



Акционерное общество «ИРИДИУМ»

ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

Платформа виртуализации ПК «Иридиум»

RU.УГСФ.00001-01 92 01

Листов 29

АННОТАЦИЯ

Настоящий документ включает в себя описание функциональных характеристик платформы виртуализации ПК «Иридиум» (далее – ПК «Иридиум», изделие), разработанной АО «Иридиум».

СОДЕРЖАНИЕ

1	Общие Сведения	4
1.1	Основные сведения о ПК «Иридиум»	4
1.2	Назначение ПК «Иридиум»	4
1.3	Комплектность изделия	5
1.4	Функциональные возможности ПК «Иридиум»	6
2	Архитектура ПК «Иридиум»	19
3	Функциональные характеристики ПК «Иридиум»	21
3.1	Защищенная специализированная закрытая ОС	21
3.2	Виртуальный коммутатор	22
3.3	Файловая система	22
3.4	Программно-определяемая СХД «Шторм»	23
3.5	Система оркестрации	23
3.6	Модуль управления удаленными рабочими столами	24
3.7	Резервное копирование и репликация	24
3.8	Межсетевой экран	25
3.9	Мониторинг	26
4	Требования к минимальному составу технических средств	27
5	Требования к программному обеспечению	27
6	Требования к надежности	27
7	Специальные требования	28

1 Общие Сведения

1.1 Основные сведения о ПК «Иридиум»

Платформа виртуализации ПК «Иридиум» – это многокомпонентное изделие, предназначенная для использования в клиент-серверных системах.

ПК «Иридиум» включен в единый реестр российских программ для электронных вычислительных машин и баз данных Минкомсвязи России – реестровая запись №16819 от 01.03.2023.

ПК «Иридиум» является комплексным решением для создания как классических конвергентных, так и гиперконвергентных виртуальных сред. Изделие поддерживает работу с классическими системами хранения данных (СХД) по протоколам Fibre Channel, iSCSI, NFS. ПК «Иридиум» также может быть использован для развертывания гиперконвергентного распределенного программно-определяемого СХД на базе локальных дисков, установленных в физические хосты, без использования классической разделяемой СХД. Ближайший аналог – продукт VMware vSAN.

1.2 Назначение ПК «Иридиум»

Сфера применения ПК «Иридиум» – как предприятия госсектора, так и коммерческие предприятия. ПК «Иридиум» может быть использован как на предприятиях крупного бизнеса, так и среднего и даже малого бизнеса.

В составе ПК «Иридиум» есть все необходимые инструменты для миграции нагрузок с любых импортных систем виртуализации (таких, как VMware vSphere и Microsoft Hyper-V), а также с любых отечественных систем виртуализации.

1.3 Комплектность изделия

Обозначение изделия	Наименование изделия	Количество	Примечание
RU.УГСФ.00001-01	1 Программный комплекс “Иридиум” в составе:		Примечание 2,3
RU.КНРШ.00014-01	1.1 Средство виртуализации “Звезда”		
RU.КНРШ.00007-01	1.2 Система хранения данных “Шторм”		Примечание 4
RU. УГСФ.00005-01	1.3 Программный комплекс “Иридиум-VDI”		Примечание 5
RU.ЛНТФ.00001-01	1.4 Программный комплекс “Средство управления единичным хостом ПВ”		Примечание 6
RU.ЛНТФ.00002-01	1.5 Программный комплекс “Средство управления группой хостов ПВ”		Примечание 7
RU.КНРШ.00008-01	1.6 Программный комплекс “Звезда”		Примечание 8
Примечания 1 Количество и набор составных частей определяется по решению Заказчика спецификацией поставки. 2 Составные части ПК “Иридиум” поставляются на одном USB-носителе. 3 Программный комплекс “Иридиум” зарегистрирован в Реестре российского программного обеспечения (запись в реестре от 01.03.2023 №16819). 4 Система хранения данных “Шторм” зарегистрирована в Реестре российского программного обеспечения (запись в реестре от 13.02.2023 №16626). 5 Программный комплекс “Иридиум-VDI”. Свидетельство о государственной регистрации программы для ЭВМ № 2025619685. 6 Программный комплекс “Средство управления единичным хостом ПВ” является опционально входящим в состав ПК “Иридиум” компонентом 7 Программный комплекс “Средство управления группой хостов ПВ” является опционально входящим в состав ПК “Иридиум” компонентом 8 Программный комплекс “Звезда” является опционально входящим в состав ПК “Иридиум” компонентом. Программный комплекс “Звезда” зарегистрирован в Реестре российского программного обеспечения (запись в реестре №16845 от 01.03.2023). По спецификации поставки в состав ПК “Иридиум” может входить гипервизор Средство виртуализации “Звезда” или гипервизорный компонент из состава Программного комплекса “Звезда”.			

