ГОРИЗОНТ-ВС

ЦИФРОВОЕ БУДУЩЕЕ
НАЧИНАЕТСЯ СЕГОДНЯ

Платформа виртуализации

ПАК «Горизонт-ВС»

Оглавление

Введение 3

Применение 4

Продуктовая линейка 4

Серверная виртуализация инфраструктуры «Горизонт-ВС» 4

Возможности: 5

Особенности 5

Применение: 5

Гиперконвергентное решение виртуализации вычислительной инфраструктуры «Горизонт-ВС» 6

Возможности: 6

Особенности 7

Применение: 7

Защищенное удаленное рабочее место «Горизонт-ВС» 7

Возможности 7

Особенности 8

Архитектура 8

Комплекс программ «Терминал-Сервер» 10

Сервер виртуальных машин 10

Тонкий клиент 13

Администратор безопасности 14

Модуль идентификации и контроля доверенной среды «Шина» 14

Режим «Терминал» 14

Режим «Сервер» 15

Режим «АРМ Администратора» 15

Пример конфигурации 16

Сертификаты и совместимость 18

Техническая поддержка 22

Уровень Базовый 23

Уровень Расширенный 23

Введение

Программно-аппаратный комплекс виртуализации «Горизонт-ВС» является лидирующим, отечественным, гиперконвергентным решением виртуализации, включающим в себя полный перечень подсистем, позволяющих создавать защищенные корпоративные платформы и центры обработки данных, обеспечивающие следующий функционал:

- Виртуализация вычислительных ресурсов;
- Виртуализация распределенных систем хранения данных;
- Виртуализация сетевых ресурсов;
- Виртуализация рабочих мест.

ПАК «Горизонт-ВС – единственная в России сертифицированная платформа виртуализации, являющаяся полноценным средством защиты информации (СЗИ), благодаря чему она может использоваться как самостоятельное законченное решение в государственных информационных системах (ГИС) до 1 класса защищенности и для обеспечения защищенности персональных данных до 1 уровня включительно.

ПАК «Горизонт-ВС» входит в Государственный Реестр сертифицированных средств защиты информации ФСТЭК Российской Федерации и имеет сертификат соответствия требованиям по безопасности информации ФСТЭК России (№ 3723 от 21.03.2017 г.):

- по 5-му классу защищенности от несанкционированного доступа к информации;
- по 4-му классу защиты средств доверенной загрузки на уровне платы расширения;
- имеет 4-ый уровень контроля отсутствия недекларированных возможностей.

Таким образом защищенная платформа виртуализации «Горизонт-ВС» в полной мере применима для построения решений для субъектов критической информационной инфраструктуры, а также для построения информационных систем, требующих последующую аттестацию в области информационной безопасности:

- в государственных информационных системах (ГИС) до 1 класса защищенности включительно,
- для обеспечения защищенности персональных данных в информационных системах персональных данных (ИСПДн) до 1 уровня включительно,

- в автоматизированных системах управления технологическими процессами (АСУ ТП) до 1 класса защищенности включительно,
- на значимых объектах критической информационной инфраструктуры (КИИ) до 1 категории включительно.

ПАК «Горизонт-ВС» - российское решение, имеет многоуровневую систему защиты информации от несанкционированного доступа, оснащено системой доверенного подключения и доверенной загрузки и по своим функциональным возможностям и производительности сопоставимо с зарубежными аналогами.

ПАК «Горизонт-ВС» включен в единый реестр российских программ для электронных вычислительных машин и баз данных Минкомсвязи России.

- Регистрационный номер Комплекса программ «Терминал-Сервер» в реестре – №2338.
- Регистрационный номер Модуля идентификации и контроля доверенной среды «Шина» – №2340.

Применение

ПАК «Горизонт-ВС» может быть применим в крупных и средних компаниях и государственных органах для целей модернизации и защиты, имеющихся ИТ-ресурсов и ЦОД:

- в органах государственной власти
- оборонно-промышленном комплексе
- телекоммуникационной сфере
- банковском секторе
- топливно-энергетическом комплексе
- здравоохранении

Продуктовая линейка

Серверная виртуализация инфраструктуры «Горизонт-ВС»

Решение серверной виртуализации применимо для реализации проектов по

построению защищенной и отказоустойчивой виртуализованной инфраструктуры на основе типовых x86 узлов.

