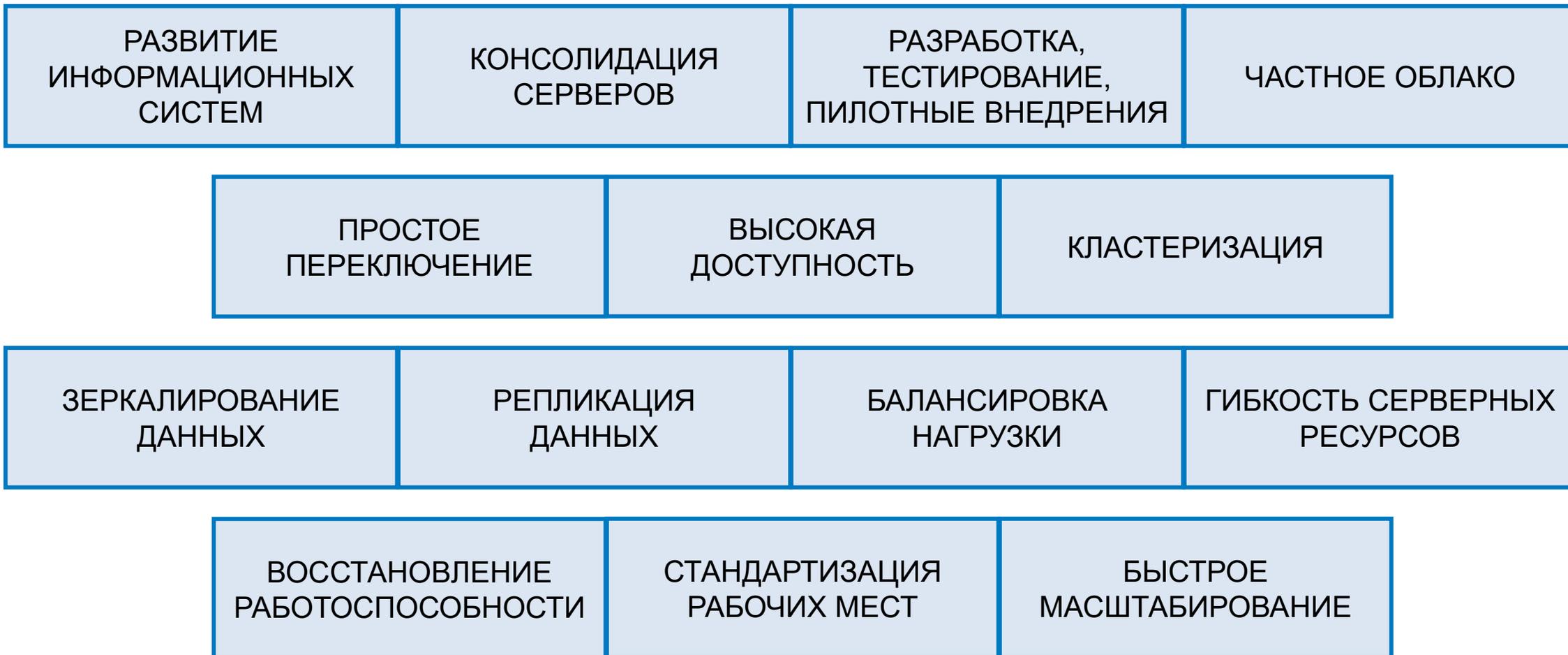




**Система виртуализации
Astra Linux
как основа инфраструктуры в
импортозамещении**

Февраль 2021 года

ЗАДАЧИ И ПРОБЛЕМЫ КЛИЕНТОВ РЕШАЕМЫЕ СИСТЕМОЙ ВИРТУАЛИЗАЦИИ



ВИДЫ ВИРТУАЛИЗАЦИИ



Локальная и серверная виртуализация



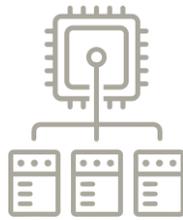
«Облачная» виртуализация



VDI — виртуализация рабочих мест



Сетевая виртуализация



I/O виртуализация



СИСТЕМА ВИРТУАЛИЗАЦИИ ASTRA LINUX



RuBackup

Система резервного копирования



Termidesk for Astra – дополнительный компонент ПК СВ «Брест» для организации защищенной инфраструктуры виртуальных рабочих мест

Обязательные компоненты, необходимы для функционирования системы и управления комплексом виртуализации

- Функционал расширения позволяет создавать пулы виртуальных рабочих мест, в том числе с помощью шаблонов, а также эффективно ими управлять: модифицировать, клонировать, хранить, делать резервные копии и предоставлять к ним защищенный удаленный доступ, используя различные средства и протоколы доставки.