1.4 Функциональные возможности ПК «Иридиум»

ПК «Иридиум» обеспечивает:

- установка непосредственно на аппаратное обеспечение без использования хостовой операционной системы (гипервизор I типа СВ “Звезда”);
- гипервизор I типа СВ “Звезда” включает гипервизор II типа — эмулятор QEMU;
- создание и управление виртуальной средой на группе серверов (кластере);
- поддержка графического установщика;
- возможность установки в режиме выделенной физической или виртуальной машины вне управляемого кластера и в режиме виртуальной машины на гипервизорах управляемого кластера;
- возможность установки в локальном режиме без подключения к сети Интернет;
- объединение физических серверов в кластер до 1536 узлов, обеспечивающих постоянную доступность виртуальной машины, даже в случае отказа физического сервера;
- обеспечение возможности использования в качестве гостевой ОС операционных систем семейств Linux, Windows;
- функционирование средств защиты информации в среде виртуализации, а также возможность интеграции:
 - виртуальных систем обнаружения вторжения;
 - межсетевых экранов;
 - антивирусных средств;
 - средств анализа защищенности;
 - средств защиты информации от DDoS атак;
 - средств корреляции событий безопасности;

- средств контроля утечки информации из информационной систем;
- средств централизованного управления безопасностью, событиями и информацией (SIEM);
- наличие сертифицированной и несертифицированной версии изделия;
- поддержка функции Multipathing;
- обеспечение виртуализации аппаратных ресурсов в виде обособленных ВМ, работающих на физическом сервере x86 архитектуры;
- создание виртуальных машин (ВМ), их образов и шаблонов с поддержкой 32 и 64-битных гостевых операционных систем;
- поддержка графического веб-интерфейса и CLI (интерфейса командной строки);
- возможность создания ВМ из настраиваемых шаблонов с помощью графического и консольного интерфейсов;
- возможность группового создания ВМ из шаблонов;
- возможность автозапуска виртуальных машин при старте работы ПО;
- поддержка в ВМ до 255 виртуальных процессоров;
- возможность управления конфигурацией ВМ с помощью графического и консольного интерфейсов;
- включает в состав, программное обеспечение для управления виртуальными рабочими местами (VDI);
- поддержка различных сценариев виртуализации рабочих мест — с одним или несколькими брокерами (с балансировкой), внутри одного кластера или с выделенным кластером VDI;
- поддержка технологии NVIDIA vGPU;

- возможность изменения количества выделенных процессоров и размера оперативной памяти виртуальным машинам без завершения их функционирования;
- возможность подключения к ВМ устройств из состава аппаратных средств, на которых функционирует серверная часть изделия, включая устройства USB 3.0;
- возможность интеграции с внешними системами управления и мониторинга (в том числе Zabbix) для сбора статистики производительности и контроля состояния (поддержка протоколов: SNMP, SSH, CLI, CIM, API и т.д.);
- возможность добавления виртуальных дисков в гостевую операционную систему и увеличение их размеров без остановки ВМ;
- возможность администратору системы получать доступ к гостевой операционной системе через сервер виртуализации даже в случае отсутствия у виртуальной машины сетевого адаптера или подключения к сети;
- доступ к консоли ВМ по протоколам SPICE, VNC, HTML5;
- возможность доступа к VNC консоли виртуальной машины с помощью API;
- поддержка открытого стандарта Open Virtualization Format (OVF);
- возможность подключения внешних хранилищ по протоколу FC;
- возможность клонирования ВМ без необходимости их выключения;
- возможность создания кластеров высокой доступности, выполняющих перезапуск ВМ в случае выхода из строя узла кластера;
- возможность изменения параметров высокой доступности одновременно для нескольких ВМ через веб-интерфейс;

- возможность автоматического восстановления (перезапуск) виртуальной машины в аварийном состоянии;
- возможность автоматической балансировки рабочих нагрузок между хостами путем «горячей» миграции без выключения виртуальных машин;
- возможность переноса ВМ между узлами кластера без прерывания трафика с управлением через веб-интерфейс;
- обеспечение автоматического распределения сервером виртуализации ресурсов между работающими ВМ;
- миграция дисков работающих ВМ между хранилищами без их остановки с управлением через веб-интерфейс;
- возможность перемещения ВМ между серверами и кластерами с одновременным перемещением файлов ВМ между системами хранения без остановки ОС ВМ через единый графический веб-интерфейс администратора;
- возможность мониторинга состояния задач на перемещение виртуальных машин и файлов виртуальных машин, включая отмену выполнения задач, через единый графический веб-интерфейс администратора;
- поддержка механизма multiqueue для распределения обработки операций ввода-вывода между несколькими очередями с использованием различных потоков выполнения;
- сервисный режим обслуживания узла с автоматическим перемещением работающих ВМ без их остановки;
- возможность перевода домена хранения в режим обслуживания;
- возможность централизованного управления кластерами, серверной частью изделия на всех узлах кластера высокой доступности, хранилищами и виртуальными коммутаторами;

