

# Программный комплекс «Средства виртуализации «Брест»

Предназначен для создания и управления облачной ИТ-инфраструктурой любой сложности с применением всего комплекса средств защиты информации серверной операционной системы специального назначения Astra Linux Special Edition.

## Экосистема совместимых продуктов «Группы Астра»



### Преимущества для заказчиков

- Повышает уровень информационной безопасности всей ИТ-инфраструктуры за счет организации изолированных виртуальных сред.
- Оптимизирует расходы на создание и использование ИТ-системы, т. к. позволяет сократить количество серверного оборудования и рабочих станций.
- Уменьшает затраты на обслуживание благодаря централизованному управлению ресурсами виртуальной инфраструктуры.
- Позволяет масштабировать и балансировать использование ресурсов: можно оперативно менять количество и мощность виртуальных серверов и рабочих мест.
- Обеспечивает стабильность бизнес-процессов и увеличивает скорость работы сотрудников, т. к. повышает доступность информационных ресурсов и рабочих мест.
- Обеспечивает возможность поэтапного перехода на отечественное ПО при реализации плана по импортозамещению в сфере ИТ.
- Работает как на новом, так и на уже имеющемся оборудовании.
- Дает возможность создавать комплексные ИТ-инфраструктуры, используя решения одного вендора, что экономит время заказчика и упрощает выбор совместимых продуктов.
- Имеет возможность расширения сторонними приложениями из экосистемы совместимых продуктов.
- Сокращает энергопотребление за счет оптимизации используемых ресурсов.

### Основные особенности

- Объединяет в себе средства виртуализации, управления и защиты, а при использовании приложений из экосистемы совместимых продуктов — предоставляет возможность резервного копирования, а также организации виртуальных рабочих мест.
- Базовый компонент — новое очередное обновление 1.7 сертифицированной ОС специального назначения Astra Linux Special Edition, которая содержит все необходимые средства виртуализации: инструменты для создания, запуска и обслуживания виртуальной инфраструктуры, а также средства ее защиты, реализующие меры, установленные нормативными и методическими документами регуляторов.
- ПК СВ «Брест» использует все средства безопасности информации, входящие в состав серверной ОС Astra Linux Special Edition\*.
- Механизмы управления защищенной средой виртуализации поддерживают, в том числе, следующие возможности:
  - Мандатное разграничение доступа к ВМ и системе управления (МРД).
  - Функционирование в режиме замкнутой программной среды (ЗПС).
  - Функционирование с учетом всех видов контроля целостности, включая мандатный контроль целостности (МКЦ).
  - Обеспечение запрета модификации ВМ.
- Обновленная пакетная база и поддержка современного оборудования, ядра 5.15 ОС Astra Linux Special Edition.
- Возможность работы с разными типами хранилищ: конвергентное и гиперконвергентное (HCI), внешняя СХД.
- Своевременно получает обновления функциональности и безопасности.

\*Актуальное обновление 3.3 в настоящее время проходит сертификацию в ФСТЭК России, ОАЦ РБ, Минобороны России. Начало серийного производства и реализация (продажа) будут осуществляться по завершении сертификации, окончание работ запланировано на IV квартал 2023 — I квартал 2024 года.

### ✓ Соответствует требованиям к ПО регуляторов рынка

Входит в реестр отечественного ПО Минцифры России (№5742 от 23.07.17).

Рекомендации по переходу на отечественное ПО (приказ Минцифры России №486).

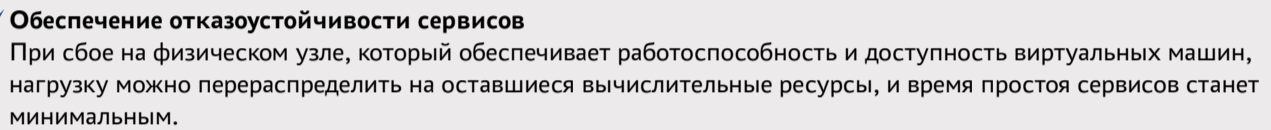
### ✓ Обеспечивает реализацию требований отечественных ГОСТ

• ГОСТ Р 56938-2016 («Защита информации. Защита информации при использовании технологий виртуализации. Общие положения»).