Обеспечивается централизованное управление и поддержка внешних СХД

Возможности:

- Построение аттестованных ГИС, ИСПдН, АСУ ТП и объектов КИИ
- Гипервизор первого типа, не требующий хостовой ОС
- Защищенная отказоустойчивая платформа виртуализации с возможностью масштабирования
- Централизованное управление всеми ресурсами управляемой инфраструктуры, включая управление хост-серверами, LAN, распределенными коммутаторами
- Поддержка внешних СХД
- Кластеризация хост-серверов, с автоматическим восстановлением работы виртуальных машин в случае выхода из строя одного или нескольких хост-серверов кластера
- Возможность сбора и анализа логов всей используемой инфраструктуры
- Поддержка интеграции с СРК для выполнения полных и инкрементальных резервных копий виртуальных машин
- Поддержка технологий оптимизации работы с памятью, такие как Memory Deduplication (KSM), Memory Ballooning, Hugepages
- Поддержка 32- и 64-битных гостевых ОС семейств Linux, Windwos, работающих на серверах стандартной архитектуры x86 (в том числе и устаревших ОС, типа МСВС итд)
- Автоматизация предоставления персонализированной инфраструктуры и приложений
- Поддержка наиболее распространенных серверных платформ как иностранного (HPE, Lenovo, Huawei), так и отечественного производства (DEPO, Булат, Kraftway)

Особенности

- Установка на аппаратное обеспечение
- Полнофункциональная СГУ
- Отказоустойчивость
- Непрерывный кластер

Применение:

- Государственные информационные системы (до 1 класса) и информационные системы персональных данных (до 1 уровня защищенности).
- Построение частных облачных структур
- ЦОД

Гиперконвергентное решение виртуализации вычислительной инфраструктуры «Горизонт-ВС»

Полнофункциональное решение для построения горизонтально и вертикально масштабируемой ИТ-инфраструктуры с распределенной СХД
Повышенная отказоустойчивость, доверенная среда, централизованное управление всеми функциями.

Возможности:

- Построение аттестованных ГИС, ИСПдН, АСУ ТП и объектов КИИ
- Гипервизор первого типа, не требующий хостовой ОС
- Защищенная отказоустойчивая гиперконвергентная платформа виртуализации с возможностью масштабирования: как вертикальное - наращивание мощности отдельных серверов, так и горизонтальное - добавление серверов для распределения нагрузки
- Возможность создания гиперконвергентной отказоустойчивой СХД на базе локальных дисков хостов
- Централизованное управление всеми ресурсами управляемой инфраструктуры, включая управление хост-серверами, LAN, СХД, распределенными коммутаторами
- Кластеризация хост-серверов, с автоматическим восстановлением работы виртуальных машин в случае выхода из строя одного или нескольких хост-серверов кластера
- Возможность сбора и анализа логов всей используемой инфраструктуры
- Поддержка интеграции с СРК для выполнения полных и инкрементальных резервных копий виртуальных машин
- Поддержка технологий оптимизации работы с памятью, такие как Memory Deduplication (KSM), Memory Ballooning, Hugepages
- Поддержка 32- и 64-битных гостевых ОС семейств Linux, Windwos, работающих на серверах стандартной архитектуры x86 (в том числе и устаревших ОС, типа МСВС итд)

- Автоматизация предоставления персонализированной инфраструктуры и приложений
- Поддержка наиболее распространенных серверных платформ как иностранного (HPE, Lenovo, Huawei), так и отечественного производства (DEPO, Булат, Kraftway)

Особенности

- Установка на аппаратное обеспечение
- Полнофункциональная СГУ
- РСХД
- Отказоустойчивость
- Непрерывный кластер

Применение:

- Государственные информационные системы (до 1 класса) и информационные системы персональных данных (до 1 уровня защищенности).
- Гиперконвергентная инфраструктура частных компаний
- ЦОД

Защищенное удаленное рабочее место «Горизонт-ВС»

Гибко масштабируемое, отказоустойчивое решение удаленного доступа к рабочим столам пользователя с поддержкой всех российских и зарубежных операционных систем. Защищенная сертифицированная инфраструктура, собственный тонкий клиент