- возможность мониторинга работоспособности и использования ресурсов ВМ;
- наличие единого окна отслеживания состояния системы в реальном времени;
- возможность предоставления информации по загрузке ресурсов хранения в реальном времени в графическом интерфейсе и предоставлять возможность задания пороговых значений (при достижении которых приходят уведомления) по следующим параметрам: скорость чтения на диск, скорость записи на диск, задержка чтения, задержка записи;
- возможность экспорта списка виртуальных машин, хостов виртуализации, кластеров, профилей виртуальных сетевых адаптеров, доменов хранения, пулов, квот, провайдеров, активных сессий пользователей, списка пользователей и событий в CSV формат через веб-интерфейс администратора;
- мониторинг и вывод событий маппинга страниц памяти подсистемами ядра;
- возможность централизованной настройки сетевых компонентов на хостах виртуализации;
- возможность распределенной коммутации пакетов уровня L2 без привязки к нижележащей топологии сети и физическому расположению с управлением через веб-интерфейс;
- наличие средств управления IP-адресацией подключенных ВМ к распределенному коммутатору с управлением через веб-интерфейс;
- поддержка виртуальных коммутаторов с технологией VLAN (Virtual Local Area Network);
- поддержка создания внешних виртуальных растянутых сетей (VXLAN) для организации единого доступа к логическим сетям в различных центрах обработки данных;

- возможность настройки MTU через веб-интерфейс;
- возможность настройки маршрутизации трафика между изолированными сетями без выхода трафика за пределы виртуального коммутатора через веб-интерфейс администратора;
- возможность настройки маршрутизации трафика между физической сетью и изолированными сетями через веб-интерфейс;
- возможность трансляции сетевых адресов (SNAT) с управлением через веб-интерфейс администратора;
- возможность настройки правил микросегментации (распределенного межсетевого экрана) входящего и исходящего трафика виртуальных машин на уровне L3 и L4 на порту виртуальной машины и по IP-адресам, включая запрещающие правила, через единый графический веб-интерфейс администратора;
- возможность объединять IP-адреса в группы с возможностью использования в правилах микросегментации;
- возможность объединения правил микросегментации в блоки (группы безопасности) через единый графический веб-интерфейс администратора;
- возможность редактирования таблицы маршрутизации логического маршрутизатора и задания статических маршрутов через единый графический веб-интерфейс администратора;
- возможность подключения виртуальной машины к существующему широкополосному домену с сохранением функционала управления IP-адресацией с управлением через единый графический веб-интерфейс администратора;
- возможность присвоения IP-адресов с момента создания виртуального интерфейса - как при создании ВМ, так и при изменении конфигурации (добавление или удаление виртуальных сетевых карт);

- возможность назначения MAC-адресов виртуальных машин как в автоматическом режиме, так и в ручном;
- возможность настройки отказоустойчивости логического маршрутизатора, включая назначение нескольких серверов виртуализации для данного маршрутизатора и определение приоритета подключения через веб-интерфейс;
- возможность наблюдения за трафиком виртуальных машин без вмешательства в конфигурацию сетевого обмена (зеркалирование и приема трафика) через веб-интерфейс;
- возможность изменения адресов источника и назначения пакетов, проходящих логический маршрутизатор, включая DNAT, SNAT и 1-to-1 NAT, через веб-интерфейс;
- возможность контроля используемых виртуальной машиной адресов, включая настройку правил, описывающие допустимые комбинации MAC и IP адресов, через веб-интерфейс;
- наличие API для управления программными сетями;
- возможность создавать внешние сети, которые можно использовать для единого доступа к логическим сетям в различных центрах данных;
- возможность управления сертификатами, включая мониторинг срока действия сертификатов с настройкой уведомлений, обновление срока и замену сертификатов, через веб-интерфейс;
- возможность мониторинга состояния заданий, включая удаление зависших заданий, через единый графический веб-интерфейс администратора;
- возможность сброса всех назначенных прав пользователя через веб-интерфейс;

