Требования по безопасности облачных вычислений и сред виртуализации

начальник управления ФСТЭК России
Лютиков Виталий Сергеевич

Облачные технологии

Облачные технологии – это технологии, обеспечивающие:

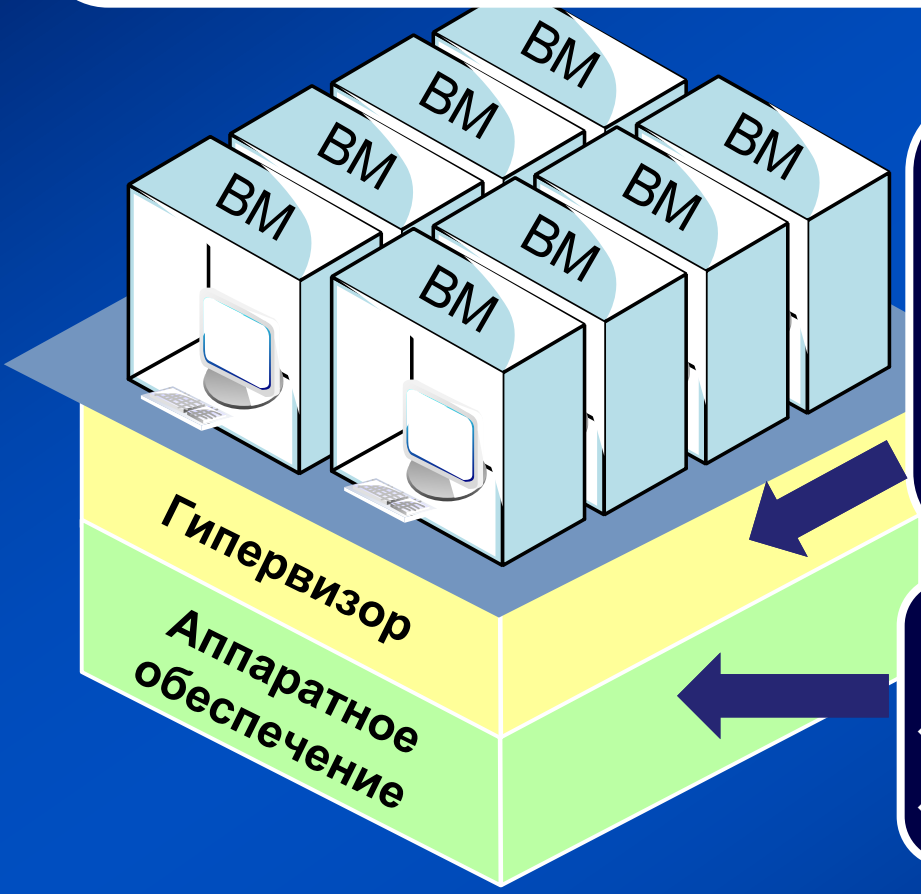
- самообслуживание по запросу потребителей
- повсеместный сетевой доступ
- объединение компьютерных ресурсов в единый пул
- оперативная реакция
- измеримость

Виды облачных услуг

- **SaaS** – Программное обеспечение как услуга
- **PaaS** – Платформа как услуга
- **HaaS** – Аппаратное обеспечение как услуга
- **BPaaS** – Бизнес-процесс как услуга
- **SecaaS** – Безопасность как услуга
- Другие виды услуг

Технологии виртуализации

Виртуализация – группа технологий, основанных на преобразовании формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы



Виртуализация серверов

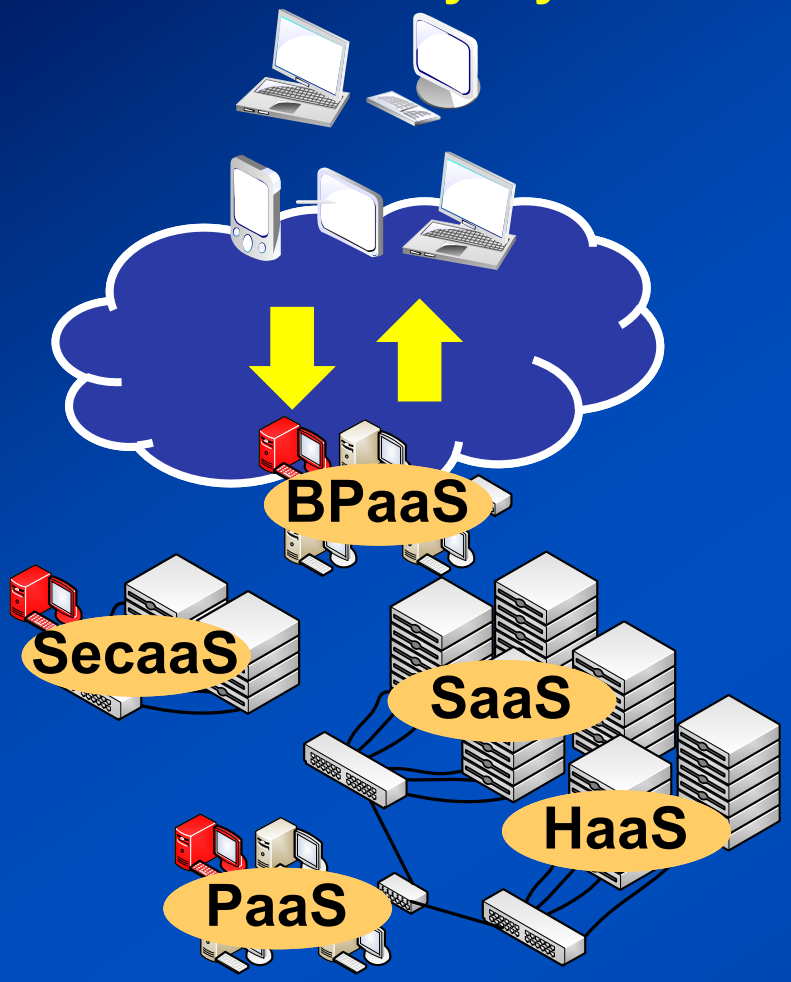
- VMware (ESX Server)
- Microsoft (Hyper-V)
- Citrix (XenServer)
- другие

Аппаратная поддержка виртуализации

- Intel VT
- AMD-V

Основные риски безопасности
при применении облачных технологий

Потребители облачных услуг



Поставщики облачных услуг

Основные риски для потребителей облачных услуг

- Неопределённость ответственности
- Потеря управления, доверия
- Привязка к провайдеру облачных услуг
- Недостатки управления информацией/облачными ресурсами
- Потеря и утечка данных