Возможности

- Управление публикацией рабочих столов и приложений на основании членства пользователей в группах безопасности Active Directory/Open LDAP
- Ограничение выделения ресурсов под нужды конкретного пользователя
- Поддержка печати на локальные и сетевые принтеры, подключенные на рабочем месте пользователя
- Поддержка проброса USB-устройств с рабочего места пользователя, в том числе микрофонов, принтеров, смарт-карт и токенов
- Полностью защищенная сертифицированная инфраструктура, установка безопасного соединения между тонким клиентом и гипервизором

- Обслуживание десятков тысяч одновременных пользовательских подключений
- Тонкий клиент как общесистемное ПО, так и приложение под ОС Linux

Особенности

- Собственный тонкий клиент
- Отказоустойчивость
- Непрерывный кластер

Совместимость

Поддержка виртуальных машин с операционными системами из реестра Российского ПО, в том числе на базе Linux.

Разработанная платформа успешно интегрирована с отечественными архитектурами «Байкал» и «Эльбрус».

Архитектура

ПАК «Горизонт-ВС», предназначен для использования аппаратных возможностей процессорной архитектуры x86-64 для функционирования виртуальных машин и управления доступом к ним.

В составе гипервизора ПАК «Горизонт-ВС» отсутствует операционная система общего назначения, управление производится операционной средой ПАК «Горизонт-ВС», представляющей собой встроенное ПО, состоящее из пространства ядра и пользовательского пространства.

Гипервизор ПАК «Горизонт-ВС» поддерживает виртуальные машины с несколькими виртуальными процессорами и не менее 256 ГБ оперативной памяти, а также хост-системы с 256 ядрами и более 1 ТБ ОЗУ.

В ПАК «Горизонт-ВС» реализован непрерывный кластер. Задача создания кластера заключается в обеспечении согласованной работы всех узлов для достижения поставленной цели. Целью может быть высокая устойчивость или доступность (HA, High Availability), высокая вычислительная способность (HP, High Performance), параллельное вычисление, параллельное обслуживание запросов.

Для создания кластерного хранилища с числом хостов равным двум, применяется

подход создания реплицируемого блочного устройства.

Для создания кластерного хранилища с числом хостов больше двух, применяется подход создания реплицируемого блочного устройства, либо распределённой файловой системы средствами ПАК «Горизонт-ВС».

Для резервирования технических средств из состава серверов виртуализации, в платформе «Горизонт-ВС» имеется поддержка следующих программных, аппаратных и смешанных технологий:

– подсистема памяти: имеется поддержка ECC памяти и механизм восстановления после сбоев;

– дисковая подсистема и система хранения данных: поддерживается большинство современных аппаратных средств создания отказоустойчивых локальных хранилищ (RAID ит.д.), имеется возможность создания программных RAID, создание программно-определяемых, в том числе распределенных отказоустойчивых хранилищ, с применением технологий кластеризации;

– сетевая подсистема: поддержка агрегации сетевых каналов с использованием различных алгоритмов включая LACP;

– вычислительная подсистема: реализуется за счет применения облачных технологий высокой доступности (High Availability), базирующихся на технологиях отказоустойчивости и кластеризации систем хранения данных.

В ПАК «Горизонт-ВС» реализована модульная архитектура, которая позволяет создавать гибкие инфраструктуры. Возможно подключение внешних хранилищ данных, в том числе и по протоколу Fibre Channel, для хранения образов дисков виртуальных машин и данных. Для улучшения пропускной способности системы хранения данных и резервирования может использоваться многопоточный ввод/вывод. При этом возможна перенастройка путем подключения соответствующих модулей и организация программно-определяемых хранилищ данных средствами гипервизора «Горизонт-ВС».

ПАК «Горизонт-ВС» является многокомпонентным распределённым комплексом с единой политикой безопасности и включает в себя две основные функциональные части:

– модуль идентификации и контроля доверенной среды (далее по тексту – «Шина»)

– комплекс программ «Терминал-Сервер» (далее по тексту – КП «Терминал-Сервер»).