- Средства построения отказоустойчивых конфигураций
- Служба доступа к сетевой защищенной файловой системе
- Консольный интерфейс управления виртуальными машинами
- Графический веб-интерфейс управления виртуальными машинами
- Графический интерфейс для удаленного доступа (VDI) пользователей к виртуальным машинам по протоколам SPICE, RDP, HTML5

- Средства эмуляции аппаратного обеспечения
- Сервер виртуализации

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ ВИРТУАЛИЗАЦИИ



Локальная и серверная
виртуализация



«Облачная»
виртуализация



VDI — виртуализация
рабочих мест

X86-64

ARM (БАЙКАЛ-S)*

ЭЛЬБРУС (16S)*



RuBackup

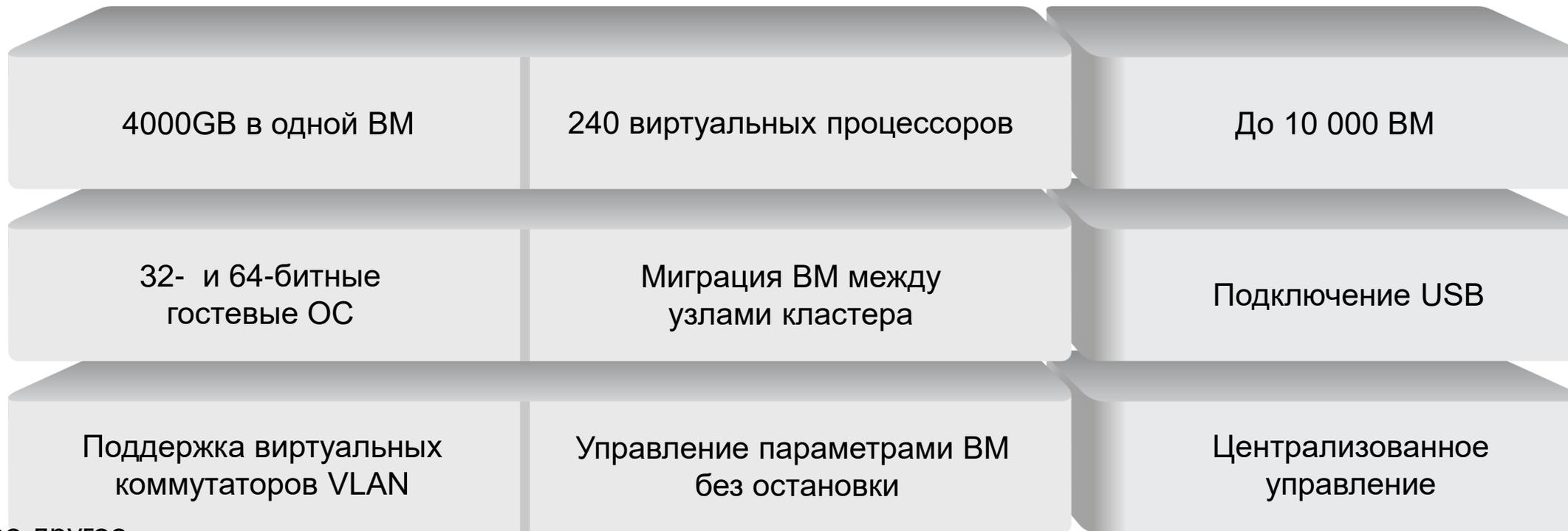
Система резервного копирования

* к концу 2021 года

НАПРАВЛЕНИЯ РАЗВИТИЯ СИСТЕМЫ ВИРТУАЛИЗАЦИИ



ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ



И многое другое

ЗАЩИЩЕННАЯ ОПЕРАЦИОННАЯ СИСТЕМА ASTRA LINUX – основа обеспечения информационной безопасности IT-систем



ТРЕБОВАНИЯ К ВИРТУАЛИЗАЦИИ

(Из приказов ФСТЭК России)

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы		
		3	2	1
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.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры		+	+
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.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным	+	+	+

ПРОГРАММНЫЕ СРЕДСТВА ВИРТУАЛИЗАЦИИ

В СОСТАВЕ ОС CH ASTRA LINUX SPECIAL EDITION 1.6 И ПК СВ «Брест»

СЕРВЕРНАЯ ЧАСТЬ

СРЕДСТВА ЭМУЛЯЦИИ АППАРАТНОГО ОБЕСПЕЧЕНИЯ:

- **Qemu** - эмулятор аппаратных средств, виртуальных машин, предоставляемых хостовой ОС (эмуляция VNC или Spice видео);
- **Open vSwitch** - программный многоуровневый коммутатор, для работы в гипервизорах.

