Акционерное общество «ИРИДИУМ»

ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

Платформа виртуализации ПК «Иридиум»

RU.УГСФ.00001-01 92 01

Листов 15

Москва, 2023

АННОТАЦИЯ

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

Указанные характеристики подсистемы подлежат представлению экспертной комиссии с целью проведения экспертных проверок.

СОДЕРЖАНИЕ

1 Общие Сведения

1.1 Основные сведения о ПК «Иридиум»

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

1.2 Назначение ПК «Иридиум»

Программное обеспечение (далее – ПО) ПК «Иридиум» предназначено для использования в частных и публичных облачных структурах.

1.3 Комплектность изделия

Обозначение изделия	Наименование изделия	Количество	Примечание
RU.УГСФ.00001-01	1 Программный комплекс “Иридиум” в составе:		Примечание 5
МБРЦ.468313.001	1.1 Программно-аппаратный комплекс (ПАК) “Горизонт-ВС”		Примечание 6
RU.КНРШ.00007-01	1.2 Система хранения данных “Шторм”		Примечание 7
RU.КНРШ.00006-01	1.3 Программное обеспечение подсистемы VDI		
RU.ЛНТФ.00001-01	1.4 Программный комплекс «Средство управления единичным хостом ПВ»		Примечание 8
RU.ЛНТФ.00002-01	1.5 Программный комплекс «Средство управления группой хостов ПВ»		Примечание 9
61649217.401200.003	1.6 Многофункциональный комплекс сетевой защиты «Diamond VPN/FW» (редакция для ПК «Иридиум»)		Примечание 10

Примечания

1 Количество и набор составных частей определяется по решению Заказчика спецификацией поставки.

2 Количество определяется спецификацией поставки.

3 Составные части ПК “Иридиум” поставляются на одном USB-носителе.

4 В приложении А даны контрольные суммы неизменяемых компонентов программного обеспечения (ПО) ПК “Иридиум”.

5 Программный комплекс “Иридиум” зарегистрирован в Реестре российского программного обеспечения (запись в реестре от 01.03.2023 №16819).

6 Комплекс программ “Терминал-Сервер” из состава ПАК “Горизонт-ВС” зарегистрирован в Реестре программ для ЭВМ (свидетельство о государственной регистрации № 2016618025

от 19.07.2016). Сертификат соответствия требованиям безопасности информации № 3723 выдан ФСТЭК России 21.03.2017, действителен до 21.03.2025.

7 Система хранения данных "Шторм" зарегистрирована в Реестре российского программного обеспечения (запись в реестре от 13.02.2023 №16626).

8. Программный комплекс «Средство управления единичным хостом ПВ» является опционально входящим в состав ПК «Иридиум» компонентом

9.Программный комплекс «Средство управления группой хостов ПВ» является опционально входящим в состав ПК «Иридиум» компонентом

10 Права на Многофункциональный комплекс сетевой защиты «Diamond VPN/FW» принадлежат ООО «ТСС». Сертификат ФСТЭК России № 4066 действителен до 24.01.2024, на соответствие требованиям документов: Требования доверия (4), Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ(Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), Профиль защиты МЭ(В четвертого класса защиты. ИТ.МЭ.В4.ПЗ), Требования к СОВ, Профили защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ).

1.4 Функциональные возможности ПК «Иридиум»

ПК «Иридиум» обеспечивает:

− установка непосредственно на аппаратное обеспечение без использования хостовой операционной системы (гипервизор 1 типа);

− создание и управление виртуальной средой на группе серверов (кластере);

− поддержка графического установщика;

− объединение физических серверов в кластер до 64 узлов, обеспечивающих постоянную доступность виртуальной машины с числом виртуальных процессоров не менее 4, даже в случае отказа физического сервера;

− обеспечение возможности использования в качестве гостевой ОС операционных систем семейств Linux, Windows;

− функционирование средств защиты информации:

  − 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;

– наличие сертифицированной и несертифицированной версии изделия;

– поддержка функции Multipathing;

– создание виртуальных машин (ВМ), их образов и шаблонов с поддержкой 32 и 64-битных гостевых операционных систем;

– возможность создания ВМ из настраиваемых шаблонов с помощью графического и консольного интерфейсов;

– возможность группового создания ВМ из шаблонов;

– поддержка в ВМ до 240 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;

– 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 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;

– поддержка открытого стандарта Open Virtualization Format (OVF);

– возможность подключения внешних хранилищ по протоколу FC;

– возможность клонирования ВМ;