Комплекс программ «Терминал-Сервер»

Непосредственно функциональные возможности по исполнению виртуальных машин и управлению доступом к ним реализованы в КП «Терминал-Сервер». КП «Терминал-Сервер» является гипервизором, устанавливаемым непосредственно на аппаратное обеспечение в качестве системного программного обеспечения (гипервизором I типа[1]). КП «Терминал-Сервер» обеспечивает защищённое исполнение виртуальных машин, а также подключение терминалов к виртуальным машинам, исполняемым на сервере виртуализации, и состоит из трех компонентов:

– компонент «Тонкий клиент» (далее по тексту – «Клиент»), который устанавливается на персональные электронные вычислительные машины (ПЭВМ), выполняющие функции терминала;

– компонент «Сервер виртуальных машин» (далее по тексту – «Сервер»), который устанавливается на ПЭВМ, выполняющие функции сервера виртуализации;

– компонент «Администратор безопасности» (далее по тексту – «Администратор»), который устанавливается на ПЭВМ, выполняющие функции автоматизированного рабочего места (АРМ) администратора.

«Сервер» предоставляет возможность создания и редактирования виртуального аппаратного окружения виртуальных машин, исполнение виртуальных машин и управление доступом к ним.

«Клиент» предназначен для подключения тонких клиентов по протоколу SPICE к виртуальным машинам, исполняемым на сервере виртуализации. «Клиент» обеспечивает доверенное подключение к серверу виртуализации. Подключение можно считать доверенным, если на момент подключения средствами «Сервера» установлена достоверность подключаемого терминала, а средствами «Клиент» установлена достоверность сервера виртуализации, к которому производится подключение. Проверка достоверности осуществляется с использованием механизмов, реализованных «Шина».

Сервер виртуальных машин

К функциональному назначению компонента «Сервер» относятся:

[1] ГОСТ Р 56938-2016 Защита информации. Защита информации при использовании технологий виртуализации. Общие положения

– поддержка графического установщика;

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

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

– создание и редактирование ВМ;

– обеспечение возможности использования в качестве гостевой операционной системы (ОС) операционных систем семейств Linux, Windwos;

– поддержка 32- и 64-битных гостевых ОС, работающих на серверах стандартной архитектуры x86;

– возможность предоставления суммарного объема оперативной памяти виртуальным средам больше, чем доступно на физическом сервере, за счет применения динамического перераспределения памяти между виртуальными средами и освобождением неиспользуемой памяти;

– возможность автоматического восстановления работы виртуальной среды (режим высокой доступности ВМ в случае отказа одного из серверов виртуализации с помощью автоматического перезапуска ВМ на работоспособных серверах);

– возможность включения или отключения режима высокой доступности для каждой ВМ;

– возможность создания шаблонов ВМ и быстрого развертывания виртуальных машин из этих шаблонов;

– создание «снимка» работающей ВМ (контрольной точки состояния операционной системы виртуальной машины на уровне файловой системы, обеспечивающей возврат в произвольный момент вернуться к состоянию на момент создания контрольной точки);

– возможность миграции (переноса исполнения) виртуальных машин между серверами виртуализации;

– создание и хранение образов ВМ для автоматического развертывания ВМ;

– создание виртуальных сетевых мостов, а также использование для изоляции и/или объединения в виртуальные сети сетевого трафика виртуальных машин следующих протоколов: VLAN (IEEE 802.1Q); VXLAN (RFC-7348);

– возможность предоставления доступа к хранилищу данных через протоколы iSCSI, NFS, CIFS/SMB;

– поддержка технологий оптимизации работы с памятью, такие как Memory Deduplication (KSM), Memory Ballooning, Hugepages;

– возможность управления с использованием графического

интерфейса, доступного из веб-браузера;

– возможность управления виртуальными средами посредством графического интерфейса в следующем объёме:

- создание и редактирование виртуального окружения виртуальных машин (формирование виртуальной аппаратной конфигурации: определение количества процессоров, объёма оперативной памяти, количества и объёма дисков, количества и параметров сетевых интерфейсов);
- регистрация физических серверов виртуализации;
- создание логических структур (кластеров) на базе физических серверов виртуализации;
- создание и управление шаблонами виртуальных машин;
- создание и управление образами виртуальных машин;
- управление ресурсами виртуальных машин (ЦПУ, оперативная память, дисковое пространство);
- управление и добавление устройств в виртуальные машины;
- выполнение групповых операций с виртуальными машинами;
- мониторинг загрузки процессора, памяти, диска и сети в ВМ;
- управление сервисами формирования отказоустойчивого кластера;
- создание и редактирование виртуальных сетевых мостов;
- возможность миграции виртуальных дисков в процессе работы ВМ;
- возможность миграции функционирующих ВМ между хостами с процессорами разных поколений;
- поддержка функции Multipathing;
- поддержка создания программно-определяемой СХД/ распределенной СХД на базе ПО из состава платформы гипервизора;
- возможность одновременного использования дисков SSD, SAS и SATA разной емкости для реализации хранилища данных;
- возможность конвертации физических серверных систем в виртуальные машины, реализованные на базе подсистемы виртуализации;
- поддержку стандарта VirtIO виртуализации дисковых и сетевых устройств;
- возможность обеспечения доступа сервисов виртуальных машин к USB-портам хостового сервиса и подключаемых терминалов без установки дополнительных драйверов на тонких клиентах;

- доверенное подключение терминалов к серверам виртуализации с использованием функционала диспетчера подключений, проксирования и балансировки подключений;
- ведение журнала регистрации событий;
- защита ввода и вывода на отчуждаемый носитель информации;
- тестирование всех функциональных блоков;
- протоколирование сбойных ситуаций;
- восстановление системы после сбоя;
- непрерывная круглосуточная работа;
- реализация функций безопасности:
- идентификация и аутентификация;
- разграничение доступа к управлению ПАК;
- управление работой ПАК;
- управление параметрами ПАК;
- аудит безопасности ПАК;
- тестирование ПАК, контроль целостности программного обеспечения и параметров ПАК;
- контроль компонентов СВТ;
- блокирование загрузки операционной системы средства доверенной загрузки
- СДЗ);
- сигнализация СДЗ;
- дискреционный контроль доступа;
- защита остаточной информации;
- управление компонентами виртуальной инфраструктуры.

Тонкий клиент

Компонент «Клиент» обеспечивает выполнение следующих функций:

- вывод графической и звуковой информации терминала;
- ввод информации с клавиатуры терминала в виртуальную машину;
- подключение манипулятора типа “мышь” терминала к виртуальной машине;
- ввод звуковой информации в ВМ через микрофон терминала;
- подключение USB-устройств терминала к виртуальной машине;
- предоставление средств для настройки сетевых параметров соединения терминала,

ввода информации для авторизации пользователя, настройки режима работы терминала;

- доверенную загрузку программного обеспечения терминала;
- протоколирование сбойных ситуаций;
- восстановление системы после сбоя;
- непрерывную круглосуточную работу.

Администратор безопасности

Компонент «Администратор» обеспечивает:

- конфигурирование административной группы (регистрацию и удаление узлов);
- регистрацию, удаление и блокировку пользователей на всех узлах административной группы;
- администрирование ключей (генерацию ключей маскирования и аутентификации, выполнение операций рассылки и смены ключей);
- чтение журналов регистрации событий всех узлов, входящих в административную группу;
- подключение шлюзов административной группы и установку связи между административной группы, входящими в одну серию.

Модуль идентификации и контроля доверенной среды «Шина»

«Шина» используется в клиент-серверных системах для защиты АРМ, являющихся терминалами, серверами виртуализации и АРМ администратора от несанкционированного доступа (НСД).

«Шина» работает в трех режимах:

- режим «Терминал» – устанавливается на терминале;
- режим «Сервер» – устанавливается на сервере виртуализации;
- режим «АРМ Администратора» – устанавливается на АРМ Администратора.

Режим «Терминал»

«Шина» обеспечивает выполнение следующих основных функций при работе в режиме «Терминал»:

- идентификацию и аутентификацию администраторов/пользователей;

- доверенную загрузку специального программного обеспечения (СПО);
- контроль целостности СПО;
- блокировку работы терминала в случае неудачной идентификации и аутентификации администратора/пользователя;
- ведение журнала регистрации событий, регистрирующего события имеющие отношение к безопасности системы;
- блокировку входа в систему зарегистрированного пользователя в следующих случаях: нарушение целостности контролируемой информации СПО; превышение предельного числа неудачных попыток входа и истечение срока действия пароля; блокирование администратором входа пользователя;
- самотестирование (проверка технического состояния).