СЕРВЕР ВИРТУАЛИЗАЦИИ:

- **Libvirt** - библиотека программных интерфейсов управления средствами виртуализации хостовой ОС;
- **KVM** - модуль ядра ОС Astra Linux.

СРЕДСТВА ПОСТРОЕНИЯ ОТКАЗОУСТОЙЧИВЫХ КОНФИГУРАЦИЙ:

- **Ansible** - система управления конфигурациями для автоматизации настройки и развертывания программного обеспечения;
- **PaceMaker + PCSD** - менеджер ресурсов кластера с графическими Web-ориентированными средствами управления;
- **HAProxy** - служба обеспечения высокой доступности и балансировки нагрузки.

СЛУЖБА ДОСТУПА К СЕТЕВОЙ ЗАЩИЩЕННОЙ ФАЙЛОВОЙ СИСТЕМЕ

Ceph - программно определяемая распределенная кластерная файловая система.

КЛИЕНТСКАЯ ЧАСТЬ

КОНСОЛЬНЫЙ ИНТЕРФЕЙС УПРАВЛЕНИЯ ВИРТУАЛЬНЫМИ МАШИНАМИ:

- **Virsh** - управление виртуальными машинами из командной строки;
- **OpenNebula** - облачная платформа для управления виртуальными серверами и сервисами и программный API для управления кластером физических серверов.

ГРАФИЧЕСКИЙ ИНТЕРФЕЙС ДЛЯ УДАЛЕННОГО ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ВИРТУАЛЬНЫМ МАШИНАМ (VDI):

- **VNC-клиент** - графическое приложение доступа к виртуальной машине по протоколу VNC;
- **SPICE-клиент** - графическое приложение доступа к виртуальной машине по одноименному протоколу.

ГРАФИЧЕСКИЙ ИНТЕРФЕЙС УПРАВЛЕНИЯ ВИРТУАЛЬНЫМИ МАШИНАМИ:

- **Virt-manager** - графическое управление виртуальными машинами;
- **OpenNebula** - управление виртуальными серверами и сервисами, веб-интерфейс управления кластером физических серверов, облачная платформа.

ЧТО НОВОГО В ВЕРСИЯХ ПК СВ «БРЕСТ» 2.5/2.6:

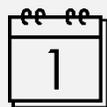
- поддержка службы каталога FreeIPA;
- поддержка работы контекстуализации;
- механизм автомиграции VM;
- статус подключения к консоли VM;
- автоматическая настройка БД Postgresql;
- автоматический перевод на 127 уровень;
- поддержка UEFI;
- механизм наследования и сохранения всех опций VM;
- модуль для управления пользователями и группами из интерфейса;
- автостарт VM из под сервисного пользователя;
- наследование прав владельца и группы на уровень libvirt;
- добавлен режим обслуживания хоста;
- добавлена поддержка контейнеров LXC.



СХЕМА ЛИЦЕНЗИРОВАНИЯ

Лицензирование

Доступные лицензии

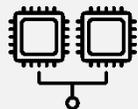


На 1 год



На 3 года

Лицензия ПК СВ «Брест» включает



Право установки компонентов на два процессора/сокета



Установку ОС Astra Linux SE 1.6 с сертификатом ФСТЭК и ПК СВ «Брест» на узел (сервер), количество ядер процессора любое



Право создания и использования неограниченного количества виртуальных машин

Версии ПК СВ «Брест»



«Стандарт»
на гостевых виртуальных машинах используется только Linux

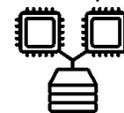


«Корпоратив»
на гостевых виртуальных машинах используются Linux и Microsoft Windows

Условия лицензирования ПК СВ «Брест»

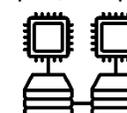
Лицензирование – по количеству процессоров. На каждый сервер требуется минимум одна лицензия в зависимости от количества процессоров (одна лицензия на каждые два процессора).