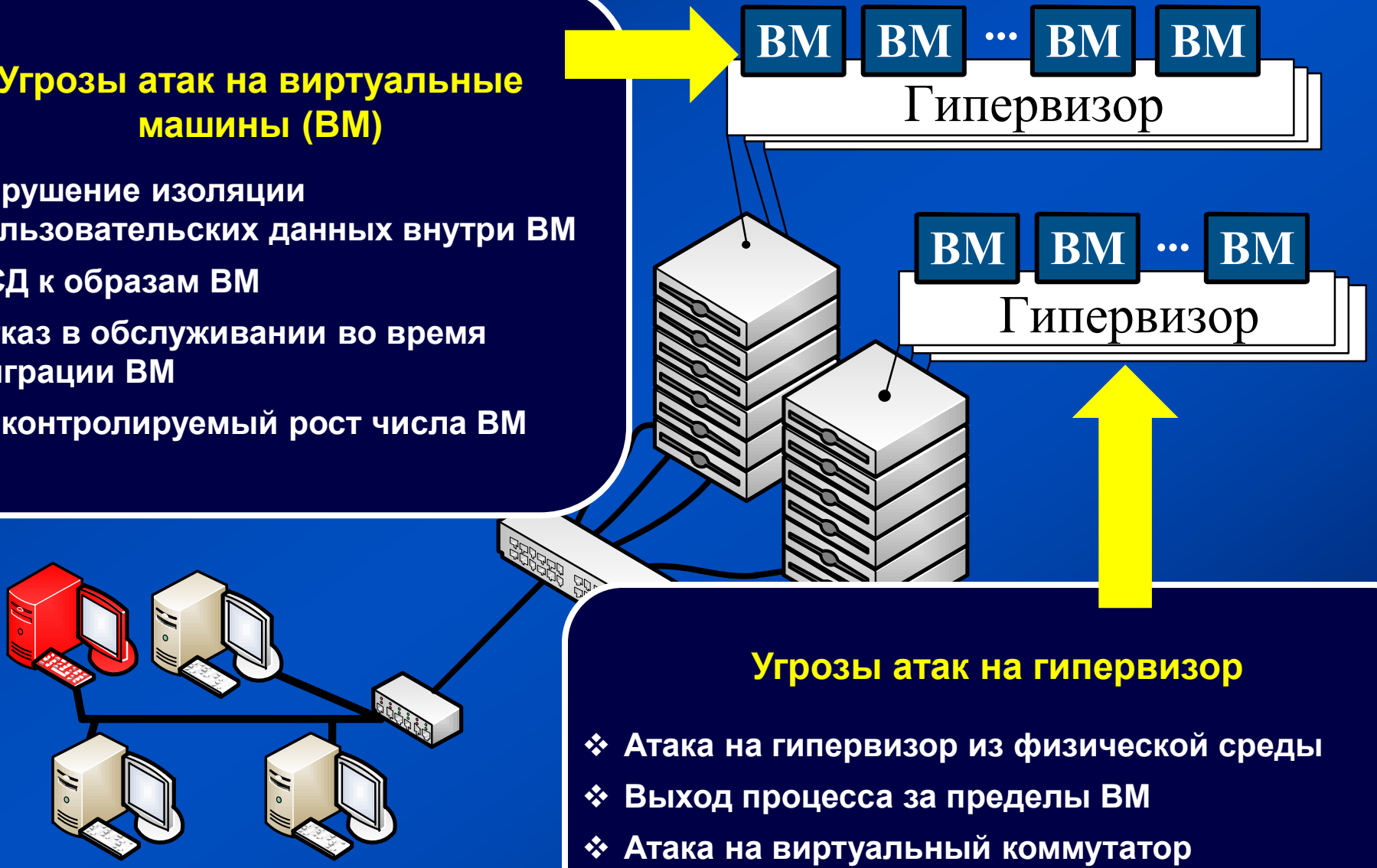
Основные риски для поставщиков облачных услуг

- Неопределённость в распределении ответственности
- Несогласованность политик безопасности
- Непрерывная модернизации
- Конфликт юрисдикций различных стран
- Общедоступность инфраструктуры
- Недобросовестное исполнение обязательств, злоупотребления поставщиками облачных услуг
- Злоупотребления со стороны потребителей облачных услуг

Основные угрозы безопасности информации
при применении технологий виртуализации

Угрозы атак на виртуальные машины (ВМ)

- Нарушение изоляции пользовательских данных внутри ВМ
- НСД к образам ВМ
- Отказ в обслуживании во время миграции ВМ
- Неконтролируемый рост числа ВМ



Угрозы атак на гипервизор

- Атака на гипервизор из физической среды
- Выход процесса за пределы ВМ
- Атака на виртуальный коммутатор

Меры защиты
при применении облачных технологий

- выбор облачного провайдера с учётом законодательства страны-местонахождения провайдера
- документальное оформление соглашений

- менеджмент информационной безопасности
- реализация политики информационной безопасности
- инвентаризация оборудования
- контроль доступа

- разграничение доступа к облачным ресурсам
- защита виртуальной среды
- централизованное управление средствами защиты
- применение программно-аппаратных средств защиты

Технические меры защиты
при применении облачных технологий

Приказ ФСТЭК России № 17

Меры защиты
(проект документа)
ФСТЭК России, 2014

ГОСТ Р (проект)
Защита информации при применении облачных технологий

Уровень оркестровки

- управление межоблачным взаимодействием
- удаление неиспользуемых данных о потребителях облачных услуг

Уровень управления

- объединение гипервизоров в кластеры, облачных ресурсов в пулы
- прогнозирование исчерпания вычислительных ресурсов