– возможность создания кластеров высокой доступности, выполняющих перезапуск ВМ в случае выхода из строя узла кластера;

– возможность переноса ВМ между узлами кластера без прерывания трафика;

– обеспечение автоматического распределения сервером виртуализации ресурсов между работающими ВМ;

– миграция дисков работающих ВМ между хранилищами без их остановки;

– сервисный режим обслуживания узла с автоматическим перемещением работающих ВМ без их остановки;

– возможность централизованного управления кластерами, серверной частью изделия на всех узлах кластера высокой доступности, хранилищами и виртуальными коммутаторами;

– возможность мониторинга работоспособности и использования ресурсов ВМ;

– поддержка виртуальных коммутаторов с технологией VLAN (Virtual Local Area Network);

– 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;

– поддержка механизмов оптимизации оперативной памяти:

  – дедупликация страниц;

  – динамическое распределение;

  – выгрузка в файл подкачки, область подкачки, сформированную на постоянном накопителе, либо оперативной памяти;

  – Memory Balooning;

– 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;

– 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;

– поддержка создания программно-определяемой СХД;

– возможность параллельного доступа нескольких ВМ к одному виртуальному диску;

– возможность централизованного обновления с использованием штатных средств;

– возможность резервирования интерфейсов управления инфраструктурой виртуализации;

– возможность размещения контроллера на хосте (без использования дополнительного физического сервера);

– возможность создания снэпшотов ВМ;

– миграция ВМ из сред виртуализации, в том числе VMware;

– создание шаблона на базе существующей ВМ.

– поддержка Affinity Rule – размещение выбранных ВМ на одном хосте виртуализации и Anti-Affinity Rule – размещение выбранных ВМ на разных хостах виртуализации;

– 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;

– функционирование в условиях мандатного и/или дискреционного разграничения доступа при межпроцессном и сетевом взаимодействии, включая взаимодействие между ВМ по протоколам стека IPv4 в условиях мандатного разграничения доступа и доступ субъектов к файлам-образам и экземплярам функционирующих ВМ;

– 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;

– регистрация событий с использованием средств централизованного протоколирования;

– регулярное обновление для нейтрализации угроз эксплуатации уязвимостей;

– управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

– разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

– интерфейс на русском языке с возможностью переключения на иностранный язык.

– 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, ceph и S3-хранилища).

2 Архитектура Подсистемы

ПК «Иридиум» состоит из группы серверов.

Архитектурная схема изделия представлена на рисунке 1.

