скала^р

Машина динамической инфраструктуры Скала^р МДИ.О

Масштабируемый и отказоустойчивый ПАК
для динамической облачной инфраструктуры виртуализации

Технический обзор

Релиз МДИ.О 2026.1

Версия документа 1.98 от 27.04.2026

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Уведомление

Документ носит исключительно информационный характер и является актуальным на дату размещения.

Технические характеристики, указанные в документе, носят исключительно справочный характер и не могут служить основанием для претензий.

Технические характеристики произведенных ПАК могут отличаться от приведенных в настоящем документе вследствие модификации ПАК.

Технические характеристики и комплектация ПАК могут быть изменены производителем без уведомления.

Документ не является публичной офертой и не содержит каких-либо обязательств ООО «СКАЛА-Р».

Описание документа

Документ раскрывает, как оптимизированные программно-аппаратные комплексы отвечают современным вызовам, и дает концептуальный и архитектурный обзоры **Машины динамической инфраструктуры Скала^р МДИ.О** (далее **Скала^р МДИ.О**, **Машина, МДИ.О, ПАК**).

Аудитория

Технический обзор предназначен для партнеров **Скала^р** и заказчиков, перед которыми ставятся задачи разработки решения, закупки, управления или эксплуатации **Машины динамической инфраструктуры Скала^р МДИ.О**.

Обратная связь

Скала^р и авторы этого документа открыты для дискуссии и будут благодарны за любые конструктивные замечания. Ваши отзывы и предложения просим направлять по электронной почте на адрес info@skala-r.ru, обязательно указав в теме письма название документа.

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Термин, сокращение	Определение
IaaS	(англ. Infrastructure as a Service) Инфраструктура как услуга, одна из моделей обслуживания в облачных вычислениях, по которой потребителям предоставляются по подписке фундаментальные информационно-технологические ресурсы — виртуальные серверы с заданной вычислительной мощностью, операционной системой (чаще всего — предустановленной из шаблона) и доступом к сети
IaC	(англ. Infrastructure as Code) Инфраструктура как код, подход к созданию инфраструктурных служб, предусматривающий широкое использование заранее подготовленных декларативных конфигураций и автоматическое развертывание в противовес развертыванию с использованием интерактивного взаимодействия и ручного редактирования конфигурационных файлов
iSCSI	(англ. Internet Small Computer System Interface) Сетевой протокол для систем хранения данных
LACP	(англ. Link Aggregation Control Protocol) Протокол для объединения нескольких физических каналов в один логический
MLAG	(англ. Multi-Switch Link Aggregation) Технология агрегации каналов, позволяющая одному или нескольким линкам с двух разных сетевых узлов быть объединенными вместе таким образом, что для конечного устройства это выглядит как одиночное соединение
RAID	(англ. Redundant Array of Independent Disks) Избыточный массив независимых дисков, технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и/или производительности
ЗОКИИ	Значимый объект критической информационной инфраструктуры
ИСПДн	Информационные системы персональных данных. Совокупность информации, содержащейся в базах данных, и обеспечивающих ее обработку с использованием информационных технологий и технических средств
Машина	Автономный масштабируемый модульный программно-аппаратный комплекс (изделие с кодом ОКПД 26.20.14.160 из реестров российской промышленной и радиоэлектронной продукции Минпромторга РФ), решающий функциональную задачу хранения, обработки и передачи данных согласно предустановленному системно-прикладному ПО и предоставляющий необходимые для задачи ресурсы вычислений и хранения

Термин, сокращение	Определение
Модуль	Функционально завершенный комплект сконфигурированных для выполнения заданных функций аппаратных и/или программных компонентов, аппаратных узлов и программного обеспечения (ПО), оформленный как самостоятельная единица продаж со своим кодом (part number) и стоимостью. Является единым и неделимым элементом спецификации Машин. Зарегистрирован как программно-аппаратный комплекс (ПАК) с кодом ОКПД 26.20.14.160 в реестрах Минпромторга
ПАК	Программно-аппаратный комплекс
Подсистема	Логическое объединение компонентов по функциональному признаку, с целью пояснения состава и принципов действия ПАК
Узел	Вычислительный узел (сервер) или сетевой узел (коммутатор) или узел хранения (СХД) в составе Модуля, в зависимости от контекста

1. ВВЕДЕНИЕ

Машина динамической инфраструктуры Скала^р МДИ.О — это программно-аппаратный комплекс (ПАК) облачной платформы виртуализации в режиме «частного» или «публичного» облака. ПАК предназначен для создания отказоустойчивой, высокопроизводительной вычислительной виртуальной серверной инфраструктуры для размещения большого числа виртуальных машин (ВМ) с разнородной нагрузкой, различными гостевыми операционными системами (ОС) и прикладным ПО.