Уровень виртуализации

- контроль номенклатуры устанавливаемого ПО
- удаление неиспользуемых образов виртуальных машин

Уровень оборудования

- контроль целостности облачных клиентов
- централизованное обновление средств защиты

Меры защиты
при применении технологий виртуализации

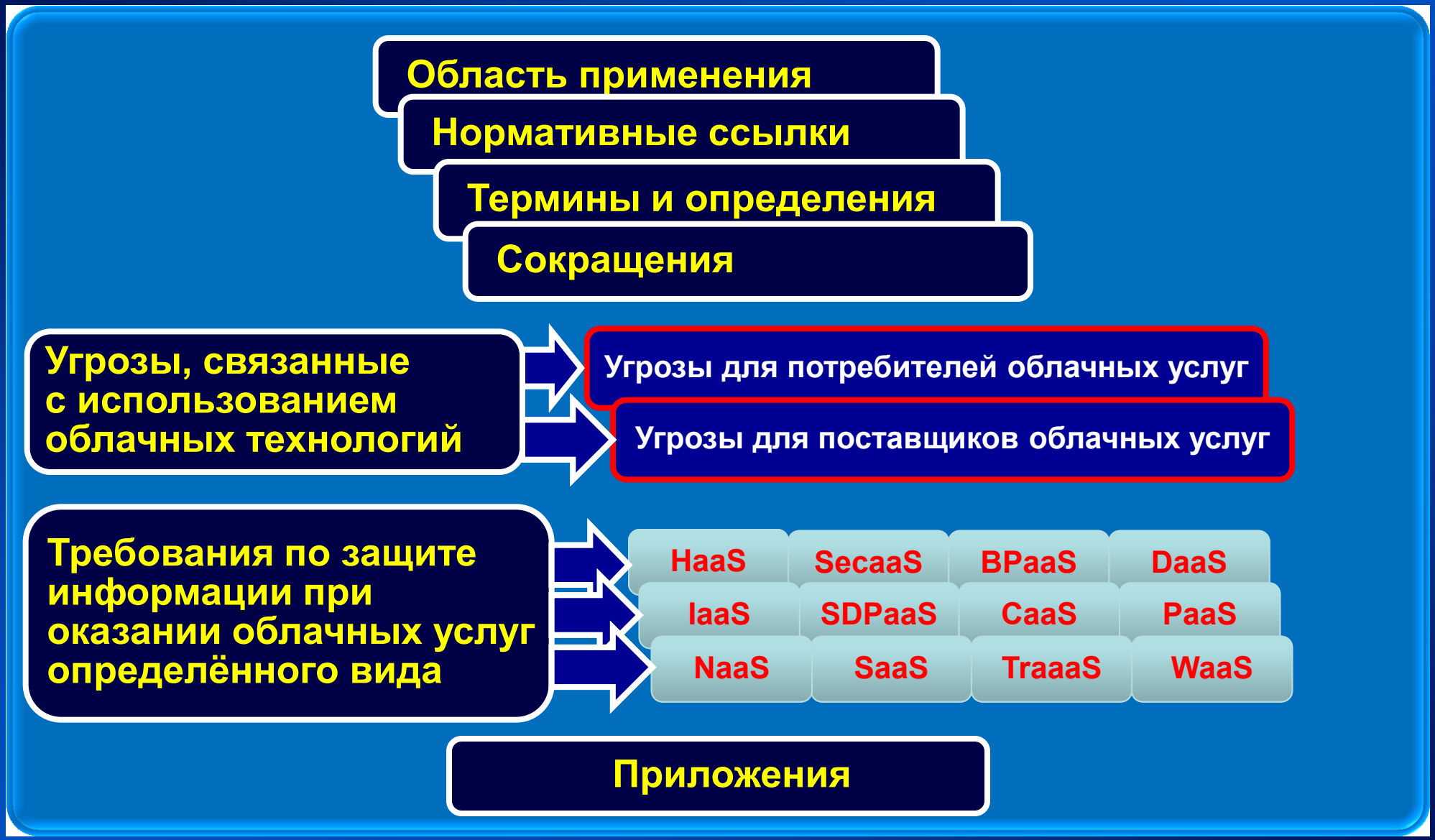
Приказ ФСТЭК России № 17

Меры защиты
(проект документа)
ФСТЭК России, 2014

ГОСТ Р (проект)
Защита информации при применении технологий виртуализации

Средства создания и управления виртуальной инфраструктурой	**- контроль запуска гипервизора и ВМ;** **- блокировка доступа к объектам виртуальной инфраструктуры**
Виртуальные вычислительные системы	**- контроль доступа к памяти гипервизора;** **- установка ПО, только разрешённого к использованию в виртуальной инфраструктуре**
Виртуальные системы хранения данных	**- блокировка доступа к объектам виртуальной инфраструктуры;** **- защита от НСД к парольной информации**