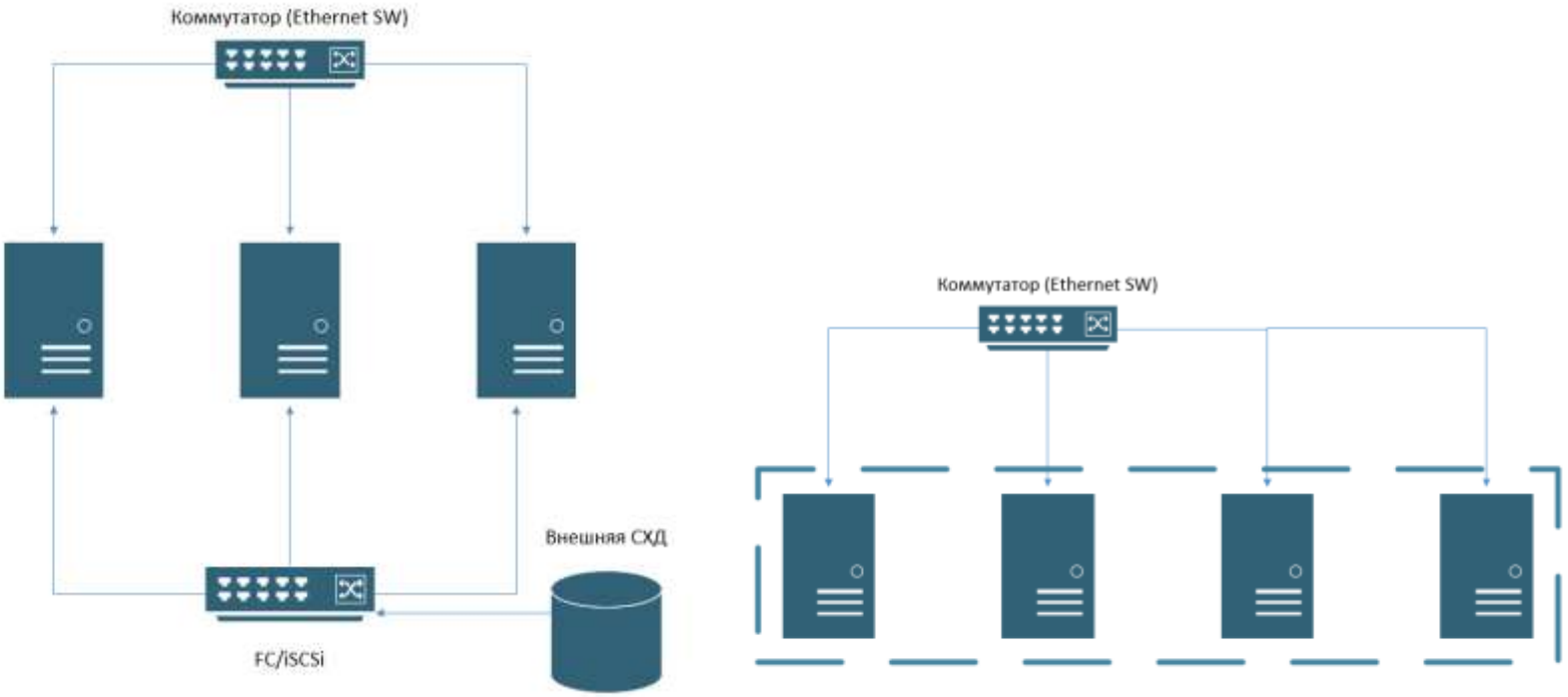

Рисунок 1 – Архитектурная схема

3 Функциональные характеристики ПК «Иридиум»

Функциональные характеристики изделия удовлетворяют следующим требованиям:

Характеристика	**Показатель**
Количество процессоров сервера виртуализации, поддерживаемых гипервизором	от 2 до 4096
Объем оперативной памяти сервера виртуализации, поддерживаемый гипервизором	от 4 Гб до 256 Тб
Объем жесткого диска сервера виртуализации	не менее 100 Гб
Количество процессорных сокетов	не менее 2
Суммарное количество физических ядер сервера виртуализации	не менее 4 до 2048
Количество виртуальных ЦПУ, поддерживаемых одной ВМ	от 2 до 256
Количество памяти, поддерживаемой ВМ	от 1 Гб до 32 Тб
Поддержка виртуальных накопителей в ВМ объёмом (максимальное значение ограничено аппаратными возможностями сервера виртуализации)	от 4 Гб
Количество виртуальных процессоров, поддерживаемых ВМ	от 2 до 2048
Возможность организации виртуальных сетевых интерфейсов со скоростями	до 10 Гбит/с
Возможность объединения физических серверов в кластер высокой доступности, с автоматическим перезапуском виртуальных машин в случае отказа физического сервера	до 200 узлов
Возможность создания в одной зоне Федерации или локации кластера высокой доступности из группы серверов	не менее чем 300 хостов суммарно
Основные поддерживаемые ОС семейства Windows	Windows Server 2016; Windows Server 2012 R2; Windows Server 2012; Windows Server 2008 R2 with Service Pack 1; Windows XP/7/10

Основные поддерживаемые ОС семейства Linux	AltLinux 8; AstraLinux 2.12; AstraLinux 1.5; AstraLinux 1.6; CentOS 8.x; CentOS 7.x; CentOS 6.x; Debian 10.x; Debian 9.x; Debian 8.x; Debian 7.x; Ubuntu 17.10; Ubuntu 16.04 LTS; Ubuntu 14.04 LTS; openSUSE 42.x; SLES 11; SLES 12; SLES 15; Oracle
	Linux 8.x; Oracle Linux 7.x; Oracle Linux 6.x; Oracle Linux 5.x; Oracle Enterprise Linux 4.x; Red Hat Enterprise Linux (RHEL), Oracle DB
Совместимое серверное оборудование	Hewlett Packard Enterprise, Huawei, Lenovo, Cisco, Dell-EMC, Fujitsu, IBM, Depo Computers, Аквариус, Булат, Т-Платформы.
Объем поддержки томов	Более 2 Тб
Поддержка ПО SAP	SAP, SAP ASE, SAP MaxDB
Поддержка систем управления реляционным базам данных	MS SQL, IBM DB2, PostgreSQL

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

Подсистема 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

Подсистема разработана 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 Состава 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;

− «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992 г.) – по 5 классу защищенности;

− Требования по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (ФСТЭК России, 2018 г.) – по 4 уровню доверия.