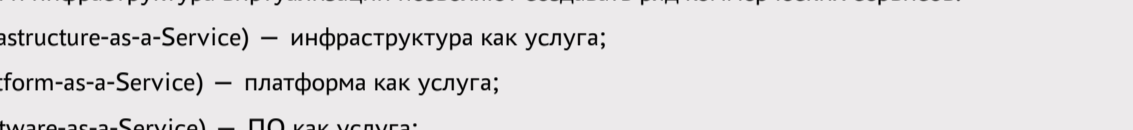
• ГОСТ Р 57580.1-2017 («Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»).

### ✓ Обеспечивает реализацию требований по безопасности к информационным системам обеспечивающим информацию ограниченного доступа

Приказы ФСТЭК России:



### Сценарии использования виртуализации



### Варианты построения хранилища

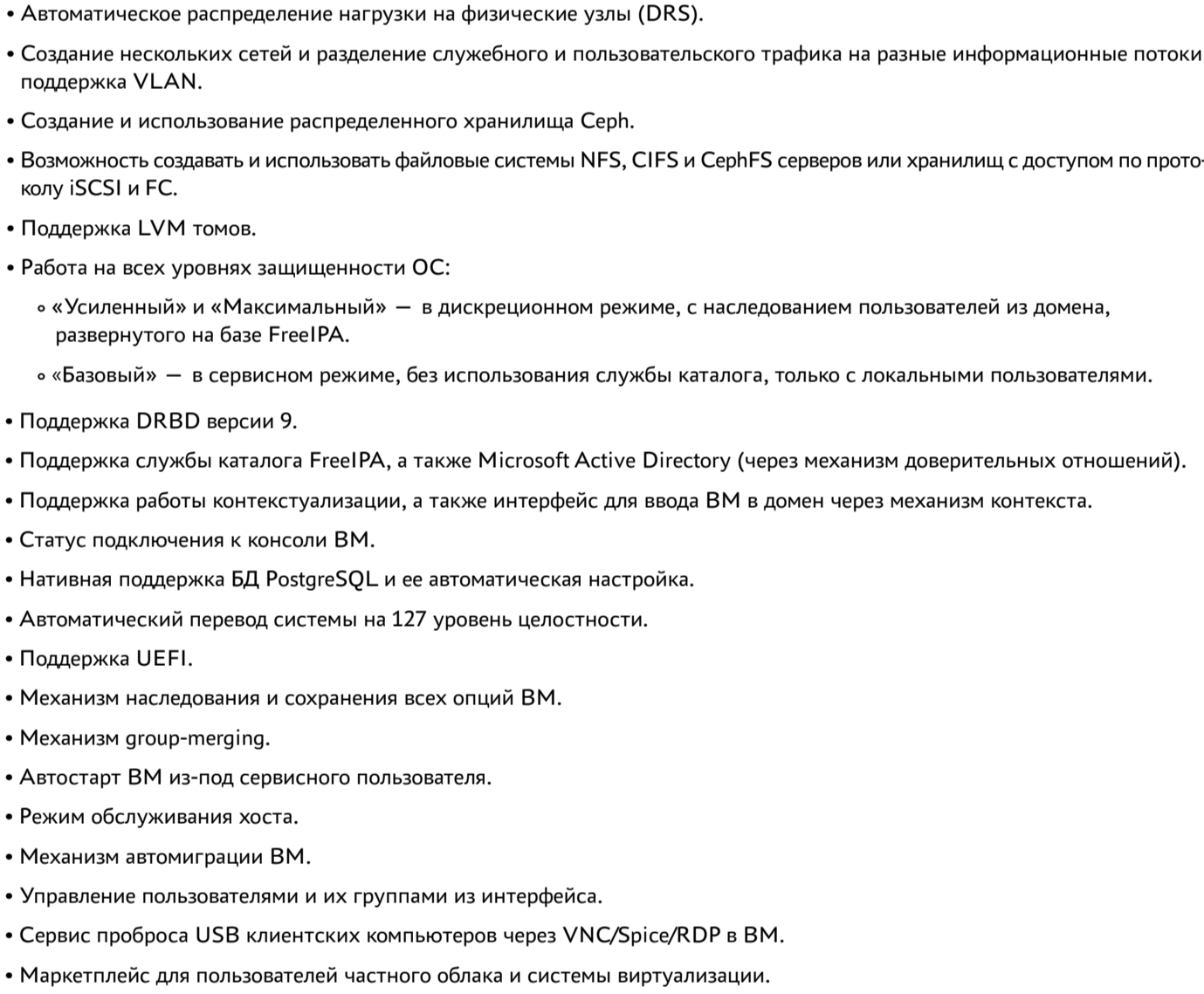
- Конвергентное и гиперконвергентное (HCI)
- Внешнее аппаратное хранилище

