TADVISER
Государство. Бизнес. ИТ

# Горизонт-ВС

Продукт

| | |
|---|---|
| **Разработчики:** | Баррикады, инновационный центр |
| **Технологии:** | Виртуализация, ИБ - Межсетевые экраны, ИБ - Резервное копирование и хранение данных, СКУД - Системы контроля и управления доступом |

**«Горизонт-ВС»** — программно-аппаратный комплекс виртуализации и защиты виртуальных вычислений, разработанный инновационным центром «Баррикады».

ПАК представляет собой отечественную платформу для создания доверенных отказоустойчивых облачных инфраструктур любого масштаба. Комплекс обеспечивает полный контроль над виртуальной инфраструктурой из слоя гипервизора — недостижимой для злоумышленников и вредоносного программного обеспечения области. В слое гипервизора сосредоточены средства мониторинга и защиты информации.

«Горизонт-ВС» позволяет вывести ряд функций по обеспечению безопасности информации и администрированию за пределы виртуальной инфраструктуры и гарантировать корректное ее функционирование даже при наличии в ней уязвимостей. На базе платформы «Горизонт-ВС» возможно построение антифрод-систем с гарантированным уровнем защищенности. Средствами платформы обеспечивается защита от внутреннего нарушителя и предоставляется возможность полного контроля со стороны служб информационной безопасности потребителя над функционирующими сервисами с использованием средств аппаратной защиты.[1]

**Особенности**

- Встроенные программные и аппаратные сертифицированные средства защиты
- Единое комплексное отказоустойчивое сертифицированное решение с централизованным управлением, миграцией, масштабированием и поддержкой мобильных технологий
- Технические решения импортозамещения и обеспечения доверенной замкнутой вычислительной среды
- Возможность функционирования на существующей и перспективной импортной и отечественной элементной базе
- Возможность обновления политик безопасности и ядра системы без остановки работы гипервизора и гостевых виртуальных машин

**Скорость**

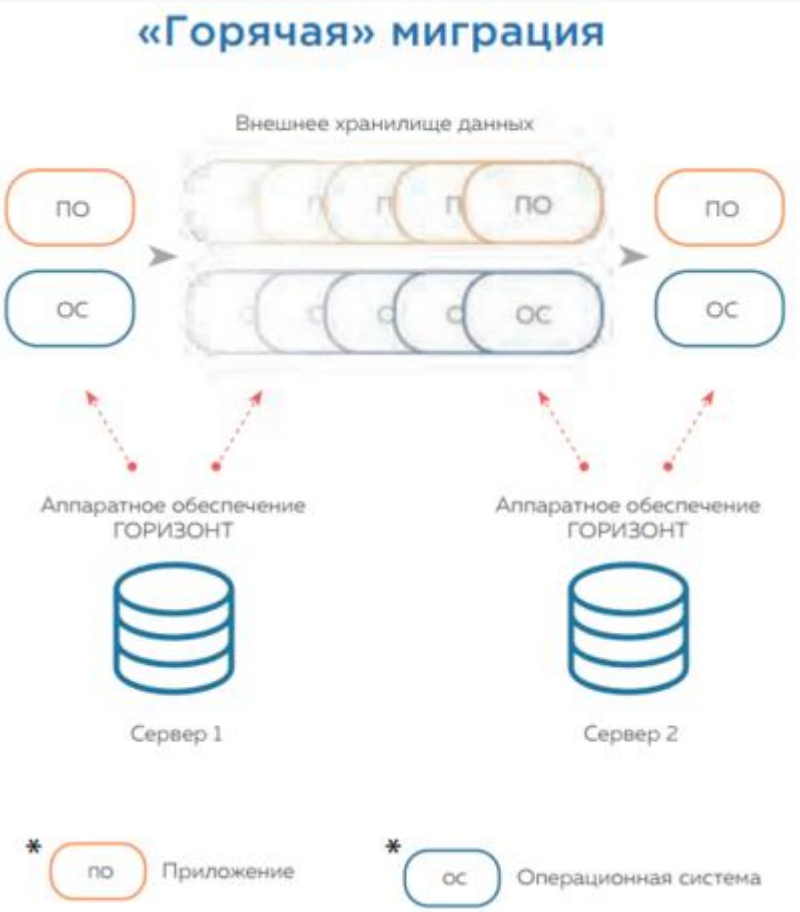
Функции виртуальной машины (ВМ):