Скала^р МДИ.О позволяет реализовать услуги «Инфраструктура-как-Сервис» и подход «Инфраструктура-как-Код» для создания часто меняющихся или непостоянных сред (например, сред разработки и тестирования), обеспечивая более быстрое и надежное внедрение изменений в инфраструктуру. Благодаря наличию RESTful API и интеграций с инструментами управления конфигурациями приложений, реализуется эффективное программное управление виртуальными ресурсами.

Скала^р МДИ.О включает в себя стандартизованные узлы управления, вычислений и узлы хранения данных, а также скоростную сетевую среду и систему интеллектуального управления.

Конструктивно **Машина** собирается из служебных и функциональных **Модулей Скала^р**, каждый их который, как и **Машина**, является самостоятельным изделием (ПАК) с записью в реестре Минпромторга.

Масштабирование **Машины** предусмотрено на уровне функциональных модулей, содержащих один или несколько узлов вычислений и/или хранения.

Скала^р МДИ.О обеспечивает:

- надежную основу для динамической инфраструктуры частного или публичного облака
- автоматизированное развертывание сред виртуализации, что значительно снижает операционные затраты
- высокую производительность — благодаря проработанной интеграции аппаратного и программного обеспечения, оптимизации алгоритмов для используемых технологий, применению широкого спектра методов обеспечения надежности
- отказоустойчивость — за счет применения надежных комплектующих и специализированного программного обеспечения, резервирования критических компонентов и использования устойчивых сетевых протоколов
- катастрофоустойчивость — благодаря наличию специальных технологий
- снижение затрат — за счет комплексности продукта и специальных условий лицензирования
- динамическое управление ресурсами, что повышает гибкость инфраструктуры
- удобный графический интерфейс администрирования
- встроенный REST API, работу с провайдером Terraform и модулем Ansible
- широкий спектр поддерживаемых ОС
- быстрое масштабирование благодаря модульной платформе
- мониторинг и управление обслуживанием встроенными средствами

Скала^р МДИ.О содержит все необходимые элементы для функционирования высоконагруженной системы на основе платформы виртуализации Basis Dynamix Enterprise. Подключение к внешним сетям осуществляется с помощью стандартного

интерфейса Ethernet на определяемых при поставке скоростях, совместимых с инфраструктурой заказчика.

В Машине реализованы функции мониторинга состояния как аппаратных, так и программных компонентов, а также все необходимые интерфейсы и функции управления.

Скала^р МДИ.О впервые была представлена в 2023 году (как МВ.ДИ) и активно развивается.

Машины успешно используются в крупных коммерческих, финансовых и государственных организациях.

Программно-аппаратные комплексы **Машины динамической инфраструктуры Скала^р МДИ.О** включены в Единый реестр российской радиоэлектронной продукции и работают на ПО, включенном в реестр Минцифры РФ.

2. ОТЛИЧИТЕЛЬНЫЕ ЧЕРТЫ

Основные отличительные черты и преимущества **Машины динамической инфраструктуры Скала^р МДИ.О** кратко перечислены ниже.

Высокая доступность

- Механизмы распределения нагрузки
- Система хранения данных (СХД) с двумя контролерами, работающими в режиме active-active, что обеспечивает высокую доступность данных и низкое время переключения путей доступа
- Защита от отказа единичных аппаратных компонентов, установленных в физические серверы (жесткие диски, блоки питания и т.п.), обеспечивается их дублированием

Высокая производительность

- Сбалансированный комплект оборудования
- Архитектурная оптимизация производительности
- Специальные настройки программного обеспечения
- Проработанные варианты для типовых применений
- Высокоскоростные сети внутренней и внешней связности

Отказоустойчивость на всех уровнях

- Надежные комплектующие
- Входное тестирование всех компонентов на совместимость и корректность функционирования
- Резервирование значимых компонентов на аппаратном уровне
- Отказоустойчивая архитектура
- Оперативное восстановление при сбоях

Гибкая система управления

- Централизованное управление из единого web-интерфейса
- Автоматизация операций над инфраструктурой благодаря доступности функций управления через программные интерфейсы (API)
- Адаптеры для Ansible и Terraform
- Расширения функций опциональным интегрированным ПО