### Задачи, которые решает ПК СВ «Брест»

- ✓ **Консолидация серверов или ресурсов**  
В системе виртуализации могут одновременно размещаться несколько необходимых для работы ИТ-инфраструктуры серверных ресурсов: WEB, DHCP, почтовый сервер, служба каталогов, базы данных, ERP, ECM, CAD и ГИС-системы с централизованным хранением, обработкой и доступом к данным.
- ✓ **Формирование среды для перевода ИТ-инфраструктуры на отечественное ПО**  
Виртуальную среду можно использовать как площадку для размещения серверных ресурсов или виртуальных рабочих мест, которые частично или полностью работают под управлением зарубежных ОС, чтобы в дальнейшем реализовать их перевод на ОС Astra Linux.
- ✓ **Разработка и тестирование информационных систем**  
Создание виртуальных серверов со средой и ресурсами для разработки, прототипирования ИС, документирования и тестирования ПО.
- ✓ **Размещение нагрузки, чувствительной к производительности**  
Масштабирование и оптимизация сервиса или системы при увеличении нагрузки.
- ✓ **Создание смешанных окружений**  
Объединение локальных серверных и «облачных» вычислительных ресурсов, чтобы обеспечить масштабируемость, безопасность и доступность инфраструктуры.
- ✓ **Обеспечение отказоустойчивости сервисов**  
При сбое на физическом узле, который обеспечивает работоспособность и доступность виртуальных машин, нагрузку можно перераспределить на оставшиеся вычислительные ресурсы, и время простоя сервисов станет минимальным.
- ✓ **Предоставление ИТ-услуг**  
Механизмы и инфраструктура виртуализации позволяют создавать ряд коммерческих сервисов:
  - IaaS (Infrastructure-as-a-Service) — инфраструктура как услуга;
  - PaaS (Platform-as-a-Service) — платформа как услуга;
  - SaaS (Software-as-a-Service) — ПО как услуга;
  - DaaS (Desktop-as-a-Service) — рабочий стол как услуга;
  - VDC (Virtual Data Center) — виртуальный дата-центр;
  - другие ИТ-услуги, предоставляемые «частным облаком».

### Функциональные возможности

- Эмуляция аппаратного обеспечения на основе модуля KVM с использованием возможностей архитектуры x86-64 на виртуализации процессоров.
- Создание защищенной среды виртуализации серверов и рабочих мест (VDI — опционально) архитектуры x86-64.
- Централизованное управление:

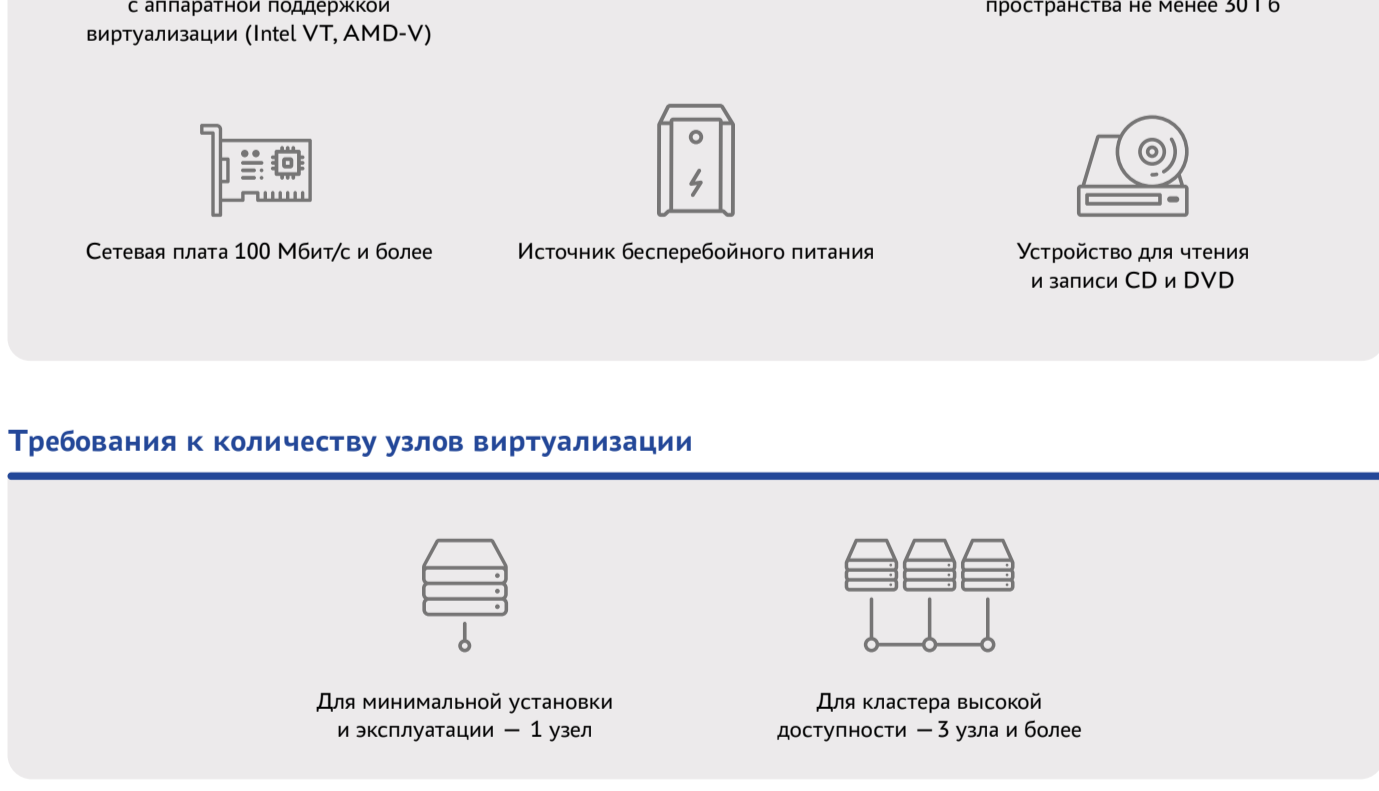


- Виртуализация сетей, хранилищ и иных ресурсов.
- Обеспечение отказоустойчивости управления.
- Масштабирование кластеров виртуализации.
- Создание и эксплуатация до 10 000 ВМ в одном управляемом системой кластере.
- Возможность масштабирования виртуальной инфраструктуры и создания распределенных ЦОД с помощью механизма Федерации.
- Поддержка в одной ВМ до 240 виртуальных процессоров и до 4 Тб оперативной памяти.
- Подключение к ВМ устройств из состава аппаратных средств хоста (сервера), включая устройства USB 3.0.
- Поддержка 32 и 64-битных гостевых ВМ с ОС Linux и Microsoft Windows.
- Создание групп ВМ из шаблонов.
- Клонирование ВМ.
- Идентификация, аутентификация и авторизация пользователей для предоставления доступа к функциям виртуализации и управления.
- Мандатное и дискреционное управление доступом при межпроцессном и сетевом взаимодействии.
- Режим запуска ВМ только для чтения — без внесения изменений в образы их дисков.
- Управление параметрами ВМ во время их работы.
- Централизованный аудит и формирование отчетов.
- Мониторинг работоспособности и использования ресурсов виртуальной инфраструктуры, а также состояния входящих в ЦОД физических узлов.
- Поддержка миграции с интерфейсом мониторинга и управления аппаратной платформой IPMI 2.0.
- Выполнение миграции работающих ВМ между узлами кластера виртуализации.
- Создание кластеров высокой доступности (High Availability - HA).
- Автоматическое резервирование виртуальной инфраструктуры.
- Автоматическое распределение нагрузки на физические узлы (DRS).
- Создание нескольких сетей и разделение служебного и пользовательского трафика на разные информационные потоки, поддержка VLAN.
- Создание и использование распределенного хранилища Сeph.
- Возможность создавать и использовать файловые системы NFS, CIFS и CephFS серверов или хранилищ с доступом по протоколу iSCSI и FC.