Виртуальные каналы передачи данных	**- мониторинг и балансирование загрузки виртуальных каналов;** **- автоматическое изменение сетевых маршрутов**
Отдельные виртуальные устройства	**- мониторинг загрузки мощностей;** **- контроль работоспособности дублирующих виртуальных устройств**
Виртуальные средства защиты информации	**- автоматическое восстановление;** **- обеспечение доверенного виртуального канала доступа к средствам защиты**

Структура проекта ГОСТ Р
«Защита информации при применении облачных технологий»

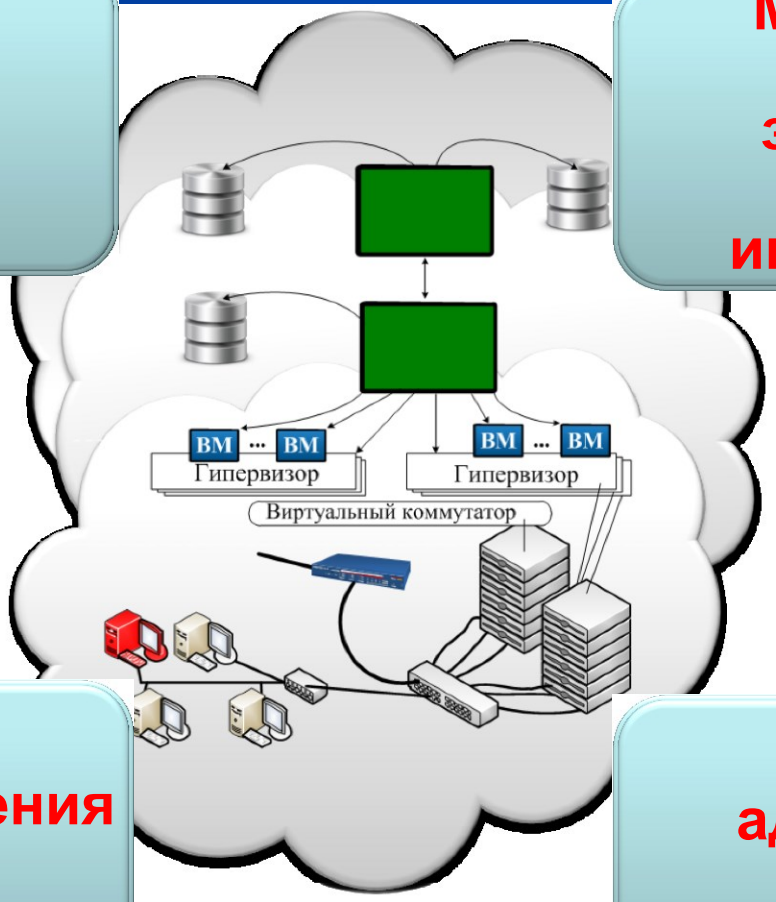


Структура проекта ГОСТ Р
«Защита информации при применении технологий виртуализации»

Основные особенности виртуальной среды как объекта защиты

Наличие гипервизора

Максимальный уровень защищенности виртуальной инфраструктуры



Наличие системы управления виртуальной инфраструктурой

Наличие администратора виртуальной инфраструктуры

Спасибо за внимание!

начальник управления ФСТЭК России
Лютиков Виталий Сергеевич