Режим «Сервер»

При работе в режиме «Сервер» основные функции «Шина» аналогичны функциям в режиме «Терминал».

Режим «АРМ Администратора»

При работе в режиме «АРМ Администратора» функции «Шина» в режиме «Терминал» дополняются механизмом удаленного администрирования, обеспечивающего следующие основные функции:

- регистрацию и удаление пользователей в изделии, установленном на удаленном терминале или сервере виртуализации;
- блокировку и разблокировку пользователей в изделии, установленном на удаленном терминале или сервере виртуализации;
- работу с журналом регистрации событий изделия, установленного на удаленном терминале или сервере виртуализации;
- мониторинг состояния «Шина» в административной группе (группе серверов виртуализации и терминалов, в которой работают пользователи);
- генерацию ключей маскирования;
- рассылку ключей маскирования;
- смену ключей маскирования;
- смену паролей администраторов и пользователей;

- создание инсталляционного ключа, транспортного ключа и электронных ключей аутентификации пользователей и администраторов.

Пример конфигурации

Схема используемых аппаратных средств представлена на рисунке 1.

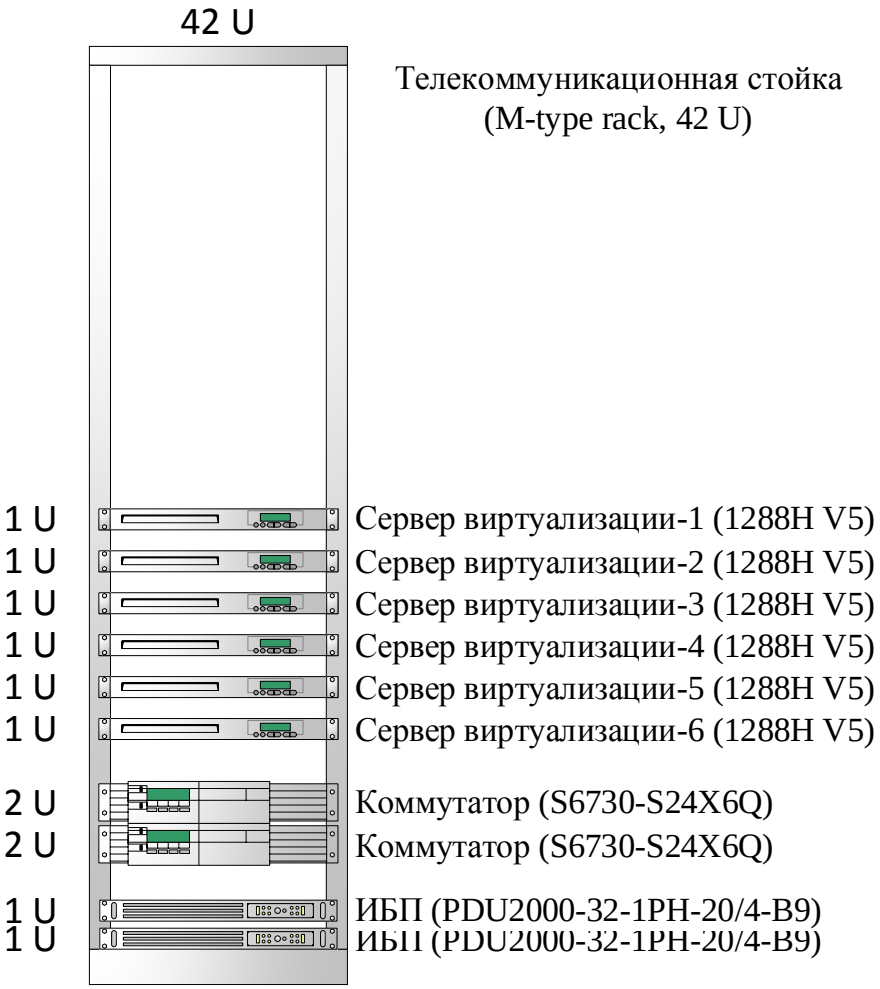

Рисунок 1

Конфигурация оборудования приведена в таблице 1.

