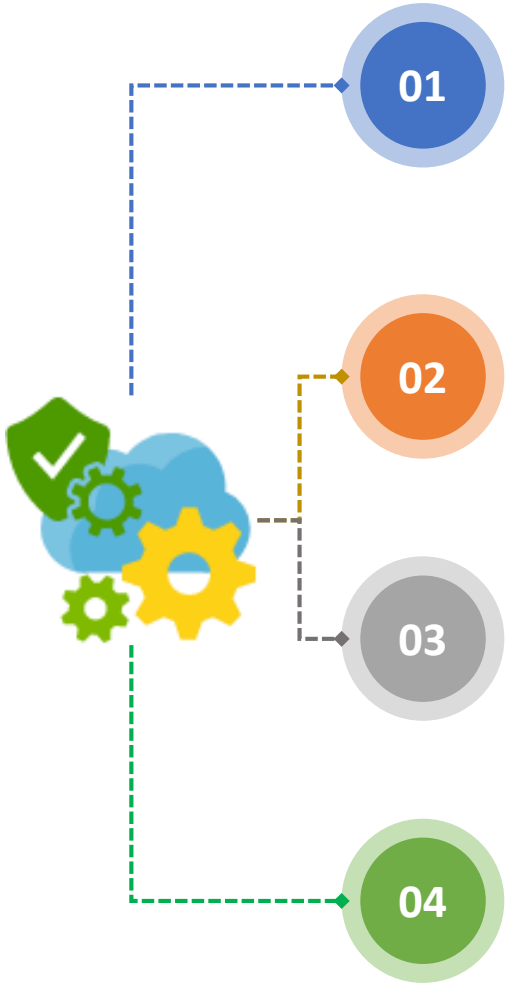
# Применение частных виртуальных сетей в ЦОД




**Варианты применения СКЗИ ViPNet в среде виртуализации:**

1. При информационном обмене между АРМ-Сервер, ЦОД-ЦОД (в местах отсутствия возможности обеспечения контролируемой зоны).
2. При изоляции вычислительных ресурсов групп пользователей посредством применения VPN-сетей.
3. При доступе пользователей к вычислительным ресурсам за счет доступа к определенным VPN-Сетям.
4. При аутентификации пользователей за счет применения СКЗИ.

# Требования к встраиванию СКЗИ в среду виртуализации




**Встраивание СКЗИ в менеджер виртуализации для обеспечения защищенного:**

- доступа к интерфейсам управления;
- управления/мониторинга службами среды виртуализации (агенты менеджера виртуализации)

**Встраивание СКЗИ в гипервизор для обеспечения защищенного:**

- взаимодействия служб среды виртуализации (агенты менеджера виртуализации) с системой виртуализации (QEMU) с использованием методов библиотеки libvirt;
- взаимодействия служб среды виртуализации (агенты менеджера виртуализации) с менеджером ВМ

**Встраивание СКЗИ в клиент удаленного доступа для обеспечения защищенного доступа к ВМ**

**Интеграция со «Службой обеспечения СКЗИ»:**

- обработки очередей запросов по принципу FIFO;
- обслуживания запросов от виртуальных СКЗИ, запущенных в разных ВМ (через Клиент Службы обеспечения СКЗИ) в рамках отдельных процессов;
- реализации интерфейса взаимодействия с ФДСЧ/АПМДЗ;
- обращения к VDSM для блокировки механизма клонирования/миграции;
- возврата «Клиенту Службы обеспечения СКЗИ» результата попытки блокировки механизма клонирования/миграции для заданной ВМ

ФИНТЕХ

Акционерное общество

# Благодарю за внимание!

Узнайте больше
www.sintezos.ru