- возможность объединения двух и более доменов хранения в логический кластер и настройки балансировки загруженности доменов хранения по объему, включая автоматическую балансировку нагрузки по расписанию и ручную балансировку в формате вывода рекомендаций по перемещению дисков ВМ, через веб-интерфейс;
- возможность собирать и предоставлять данные о ресурсах, производительности и состоянии виртуальной среды в формате Prometheus для внешних систем мониторинга;
- возможность настройки конфигурации NTP, включая распространение конфигурации на хосты виртуализации и мониторинг состояния синхронизации с источниками времени, через веб-интерфейс;
- возможность отслеживания факта срабатывания правила микросегментации путем записи в журнал хоста виртуализации;
- возможность отслеживать срабатывание правил микросегментации через веб-интерфейс в режиме реального времени, включая предоставление описания проходящего трафика и его базовых характеристик;
- возможность группировки виртуальных машин в папки, включая создание вложенных папок, назначения и отзыв прав на папки, и иметь древовидное представление папок, через веб-интерфейс;
- подключение к ВМ по протоколу SPICE USB-устройств из состава аппаратных средств, на которых функционирует клиентская часть изделия;
- возможность ограничения для сетевого и дискового ввода-вывода ВМ на основе их групповых или индивидуальных настроек (QoS ресурсов);
- поддержка механизмов оптимизации оперативной памяти:
 - дедупликация страниц;
 - динамическое распределение;

- выгрузка в файл подкачки, область подкачки, сформированную на постоянном накопителе, либо оперативной памяти;
- Memory Ballooning;
- возможность создания динамически расширяющегося виртуального дискового пространства ВМ с обеспечением возможности выделения соответствующих аппаратных средств (физических дисков, блоков физических дисков) по мере заполнения виртуального дискового пространства ВМ;
- возможность динамического добавления ресурсов: RAM, vCPU, дискового пространства, без остановки ВМ;
- клиентское приложение с графическим интерфейсом для подключения к ВМ;
- поддержка работы с контейнерами;
- возможность работы с хранилищем LVM, а также использование технологии тонких томов LVM Thin Provision;
- возможность проброса на виртуальные машины локальных дисков хостов виртуализации и LUN с СХД;
- поддержка создания программно-определяемой СХД;
- возможность параллельного доступа нескольких ВМ к одному виртуальному диску;
- возможность размещения файлов виртуальных машин на следующих типах систем хранения:
 - с файловым доступом по протоколу NFS, локальном диске гипервизора;
 - с блочным доступом по протоколам Fibre Channel и iSCSI;
 - с использования дисковых устройств NVMe-oF Ethernet TCP/RoCE (RDMA);

- программно-определяемом хранилище, включая в гиперконвергентном формате;
- возможность централизованного обновления с использованием штатных средств;
- возможность резервирования интерфейсов управления инфраструктурой виртуализации;
- возможность размещения контроллера на хосте (без использования дополнительного физического сервера);
- возможность формирования диаграммы (карты), на которой отображены объекты виртуальной инфраструктуры (кластеры, серверы, ресурсы хранения), их состояние и связи между ними в реальном времени;
- возможность создания снимков (снимков) ВМ с возможностью возврата к нему;
- возможность просматривать список всех снимков состояния ВМ через веб-интерфейс;
- миграция ВМ из других сред виртуализации, в том числе VMware;
- создание шаблона на базе существующей ВМ;
- возможность блокирования сессии пользователя;
- возможность квотирования ресурсов виртуальных машин;
- поддержка Affinity Rule – размещение выбранных ВМ на одном хосте виртуализации и Anti-Affinity Rule – размещение выбранных ВМ на разных хостах виртуализации;
- возможность управления локальными пользователями посредством веб-интерфейса;
- возможность вывода уведомления о попытках входа при авторизации пользователя в единый графический веб-интерфейс администратора;

- обеспечение идентификации и аутентификации субъектов доступа (пользователей и администраторов) до предоставления доступа к функциям виртуализации и управления в том числе в режиме взаимодействия со средствами создания единого пространства пользователей;
- запуск ВМ в виде отдельного процесса, функционирующего от имени учетной записи субъекта доступа (пользователя) с унаследованием его мандатных атрибутов;
- защита файлов-образов ВМ от модификации в процессе функционирования ВМ;
- уничтожение (стирание) информации на файлах виртуальных машин, исключающее возможность восстановления защищаемой информации;
- возможность автоматической очистки информации о хранилищах на хостах виртуализации после удаления данных хранилищ;
- регистрация событий с использованием средств централизованного протоколирования с возможностью их анализа и выгрузки;
- возможность отправки лог файлов на внешний syslog сервер для отдельного хоста виртуализации, кластера виртуализации и сервера управления и выбора протокола передачи данных лог файлов (TCP, UDP, SSL) через единый графический веб-интерфейс администратора;
- регулярное обновление для нейтрализации угроз эксплуатации уязвимостей;
- управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;
- возможность разграничения доступа к виртуальной среде, построенного на основе классической ролевой политики безопасности и ее интеграции со службой каталога;

- разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей;
- возможность создания и управления пулами виртуальных машин;
- интерфейс на русском языке с возможностью переключения на иностранный язык.
- функции микросервисной платформы как средство защищенного исполнения и управления контейнерами;
- наличие встроенного функционала резервного копирования, а также возможность интеграции с программным обеспечением для резервного копирования, выполняющим как агентное, так и безагентное резервное копирование и восстановление как самих ВМ, так и их шаблонов, образов и дисков в различных форматах (включая qcow2), на различных типах томов (включая lvm, serh и S3-хранилища);
- возможность ручного и автоматического (по расписанию) резервного копирования конфигурации сервера управления, включая конфигурацию сети (виртуальных сетей, подсетей, логических портов, внешних сетей, логических маршрутизаторов и правил микросегментации), через единый графический веб-интерфейс администратора с возможностью выбора расположения файла резервной копии и протокола (SSH, FTP, SMB и NFS);
- возможность архивирования и вычисления контрольных сумм файлов резервной копии конфигурации сервера управления;
- возможность создания отчетов о состоянии, утилизации и ошибках виртуальной инфраструктуры за выбранный период времени через единый графический веб-интерфейс администратора с учетом часового пояса сервера управления в следующих форматах: PDF, HTML;
- наличие административного и пользовательского веб-портала;

- наличие API для автоматизации и управления;
- реализация функций безопасности: «Идентификация и аутентификация» (ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, ИАФ.7), «Управление доступом» (УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.8, УПД.9, УПД.10, УПД.12), «Ограничение программной среды» (ОПС.1, ОПС.2, ОПС.3, ОПС.4), «Регистрация событий безопасности» (РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7, РСБ.8), «Анализ защищённости» (АНЗ.2, АНЗ.3, АНЗ.4, АНЗ.5), «Обеспечение целостности» (ОЦЛ.1, ОЦЛ.2, ОЦЛ.3, ОЦЛ.6, ОЦЛ.7), «Обеспечение доступности» (ОДТ.1, ОДТ.3, ОДТ.4, ОДТ.5, ОДТ.6), «Защита среды виртуализации» (ЗСВ.1, ЗСВ.2, ЗСВ.3, ЗСВ.4, ЗСВ.5, ЗСВ.6, ЗСВ.7, ЗСВ.8, ЗСВ.9, ЗСВ.10), «Защита информационной (автоматизированной) системы и ее компонентов» (ЗИС.1, ЗИС.2, ЗИС.5, ЗИС.10, ЗИС.14, ЗИС.15, ЗИС.19, ЗИС.21).

2 **Архитектура ПК «Иридиум»**

При создании ПК «Иридиум» мы постарались максимально приблизить пользовательский опыт администратора к таковому для продукта VMware vSphere. Веб-интерфейс системы оркестрации и одиночных хостов виртуализации ПК «Иридиум» максимально точно соответствует веб-интерфейсу VMware vCenter (система оркестрации в продукте VMware vSphere). По приблизительным оценкам в Российской Федерации более 100 тысяч специалистов по VMware vSphere, подготовленных за годы присутствия компании VMware на российском рынке. Эти специалисты могут начать работать с ПК «Иридиум», не являясь при этом глубокими специалистами по ОС Linux, и не проходя длительное 1-2-годичное переобучение (что требовалось бы для эксплуатации программных продуктов наших конкурентов).

Но веб-интерфейса «как у VMware» оказалось недостаточно для решения поставленной задачи. Реализация функционала платформы виртуализации на уровне VMware vSphere оказалась невозможна на базе программных продуктов Open Source, из-за существенных отличий в архитектуре. Также модели управления виртуальной средой в продуктах Open Source существенно отличаются от тех, к которым привыкли администраторы VMware.

В последние годы мы последовательно избавлялись от опенсорсной составляющей кода в наших программных продуктах и заменяли ее на нативный программный код, разработанной нашей командой. В настоящее время переписано уже более 40% имевшегося исторического опенсорсного кода.

Пример инфраструктуры с применением изделия представлен на рисунке 1.