- Настройка лимита максимального значения latency (задержки), которое позволяет избежать перегрузки системы хранения данных, сетевой подсистемы, процессов одним хостом или виртуальной машиной;
- Перезапуск виртуальных машин после сбоя в соответствии с приоритетами;
- Установка на "голую" аппаратную платформу;
- Добавление устройств во время исполнения без прерывания работы (диски, сетевые адаптеры)
- Мониторинг работы.

**Доступность**

Функции ВМ:

- Возможность создавать резервные копии по заданным сценариям;
- Миграция виртуальных машин по хостам без подключённого СХД;
- Возможность без простоя мигрировать виртуальные машины с одного хоста на другой;
- Fault tolerance (zero downtime HA) для многопроцессорных систем;
- Миграция виртуальных машин на дальние (физически, км) серверы.




**Автоматизация**

Функции ВМ:

- Конвертация физического сервера/АРМ в виртуальную среду;
- Миграция виртуальных машин
- Возможность легко и быстро создавать виртуальные машины и запускать несколько операционных систем на одном сервере;
- Возможность миграции виртуальных машин, позволяющая автоматически распределять нагрузку, в том случае, если один из хостов кластера оказывается загружен больше остальных.

**Хранение**

Функции ВМ:

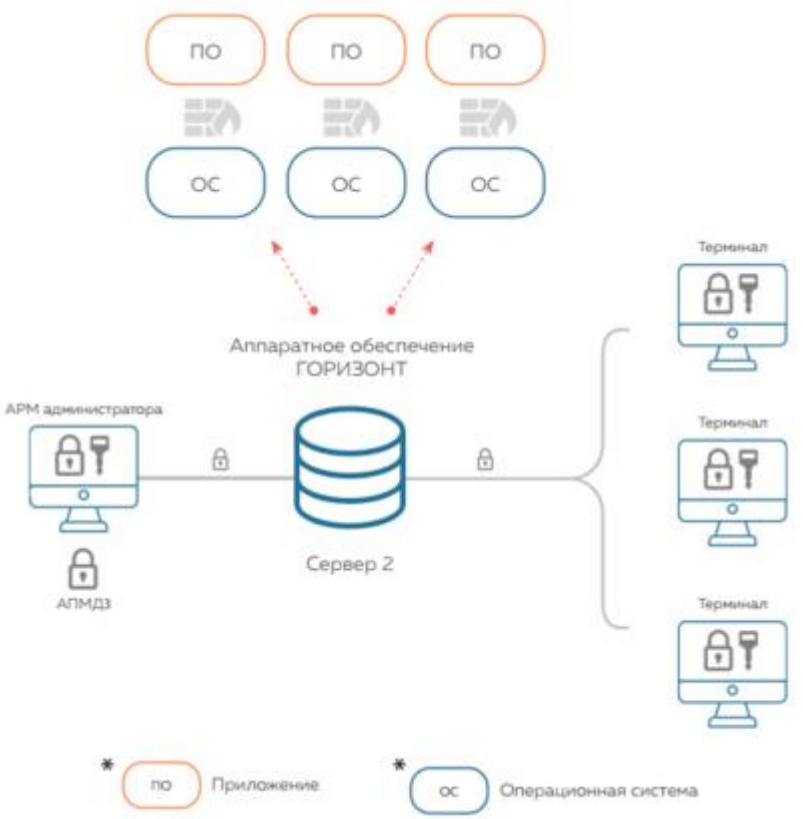
- Наличие интерфейсов для разработки программного обеспечения, необходимого для отказоустойчивых подключений системы хранения данных;
- Наличие интерфейса, позволяющего сторонним системам резервного копирования работать без оказания существенной нагрузки на сервер. Для реализации используется технология создания мгновенных снимков ВМ;
- Технология тонких дисков, позволяющая экономить дисковое пространство на системах хранения данных. Так, при создании ВМ с диском объемом 100 гигабайт с гостевой ОС Windows Server 2008в системе хранения данных будет занято всего лишь 10 гигабайт с возможностью дальнейшего динамического расширения при необходимости.