- Поддержка LVM томов.
- Работа на всех уровнях защищенности ОС:
  - «Усиленный» и «Максимальный» — в дискреционном режиме, с наследованием пользователей из домена, развернутого на базе FreeIPA.
  - «Базовый» — в сервисном режиме, без использования службы каталога, только с локальными пользователями.
- Поддержка DRBD версии 9.
- Поддержка службы каталога FreeIPA, а также Microsoft Active Directory (через механизм доверительных отношений).
- Поддержка работы контекстуальной, а также интерфейс для ввода ВМ в домен через механизм контекста.
- Статус подключения к консоли ВМ.
- Нативная поддержка БД PostgreSQL и ее автоматическая настройка.
- Автоматический перевод системы на 127 уровень целостности.
- Поддержка UEFI.
- Механизм наследования и сохранения всех опций ВМ.
- Механизм group-merging.
- Автостарт ВМ из-под сервисного пользователя.
- Режим обслуживания хоста.
- Механизм автомиграции ВМ.
- Управление пользователями и их группами из интерфейса.
- Сервис проброса USB клиентских компьютеров через VNC/Spice/RDP в ВМ.
- Маркетплейс для пользователей частного облака и среды виртуализации.
- Автоматизация базовой установки и настройки с помощью плейбуков.
- Оптимизированное перенаправление USB-устройств в гостевую ОС: веб-камера, принтеры, USB-токены, а также общих папок.
- Оптимизированная JPEG-компрессия для SPICE протокола, снижающая нагрузку на канал передачи данных.
- Канал SPICE Display для передачи изображения и его кодирования с применением алгоритмов VP8/VP9/H264/H265.
- Динамический веб-интерфейс, адаптирующийся к ширине экрана монитора.
- Возможность переименования дисковых снапшотов.
- Поддержка псевдонимов для сетевых интерфейсов.
- Возможность автоматического выбора сетевого адаптера при разворачивании ВМ.
- Горячая миграция дисков ВМ между хранилищами.
- Поддержка мультимониторного режима при удаленном доступе к ВМ.
- Функция запрета удаления работающих ВМ.