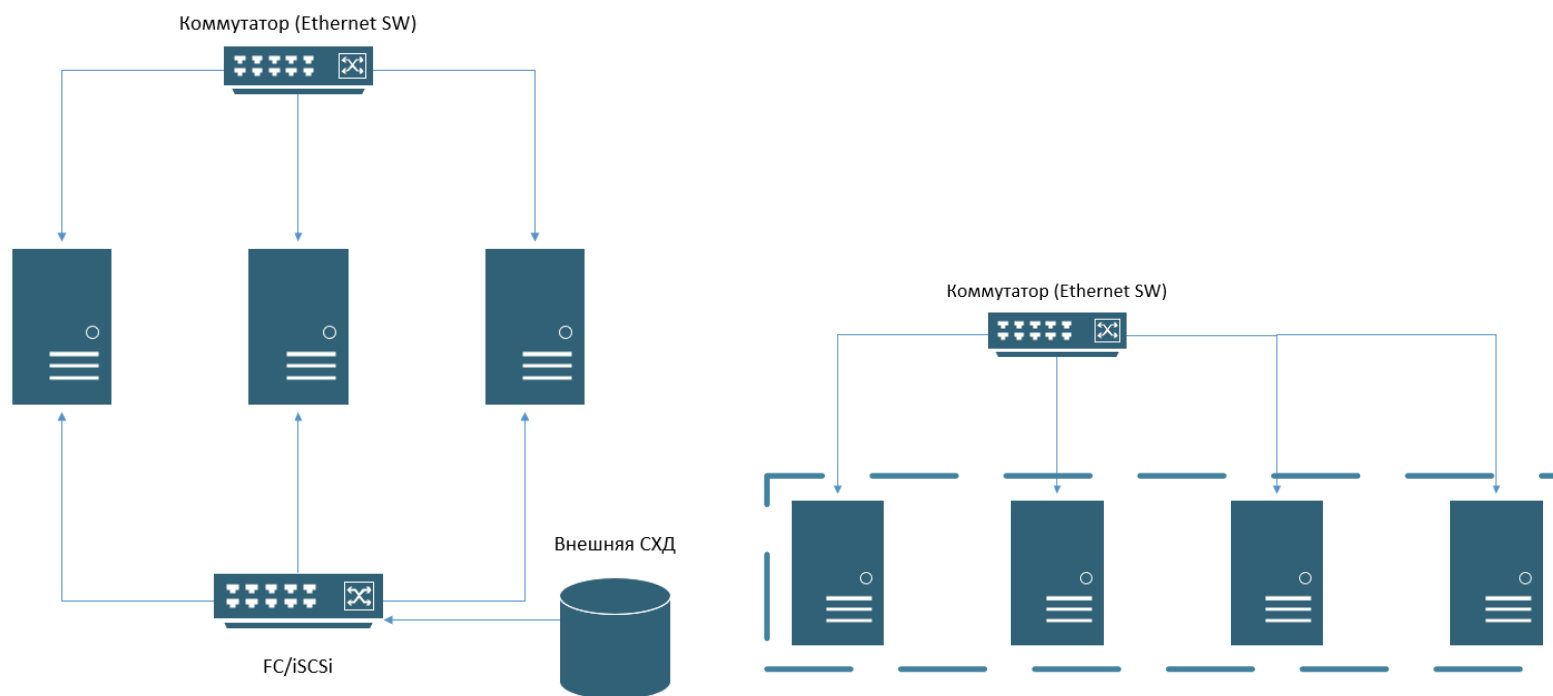


Рисунок 1 – Инфраструктурная схема для конвергентного и гиперконвергентного варианта

3 Функциональные характеристики ПК «Иридиум»

3.1 Защищенная специализированная закрытая ОС

Разработка продукта берет начало в 2009 году. ПК «Иридиум» изначально задумывался как защищенная сертифицированная отечественная система виртуализации. В процессе разработки продукта были разработаны более 150 патчей ядра операционной системы (как функциональные, так и патчи информационной безопасности). Из операционной системы было исключено все ПО, которое не имеет отношения к виртуализации, что сократило до минимума возможную площадь атаки. Был исключен менеджер пакетов с целью предотвращения установки ПО из сторонних репозиториях Open Source. С целью предотвращения запуска любого стороннего не одобренного вендором ПО был реализован динамический контроль исполняемого кода. Это предполагает проверку цифровой подписи при попытке запуска любого исполняемого кода (как бинарных файлов, так и модулей ядра). При неуспешной проверке цифровой подписи или ее отсутствии исполняемый код не запускается.

Таким образом, была разработана специализированная закрытая защищенная операционная система – гипервизор 1-го типа, которая устанавливается непосредственно на физические серверы. гипервизор I типа СВ “Звезда” включает гипервизор II типа — эмулятор QEMU. Ключевые особенности нашей специализированной закрытой защищенной операционной системы:

- Минимальная площадь атаки за счет исключения ПО, не относящегося к задачам виртуализации,
- Отсутствие возможности запуска стороннего не одобренного вендором ПО за счет динамического контроля исполняемого кода,
- Реализация встроенных средств защиты информации (СЗИ).