Таблица 1 – Конфигурация оборудования

Обозначение	**Аппаратная конфигурация**	**Программная конфигурация**	**Описание**
Сервер виртуализации-1,2,3,4,5,6	1288H V5 (10*SAS/SATA HDD Chassis, Support 4 NVMe SSDs, With 2*GE	Файлы «Горизонт-ВС» БПУ ПК	Двухсокетный стоечный сервер Huawei FusionServer 1288H V5

Обозначение	Аппаратная конфигурация	Программная конфигурация	Описание
	and 2*10GE SFP+(Without Optical Transceiver)) H12H-05(For oversea). Процессор Intel Xeon Silver 4216(2.1GHz/16-Core/22MB/100W)Cascade lake Processor (with heatsink). Память 12 DDR4 RDIMM,32GB. 2 SSD,3840GB,SATA 6Gb/s. 1 SSD,960GB,NVMe PCIe. SR150-M(Avago3408) SAS/SATA RAID Card-RAID0,1,10-12Gb/s-no Cache	«Звезда» (устанавливаются на ПЭВМ, выполняющую функции сервера виртуализации). Программный пакет Система группового управления ПАК "ЗВЕЗДА". Кластер системы группового управления. Дополнительный диспетчер VDI подключений. Дополнительный диспетчер VDI подключений Дополнительный диспетчер VDI подключений Дополнительный диспетчер VDI подключений	высотой 1U. Предназначен для запуска гиперконвергентной платформы виртуализации ПАК «Звезда» на базе программного обеспечения «Горизонт-ВС». На серверах виртуализации организуется отказоустойчивый кластер с общей разделяемой системой хранения данных на базе локальных дисковых подсистем серверов – участников кластера. Отказоустойчивость достигается за счет использования функций НА кластера «Горизонт-ВС» и функций обеспечения отказоустойчивости РСХД на базе ПО «Горизонт-ВС». Для коммутации серверов между собой используется 10G

Обозначение	Аппаратная конфигурация	Программная конфигурация	Описание
			Ethernet-коммутатор с функциями агрегации каналов связи. Кроме серверной виртуализации реализуется инфраструктура виртуальных рабочих столов (VDI)
Коммутатор	S6730-S24X6Q (24*10GE SFP+ ports, 6*40GE QSFP ports, without power module)	-	Коммутатор Huawei CloudEngine S6730-S24X6Q с коммутационной емкостью 960 Гб/с / 2.4Тб/с, фиксированными 24 портами по 10 Gig SFP+,6 x 40 Gig QSFP+
Бесперебойный источник питания	Rack Power Distribution Unit,Basic Type-PDU2000-32-1PH-20/ 4-B9-20* C13+4* C19-Full height vertical-NO Industrial connector-Free mounting plate	-	

Сертификаты и совместимость

Программно-аппаратный комплекс является сертифицированным (сертификат ФСТЭК России) средством защиты информации и соответствует требованиям документов:

- «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля;
- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности. «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013),
- «Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты. ИТ.СДЗ.ПР4.ПЗ» (ФСТЭК России, 2013).

На изделие оформлены авторские свидетельства о государственной регистрации программы для ЭВМ:

- Свидетельство на комплекс «Терминал-Сервер»;
- Свидетельство на программу «Администратор модуля идентификации и контроля доверенной среды».

ПАК внесен в реестр отечественного программного обеспечения Минкомсвязи.

Согласно приказам № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России, сертифицированное изделие может использоваться в государственных информационных системах до 1 класса защищенности и для обеспечения защищенности персональных данных до 1 уровня включительно и реализует следующие меры защиты информации:

- ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора;
- ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

- УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- УПД.6 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- УПД.17 Обеспечение доверенной загрузки средств вычислительной техники;
- ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;
- РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения;
- РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- РСБ.6 Генерирование временных меток и (или) синхронизация системного времени в информационной системе;
- РСБ.7 Защита информации о событиях безопасности;
- РСБ.8 Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе;
- ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;
- ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;
- ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;
- ЗСВ.3 Регистрация событий безопасности в виртуальной инфраструктуре;
- ЗСВ.5 Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией;

- ЗСВ.6 Управление перемещением виртуальных машин(контейнеров) и обрабатываемых на них данных;
- ЗСВ.7 Контроль целостности виртуальной инфраструктуры и ее конфигураций;
- ЗСВ.8 Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;
- ЗСВ.10 “Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей;
- ЗИС.1 Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы;
- ЗИС.21 Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы;
- ЗИС.29 Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы.