**Безопасность**

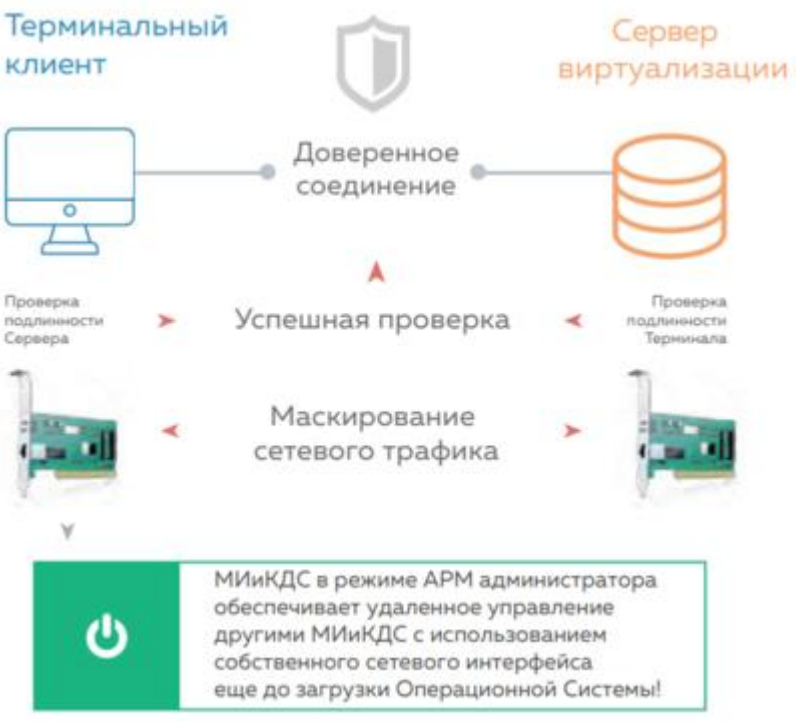
Функции ВМ:

- Возможность установки расширенных настроек безопасности и изоляции используемых ресурсов для ВМ;

- Встроенный брандмауэр для виртуальной машины, позволяющий контролировать трафик;
- Управление доступом на основе ролей;
- Аппаратная защита подключения терминалов;
- Аппаратная защита виртуальной среды;
- Встроенная подсистема учета печати;
- Встроенная подсистема учёта и контроля USB-подключений;
- Встроенная подсистема контроля доступа к разделяемым накопителям;
- Мандатное разграничение доступа виртуальных машин к внутренним и внешним ресурсам.




Одним из основных компонентов подсистемы информационной безопасности является специализированный аппаратный **модуль идентификации и контроля доверенной среды**(МИиКДС). Изделие предназначено для защиты автоматизированных рабочих мест (АРМ), являющихся терминалами рабочих станций "тонкий клиент" и серверов, от несанкционированного доступа (НСД), а также для защиты информации, передаваемой по сети, и генерации аутентификационной информации для подключения пользователей терминалов к виртуальным ОС, исполняющимся на сервере.[2]




**Изделие МИиКДС работает в трёх режимах:**

- режим терминал;
- режим сервер;
- режим АРМ администратора.

## Примечания

1. ↑ Каталог отечественного металлообрабатывающего оборудования развернут в облаке
2. ↑ ИМПОРТОНЕЗАВИСИМАЯ ДОВЕРЕННАЯ ПЛАТФОРМА ВИРТУАЛИЗАЦИИ «ГОРИЗОНТ-ВС»