

Функциональные характеристики
Программного комплекса «Гелиос-ЗВС»

RU.ЛНТФ.00006-01 92 01

Листов 9

Инв. № подл.	Подп. и дата	Взам. Инв №	Инв. № дубл.	Подп. и дата

АННОТАЦИЯ

Настоящий документ включает в себя описание функциональных характеристик программного комплекса “Гелиос-ЗВС” (далее – ПК “Гелиос-ЗВС”, изделие), разработанного АО “БФГ”.

СОДЕРЖАНИЕ

1	Общие сведения	4
1.1	Основные сведения о ПК “Гелиос-ЗВС”	4
1.2	Назначение и область применения	4
1.3	Комплект изделия	4
2	Архитектура ПК “Гелиос-ЗВС”	6
2.1	Системные требования	6
2.1.1	Требования к серверному оборудованию	7
2.2	Функциональные возможности	8
2.2.1	Виртуализация и управление ВМ.....	8
2.2.2	Сетевая инфраструктура	8
2.2.3	Хранилище данных.....	8
2.2.4	Безопасность	8
2.2.5	Мониторинг и производительность	8
2.3	Специальные требования	9

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Основные сведения о ПК “Гелиос-ЗВС”

Программный комплекс “Гелиос-ЗВС” предназначен для централизованного управления виртуализированной инфраструктурой, состоящей из одного или нескольких вычислительных узлов, функционирующих под управлением СВ “Звезда”, ОС “42”, или HV 42. ПК “Гелиос-ЗВС” предоставляет администраторам единый интерфейс для управления ресурсами виртуализации, хранилищами, сетевой инфраструктурой, а также для интеграции с внешними системами мониторинга, безопасности и учёта.

1.2 Назначение и область применения

Программный комплекс «Гелиос-ЗВС» ориентирован на использование в распределённых и отказоустойчивых виртуальных средах, где требуется централизованное управление множеством гипервизоров и виртуальных машин. Гелиос-ЗВС может быть развернута в центрах обработки данных государственных организаций, промышленных предприятий, исследовательских учреждений, а также в инфраструктуре корпоративного сектора.

Благодаря унифицированному управлению, поддержке защищённых протоколов, механизму распределённых ролей и мониторинга, ПК «Гелиос-ЗВС» обеспечивает масштабируемое и безопасное управление всей виртуальной платформой, включая миграцию, репликацию и резервное копирование виртуальных машин. Комплекс позволяет замещать зарубежные решения уровня VMware vSphere и других продуктов класса VIM (Virtual Infrastructure Management).

1.3 Комплект изделия

Обозначение изделия	Наименование изделия	Количество
RU.ЛНТФ.00006-01 91 01	1. Инструкция по установке ПК “Гелиос-ЗВС”	1

RU.ЛНТФ.00006-01 90 01	2. Руководство администратора ПК “Гелиос-ЗВС”	1
---------------------------	---	---

Для корректной работы программного комплекса необходимо убедиться, что серверное оборудование отвечает минимальным требованиям ПК “Гелиос-ЗВС”.

2.1.1 Требования к серверному оборудованию

Параметр	Рекомендация
CPU	Минимум 2 ядра; поддержка 64-разрядных процессоров x86
Оперативная память	Не менее 8 ГБ; для работы ВМ — не менее 12 ГБ
Аппаратная виртуализация	Intel VT-x или AMD-V/RVI (для 64-разрядных ВМ)
Сетевой контроллер	1 Гбит/с или выше
Загрузочный диск	Не менее 64 ГБ
Диск для ВМ	SCSI-диск или локальный RAID с неразмеченным пространством
Максимальное количество серверов в кластере виртуализации	1024
Максимальное количество кластеров под единым управлением, ВМ на кластер виртуализации	До 10 000 ВМ на кластер, из которых 8000 могут быть включены одновременно. До 2000 операций в целом или до 640 операций от пользователей с одинаковой ролью
Минимальное количество серверов в кластере виртуализации (с обеспечением отказоустойчивости)	3
Максимальный объём ОЗУ на хост виртуализации	до 32 ТБ
Максимальное количество CPU на хост виртуализации / максимальное количество ВМ на хост	4 CPU (до 160 ядер на процессор), до 3500 ВМ
Максимальное количество vCPU на ВМ / максимальный объём ОЗУ на ВМ	до 255 vCPU, до 24 ТБ ОЗУ
Дисковое пространство платформы с единым управлением	до 1 ЭБ

2.2 Функциональные возможности

2.2.1 Виртуализация и управление ВМ

- Создание и управление виртуальными машинами (32/64-бит);
- Поддержка до 255 виртуальных процессоров на ВМ;
- Создание снимков состояния ВМ;
- Миграция ВМ между хостами;
- Клонирование и шаблоны ВМ.

2.2.2 Сетевая инфраструктура

- Виртуальные коммутаторы с поддержкой VLAN;
- Поддержка технологии Multipathing;
- Управление сетевыми ресурсами.

2.2.3 Хранилище данных

- Поддержка различных типов хранилищ (LVM, NFS, iSCSI, FC);
- Тонкое выделение ресурсов (Thin Provisioning);
- Параллельный доступ ВМ к дискам.

2.2.4 Безопасность

- Интеграция средств защиты информации;
- Ролевое управление доступом;
- Аудит и протоколирование событий;
- Поддержка отечественных ОС (Альт Линукс, Астра Линукс, РЕД ОС).

2.2.5 Мониторинг и производительность

- Мониторинг использования ресурсов в реальном времени;
- Оптимизация памяти (дедупликация, баллонинг);
- Резервирование и приоритизация ресурсов;
- Централизованное обновление.

2.3 Специальные требования

ПК “Гелиос-ЗВС” 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;
- 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.