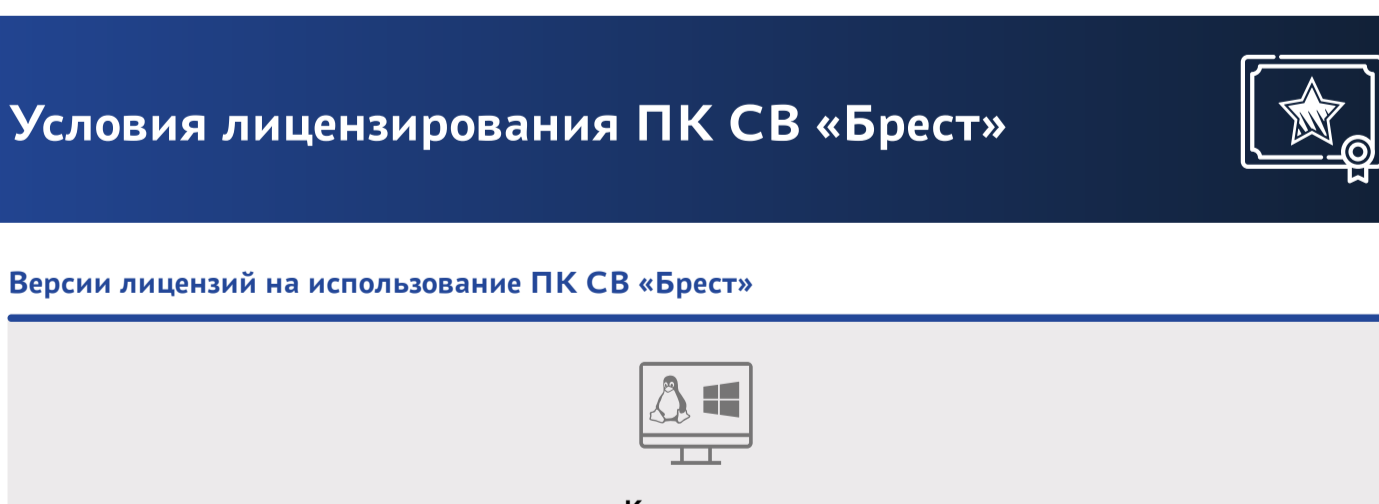
### Изменения в версиях

- Реализована совместимость с оперативным обновлением 1.7.4 и срочным обновлением 1.7.4.UU.1 ОС ALSE.
- Для работы под Требованиям ФСТЭК, теперь совместно с ОС реализуются следующие функции безопасности:
  - Доверенная загрузка виртуальных машин.
  - Контроль целостности в средстве виртуализации.
  - Регистрация событий безопасности в средстве виртуализации.
  - Резервное копирование в средстве виртуализации.
  - Ограничение программной среды.
  - Управление потоками информации в средстве виртуализации.
  - Защита памяти.
  - Идентификация и аутентификация пользователей в средстве виртуализации.
  - Централизованное управление образами виртуальных машин и виртуальными машинами.
- Возможность бесшовного обновления с версии 3.2 до 3.3.
- Графический конфигуратор системы.
- Реализация создания сервисов (SaaS) и группы виртуальных машин с автоматическим масштабированием.
- Реализация дедубликации памяти.
- Возможность создания географически распределенных ЦОД с помощью единой платформы для централизованного управления распределенными инфраструктурами.
- Поддержка технологии NUMA (в том числе возможность прикрепления ВМ к определенному CPU).

### Аппаратные требования к узлам виртуализации



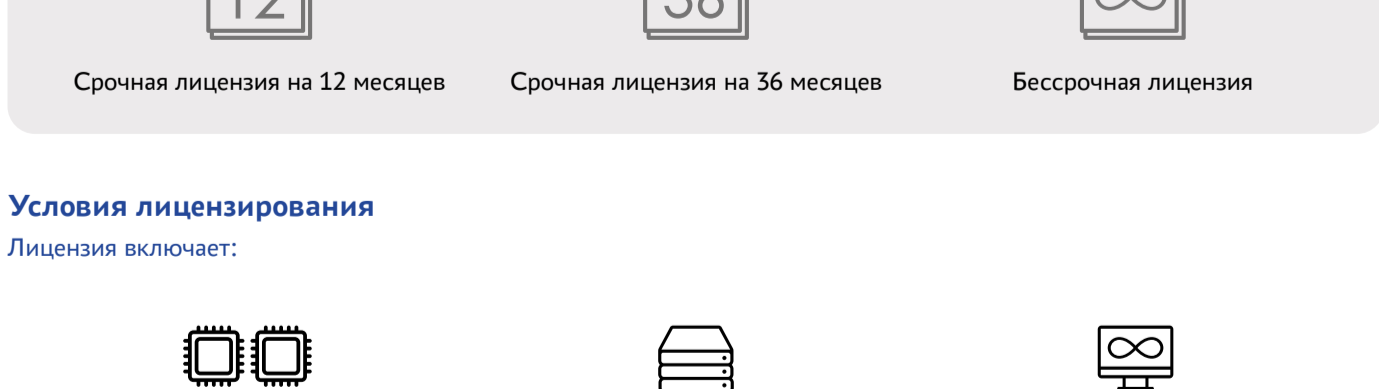
### Требования к количеству узлов виртуализации



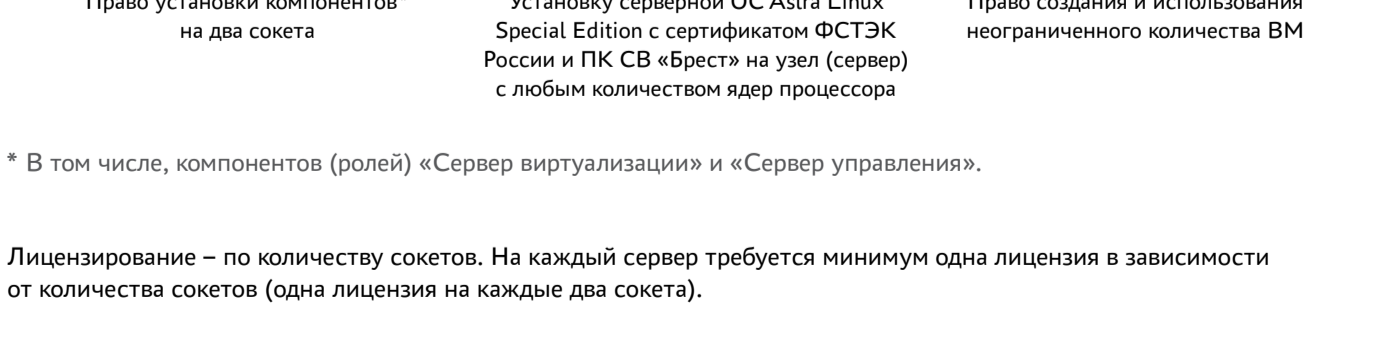
## Условия лицензирования ПК СВ «Брест»