1 сервер с 2 процессорами



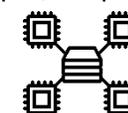
Одна лицензия

2 сервера с 1 процессором



Две лицензии

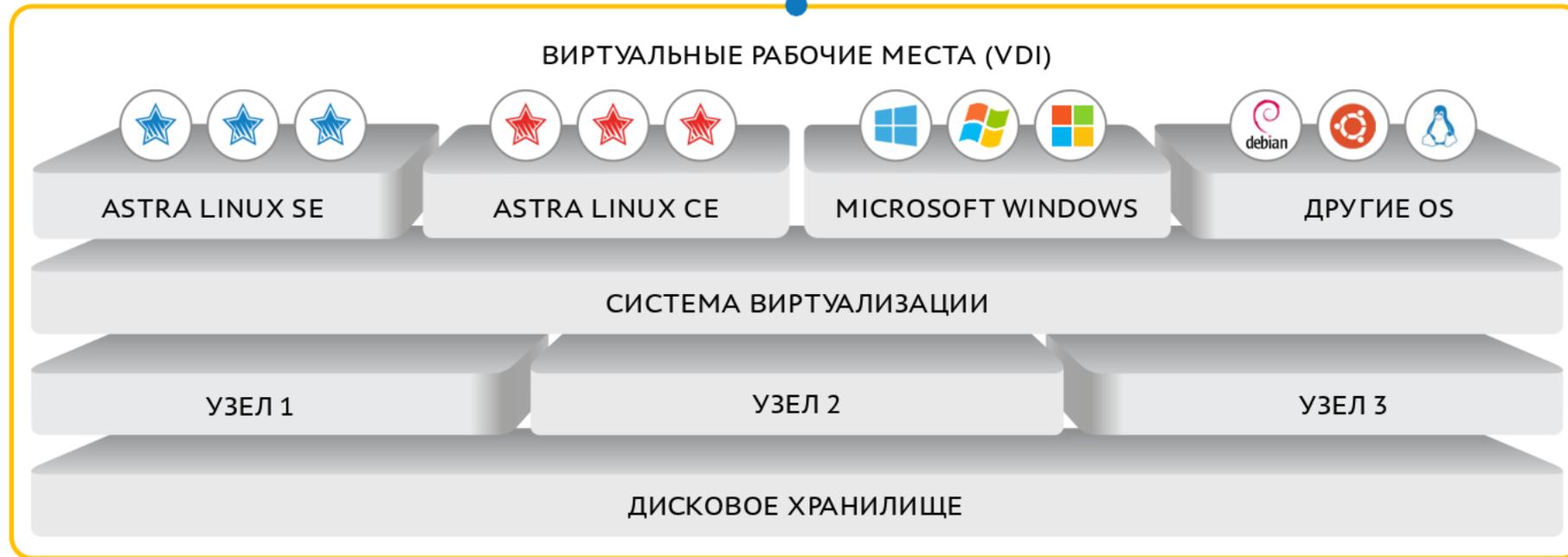
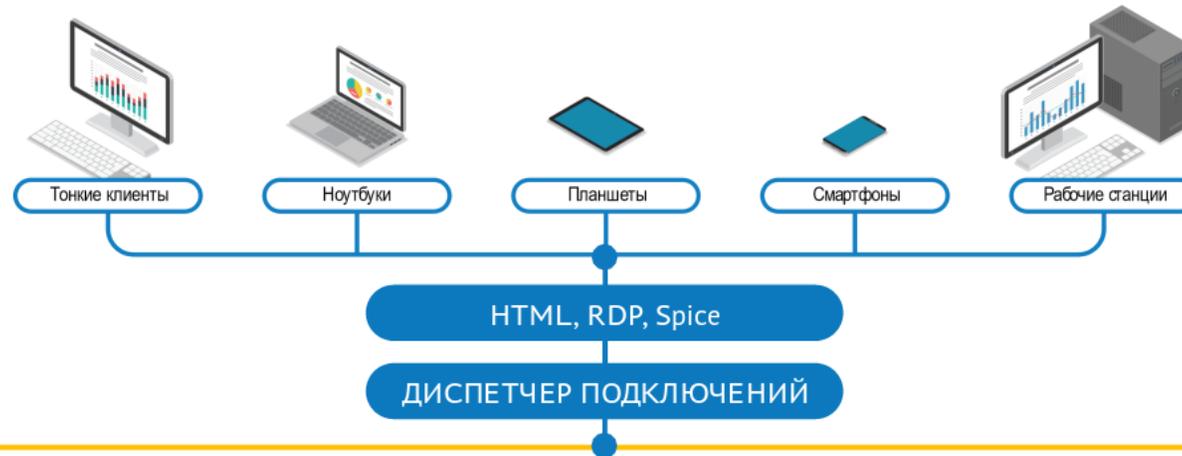
1 сервер с 4 процессорами



Две лицензии

ВАЖНО: одну лицензию (на два процессора) нельзя использовать для двух физических однопроцессорных серверов.