Для применения изделия в государственных информационных системах 2 класса защищенности и ниже предусмотрен режим работы ПАК без «Шина», при этом все функции безопасности реализуются в КП «Терминал-Сервер».

Дополнительно разработан вариант исполнения – программное изделие «Базовые средства виртуализации вычислительных процессов защищенных операционных систем», предназначенное для обеспечения соответствия:

- требованиям руководящего документа ФСТЭК России «Защита от НСД. Часть 1.
- Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999г.) - по 2 уровню контроля;
- требованиям руководящего документа ФСТЭК России «Средства вычислительной

техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992г.) - по 3 классу защищенности;

- реальных и декларируемых в документации функциональных возможностей.

На ПИ оформлено авторское свидетельство о государственной регистрации программы для ЭВМ г.

Также были успешно проведены демонстрационные испытания сертифицированного ПИ. По результатам работы комиссии рекомендовано признать возможным задействование программного изделия "Базовые средства виртуализации вычислительных процессов защищенных операционных систем в интересах Минобороны России.

В рамках развития средств вычислительной техники разработаны варианты исполнения «Шины», подключаемые к системным платам по интерфейсам miniPCI-E и M.2, а также комплекты шлейфов и вспомогательных конвертеров интерфейса, предназначенные для обеспечения соответствия требованиям «Профиля защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты».

В целях формирования завершенных программно-технических решений по созданию защищенной виртуальной инфраструктуры проводятся тестирования с оборудованием основных вендоров серверных решений и тонких клиентов. В целях оптимизации работ по интеграции и внедрению предусмотрено создание пула конструктивно-проектных решений по встраиванию вариантов исполнения ПАК в средства вычислительной техники, в том числе обеспечивающих работу с высокопроизводительными расчетными и графическими системами.

Разработанная платформа успешно интегрирована архитектурой «Байкал-М1», в том числе с расширенными возможностями графической обработки информации, что позволяет реализовать защищенную VDI-инфраструктуру с применением отечественной электронной компонентной базы.

Техническая поддержка

При покупке или продлении срока действия лицензии на программное обеспечение «Горизонт-ВС» требуемый уровень поддержки предоставляется пользователю системы на требуемый срок от 12 до 36 месяцев путем оплаты лицензии на техническую поддержку. Лицензии на программное обеспечение «Горизонт-ВС» поставляются только с

технической поддержкой.

Уровень Базовый

Это уровень поддержки, который позволит Пользователю полноценно и в сжатые сроки ознакомиться с возможностями программного обеспечения «Горизонт-ВС» и успешно применять его. В рамках стандартного уровня поддержки Пользователь получает:

- информацию о совместимом оборудовании и программных продуктах по телефону, системе учета заявок или по электронной почте, а также консультации по настройке и применению в соответствии с эксплуатационной документацией;
- технические консультации по запросам, присланным по электронной почте, через систему учета заявок и связанным с использованием программного обеспечения «Горизонт-ВС»;
- консультации специалистов компании по оптимизации работы оборудования и программного обеспечения «Горизонт-ВС», в информационных системах Пользователя.

Уровень Расширенный

Это уровень поддержки, включающий все позиции уровня Стандартный, а также:

- технические консультации по запросам, присланным по электронной почте, телефону, через систему учета заявок и связанным с использованием оборудования и программного обеспечения «Горизонт-ВС»;
- гарантию первоочередного рассмотрения запросов;
- выделение персонального специалиста технической поддержки, а также возможность привлечения к решению вопросов специалистов из отделов разработки ИЦ «Баррикады»;
- возможность получения технических консультаций по горячей телефонной линии;
- возможность организации удаленного доступа к объектам эксплуатации клиента для решения срочных запросов;
- возможность выезда специалистов ООО «Инновационный центр «БАРРИКАДЫ» на объект Заказчика (по согласованию сторон).