### Версии лицензий на использование ПК СВ «Брест»

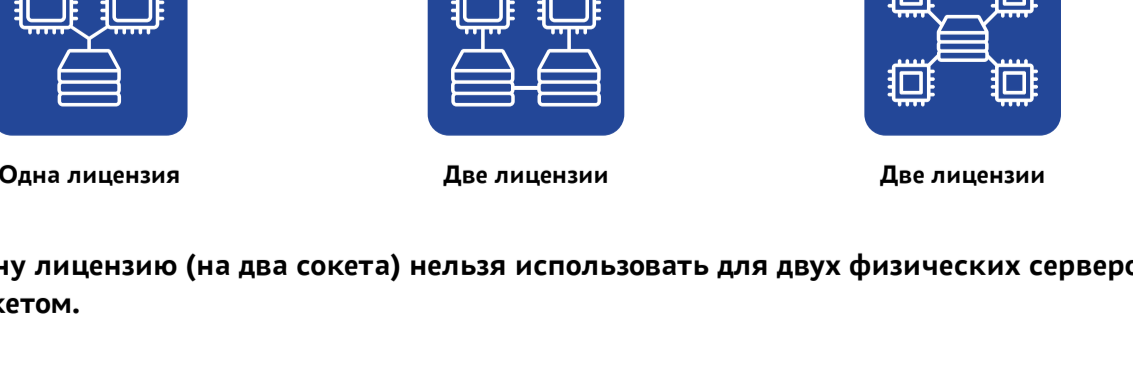


### Виды лицензий



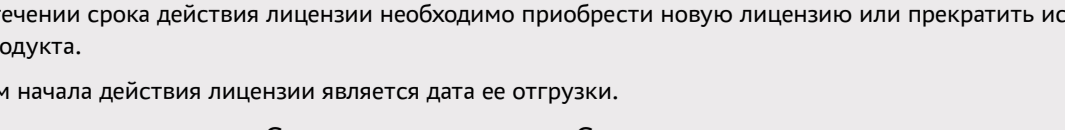
### Условия лицензирования

Лицензия включает:



\* В том числе, компонентов (ролей) «Сервер виртуализации» и «Сервер управления».

Лицензирование — по количеству сокетов. На каждый сервер требуется минимум одна лицензия в зависимости от количества сокетов (одна лицензия на каждые два сокета).



**Важно! Одну лицензию (на два сокета) нельзя использовать для двух физических серверов с одним сокетом.**

### Техническая поддержка

- Пакет услуг технической поддержки уровня «Стандартный» предоставляется:
  - на весь **срок** действия срочной лицензии;
  - на период, определенное условиями **бессрочной** лицензии (но не менее 12 мес.).
- Возможно приобретение пакета услуг уровня «Привилегированный» (до момента окончания срока действия лицензии на использование продукта).

### Важно!

- По истечению срока действия лицензии необходимо приобрести новую лицензию или прекратить использование продукта.
- Срок начала действия лицензии является дата ее отгрузки.
- Для установки компонентов «Сервер виртуализации» и «Сервер управления» на разных серверах, необходимо приобрести лицензию в количестве требуемых дополнительных ролей.
- Для гостевых ВМ, а также вспомогательных (контроллер домена, конвергентные узлы распределенной системы хранения данных Ceph) требуются отдельные лицензии на использование ОС Astra Linux Special Edition.
- Систему также можно приобрести в пакете с серверной ОС Astra Linux Special Edition с безлимитной виртуализацией. В этом случае возможно неограниченное использование лицензии на право использования ОС в гостевых ВМ без дополнительной оплаты.

Дополнительная информация — на сайте [www.astralinux.ru](http://www.astralinux.ru)