ОБЩАЯ СХЕМА РЕШЕНИЯ ASTRA LINUX+БРЕСТ+TERMIDESK FOR ASTRA



RuBackup

Система резервного копирования

TERMIDESK FOR ASTRA

Управление полным жизненным циклом фонда виртуальных рабочих мест (BPM):

- создание, размещение, запуск, выключение виртуальных машин, сохранение их состояния;
- предоставление доступных пулов виртуальных машин и назначение их пользователю;
- управление доставкой виртуального рабочего стола. Предоставление доступа к виртуальному рабочему столу после подключения или разрыва связи;
- мониторинг состояния виртуальных машин и процесса доставки виртуального рабочего места с возможностью подключения к нему администратора.

Функциональные возможности продукта:

- поддержка службы каталогов FreeIPA, ALD (Astra Linux Directory) и MS AD;
- поддержка различных протоколов доставки фонда BPM: SPICE, RDP, HTML5 (рабочее место в браузере);
- поддержка различных гостевых ОС:
 - открытые: Debian 9.0 и выше, CentOS 7, Ubuntu;
 - проприетарные: Microsoft Windows 7, 8, 10, Astra Linux «Смоленск» 1.2 и выше, Astra Linux «Орел» 1.5 и выше, AltLinux p8, p9;
- типы BPM: индивидуальные (с сохранением состояния) и коллективные (без сохранения состояния).



TERMIDESK
FOR ASTRA

СИСТЕМА РЕЗЕРВНОГО КОПИРОВАНИЯ RUBACKUP

RuBackup — масштабируемое, гибкое, надежное и производительное решение резервного копирования, которое надежно защищает IT-инфраструктуру от потери данных.

RuBackup обеспечивает:

- полное, инкрементальное и дифференциальное резервное копирование виртуальных машин в среде ПК СВ «Брест»;
- репликацию резервных копий в удаленный ЦОД.



Включен в
Единый реестр
отечественного ПО
под номером № 6808

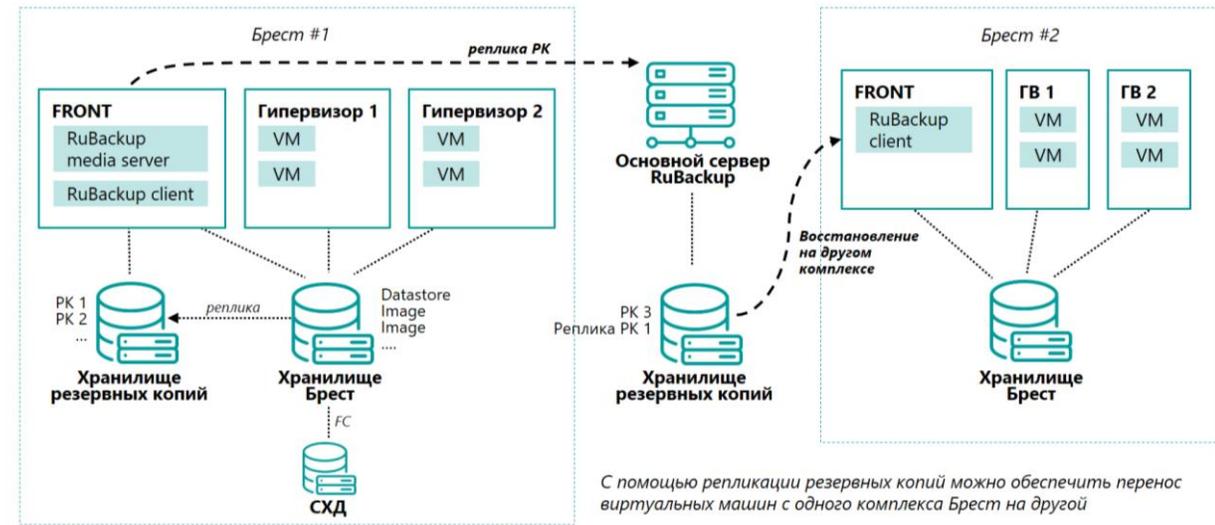


Нацелен на
Enterprise
(data-центры,
серверы
и облачные решения)



Совместим с
отечественными
дистрибутивами
Linux

Сценарий резервного копирования ПК СВ «Брест»



С помощью репликации резервных копий можно обеспечить перенос виртуальных машин с одного комплекса Брест на другой



СХЕМА ДЕМОНСТРАЦИОННОГО СТЕНДА

ВИРТУАЛЬНЫЕ РАБОЧИЕ МЕСТА (VDI)

СЛУЖБЫ



СПАСИБО ЗА ВНИМАНИЕ!