Вышеперечисленные особенности являются критичными для защищенной системы виртуализации, поскольку защищенность любой ИТ-системы не может быть выше защищенности платформы виртуализации, на которой развернута данная ИТ-

система. В случае применения ПК «Иридиум» возможно развертывание государственных информационных систем (ГИС) разных классов защищенности на одном и том же кластере и даже на одном и том же хосте виртуализации. Также за счет применения встроенных СЗИ допускается одновременное развертывание как сертифицированных, так и несертифицированных гостевых ОС на одном и том же хосте виртуализации. В защищенной операционной системе полностью исключается взлом гипервизора через гостевую ОС.

Гипервизор из состава ПК «Иридиум» сертифицирован ФСТЭК России как средство защиты информации (СЗИ) – сертификат № 4934, действителен до 05.05.2030.

3.2 Виртуальный коммутатор

В состав ПК «Иридиум» входит виртуальный сетевой коммутатор, максимально приближенный к функционалу виртуального коммутатора VMware vSphere.

Виртуальный коммутатор в ПК «Иридиум» является распределенным, что позволяет осуществлять централизованное управление сетевым функционалом платформы виртуализации.

3.3 Файловая система

В ПК «Иридиум» была полностью «с нуля» переписана подсистема ввода/вывода в части взаимодействия с СХД, а также была разработана кластерная файловая система – аналог VMware VMFS, по функционалу не уступающая VMware VMFS. Архитектура данной псевдо-файловой системы предполагает, что данные хранятся непосредственно в виде блоков на разделяемых LUN СХД, а наименования файлов и папок хранятся в виде метаданных. Сама прослойка файловой системы фактически отсутствует. Благодаря этому удалось достичь высоких показателей производительности подсистемы ввода/вывода - по результатам тестов, проведенных нашими заказчиками, производительность псевдо-файловой системы на 18-36%

превосходит производительность файловой системы VMFS от VMware, на том же самом аппаратном обеспечении.

3.4 Программно-определяемая СХД «Шторм»

В состав ПК «Иридиум» входит распределенная программно-определяемая СХД «Шторм», которая может быть использована для построения гиперконвергентных кластеров хранения на базе локальных дисков, установленных в физические хосты.

В гиперконвергентном кластере один и тот же хост виртуализации может одновременно участвовать в создании распределенного кластера хранения, и запускать продуктивные виртуальные машины.

Другой вариант – создание программно-определяемого кластера хранения на выделенных хостах (конвергентный кластер), и предоставление пространства хранения данного конвергентного кластера хостам виртуализации и другим системам по протоколам iSCSI, NFS, S3. Ближайший аналог программно-определяемой СХД «Шторм» – продукт VMware vSAN.

3.5 Система оркестрации

Весь интеллектуальный функционал системы виртуализации реализован в системе оркестрации, которая была разработана полностью «с нуля» и не основана ни на каких опенсорсных аналогах. Пример функционала, который реализован в системе оркестрации:

- Живая миграция ВМ между хостами виртуализации,
- Живая миграция виртуальных дисков ВМ между хранилищами,
- Отказоустойчивость хостов виртуализации (при падении хоста все ВМ автоматически перезапускаются на других хостах кластера),
- Отказоустойчивость самой системы оркестрации,
- Автоматическая балансировка нагрузки на хосты виртуализации,
- Многие другие функции.

Полнота функционала платформы виртуализации, реализованного в системе оркестрации, находится на уровне программных продуктов лидеров рынка (ближайшим аналогом является vCenter разработки компании VMware).

3.6 Модуль управления удаленными рабочими столами

Программный комплекс “Иридиум-VDI” – модуль управления удаленными рабочими столами (Virtual Desktop Infrastructure – VDI) предназначен для создания защищенных пользовательских сред на базе виртуальных рабочих столов Windows и Linux, а также с применением опубликованных приложений Windows и Linux. VDI-брокер обеспечивает следующие основные функции:

- Автоматическое развертывание ВМ с удаленными рабочими столами на платформе виртуализации,
- Аутентификация пользователей по внешним базам (Microsoft Active Directory, Open LDAP, FreeIPA и многие другие),
- Управление сессиями доступа к удаленным рабочим столам и опубликованным приложениям.

Разработан защищенный протокол доступа к удаленному рабочему столу на базе протокола SPICE. Разработанный протокол доступа предполагает использование таких кодеков, как H.264/H.265, и позволяет достичь превосходного качества видео, статических изображений, текста, аудио и т.д. при сравнительно низком использовании полосы пропускания (сопоставима с полосой, используемой протоколом RCoIP компании Teradici).

3.7 Резервное копирование и репликация

Модуль резервного копирования позволяет делать копии и восстанавливать ВМ на уровне образов виртуальных дисков. Также модуль резервного копирования позволяет реплицировать виртуальные диски ВМ между основной и удаленной

площадкой, позволяя строить катастрофоустойчивые решения на базе ПК «Иридиум».

Модуль резервного копирования позволяет делать резервные копии ВМ в процессе их работы, при этом консистентность данных на виртуальных дисках обеспечивается следующими двумя способами:

- Посредством агентского ПО, установленного в гостевую ОС, выполняется сброс данных из кэшей виртуальных контроллеров ВМ на виртуальный диск, после чего создается снимок состояния ВМ, и происходит резервное копирование «замороженного» базового виртуального диска ВМ. По окончании резервного копирования происходит консолидация снимка с базовым диском.
- Посредством создания слепка виртуальной памяти ВМ (вместе со всеми данными в кешах виртуальных контроллеров), после чего также создается снимок состояния ВМ, и происходит резервное копирование «замороженного» базового виртуального диска ВМ. При восстановлении ВМ виртуальная память восстанавливается из ранее сделанного слепка памяти.

3.8 Межсетевой экран

Модуль межсетевого экрана (МСЭ) предназначен для защиты виртуальных сетей с подключенными к ним ВМ. Он является сертифицированным МСЭ, а также сертифицированным средством криптозащиты информации (СКЗИ), обеспечивающим шифрование наложенных туннелей с использованием криптоалгоритмов ГОСТ.

- Максимальная скорость фильтрации до 50 Гбит/сек
- Фильтрация как на третьем уровне (маршрутизируемый режим), так и на втором уровне (режим коммутации или «прозрачный» МСЭ)
- Фильтрация по любым полям в заголовке сетевого пакета (вплоть до седьмого уровня)

- Фильтрация по расписанию
- Фильтрация по доменному имени
- Система обнаружения вторжений (СОВ), работает как в активном, так и пассивном режиме

3.9 Мониторинг

Модуль мониторинга обеспечивает отслеживание статуса всех компонент платформы виртуализации (хосты, виртуальные машины, хранилища), выявление неисправностей, сбор логов и прочей телеметрии, анализ информации, отображение ее в графическом виде и т.д. Ближайший аналог – продукт VMware Aria Operations.

4 Требования к минимальному составу технических средств

Для обеспечения нормальной работы ПК «Иридиум» в части выполнения всей заявленной функциональности, устанавливаются следующие минимальные технические требования:

Сервера для всех узлов с характеристиками не ниже:

- а) системный диск – минимум от 64 Гб, рекомендован SSD;
- б) 2-4 x 10/40 GB Ethernet.

Сервера управления и мониторинга (первые три узла кластера) с

- характеристиками не ниже: а) объем оперативной памяти – 2 Гб;
- б) объем жестких дисков – 64 Гб.

Сервера локального хранилища с характеристиками не ниже:

- а) 1 CPU на OSD диск;
- б) объем оперативной памяти – 4 Гб на OSD диск + 2% кэш-пространства;
- в) объем жестких дисков – 0-12 OSD дисков (от 64 Гб, рекомендован SSD).

Сервера iSCSI Target с характеристиками не

- ниже: а) 2 CPU;
- б) объем оперативной памяти – 16Гб.

5 Требования к программному обеспечению

ПК «Иридиум» функционирует на аппаратном обеспечении и не требует для своего запуска общесистемного ПО.

6 Требования к надежности

Средняя наработка на отказ - не менее 10000 часов.

Срок службы - 10 лет.

Гарантийный срок эксплуатации - 3 года.

7 Специальные требования

ПК «Иридиум» разработан с учетом следующих требований руководящих документов:

- Приказ ФСТЭК России № 17 “Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах” - в государственных информационных системах (ГИС) до 1 класса защищенности включительно;
- Приказ ФСТЭК России № 21 “Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных” для обеспечения защищенности персональных данных в информационных системах персональных данных (ИСПДн) до 1 уровня включительно;
- Приказ ФСТЭК России № 31 “Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды”, в автоматизированных системах управления технологическими процессами (АСУ ТП) до 1 класса защищенности включительно, значимых объектах критической информационной инфраструктуры (КИИ) до 1 категории включительно;
- Приказ ФСТЭК России от 11 апреля 2025 г. № 117 “Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений”;
- Требования по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения

безопасности информационных технологий (ФСТЭК России, 2020 г.) – по 4 уровню доверия;

– Требования по безопасности информации к средствам виртуализации (ФСТЭК России, 2022) – по 4 классу защиты;

– Требования по безопасности информации к средствам контейнеризации (ФСТЭК России, 2022) – по 4 классу защиты.