Линейная масштабируемость

- Компоненты **Машины** подобраны и сбалансированы для раскрытия всего потенциала масштабируемости
- Модульное наращивание количества вычислительных узлов и/или узлов хранения обеспечивает максимальную производительность с сохранением экономической эффективности и надлежащего уровня эксплуатационного качества

Безопасность на всех уровнях

- Комплекс сертифицированных средств защиты от различных производителей

- Предварительный анализ защищенности и анализ уязвимостей релизов **Машин**, для своевременно обнаружения слабых мест в защите и предотвращения возможных атак

Обеспечение качества при развертывании

- Оптимальность настроек подтверждена значительным количеством установок
- Автоматизированное развертывание снижает риск человеческой ошибки
- Стандартизация развертывания гарантирует соответствие продукта заявленным характеристикам

Непрерывный контроль состояния Машины

- Система управления, мониторинга и анализа состояния **Машины** собственной разработки **Скала^р**
- Мониторинг работоспособности ПО и оборудования
- Установленные пороговые значения критичных параметров
- Различные каналы информирования системой мониторинга об отклонениях

Гибкие возможности администрирования

- Проработанные рекомендации по выполнению процедур обслуживания
- Предустановлено дополнительное ПО для управления

Поддержка в эксплуатации

- Централизованная техническая поддержка ПАК
- Единая ответственность за весь комплекс
- Выпуск предварительно проверяемых патчей
- Паспорт ПАК в комплекте
- Обучение персонала заказчика

Экономическая эффективность

- Специальные условия лицензирования
- Сокращенные сроки ввода в эксплуатацию
- Только обоснованно необходимые компоненты

Альтернатива VMware и Microsoft

- Полностью российское решение
- Отлаженные инструменты и процессы миграции
- Высокие надежность и производительность
- Наличие сертифицированных средств безопасности
- Качество, подтвержденное опытом практического применения

3. ПОДТВЕРЖДЕННАЯ БЕЗОПАСНОСТЬ

3.1 Операционные системы

Машина динамической инфраструктуры Скала^р МДИ.О поставляется с сертифицированной **ОС Astra Linux Special Edition** (сертификат ФСТЭК 2557 от 27.01.2012, действует до 27.01.2031).

ОС Astra Linux Special Edition

Может применяться для защиты информации:

- в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности
- в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности
- в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных
- в информационных системах общего пользования 2 класса

Соответствует требованиям следующих нормативных документов:

- «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016) и «Профиль защиты операционных систем типа А 4 класса защиты. ИТ.ОС.А4.ПЗ» (ФСТЭК России, 2017) по 4 классу защиты
- «Требования по безопасности информации к средствам контейнеризации» (ФСТЭК России, 2022, приказ № 118) по 4 классу защиты
- «Требования по безопасности информации к средствам виртуализации» (ФСТЭК России, 2022, приказ № 187) по 4 классу защиты
- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020, приказ № 76) по 4 уровню доверия

Машина динамической инфраструктуры Скала^р МДИ.О поставляется с сертифицированной **ОС Альт 8 СП** (сертификат ФСТЭК 3866 от 10.08.2018, действует до 10.08.2028). ОС используется в качестве гостевой в служебных виртуальных машинах комплекса или основной для выделенных служебных вычислительных узлов.

ОС Альт 8 СП

Может применяться для защиты информации:

- в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности
- в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности
- в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных
- в информационных системах общего пользования 2 класса

Соответствует требованиям следующих нормативных документов:

- «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016) и «Профиль защиты операционных систем типа А четвертого класса защиты. ИТ.ОС.А4.ПЗ» (ФСТЭК России, 2017) по 4 классу защиты

- «Требования по безопасности информации к средствам контейнеризации» (ФСТЭК России, 2022, приказ № 118) по 4 классу защиты
- «Требования по безопасности информации к средствам виртуализации» (ФСТЭК России, 2022, приказ № 187) по 4 классу защиты
- «Требования по безопасности информации к системам управления базами данных» (ФСТЭК России, 2023) по 4 классу защиты
- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020, приказ № 76) по 4 уровню доверия

Машина динамической инфраструктуры Скала^р МДИ.О может поставляться с сертифицированным средством виртуализации **Basis Virtual Security** (сертификат ФСТЭК 4348 от 24.12.2020, действует до 24.12.2030).

Basis Virtual Security

Может применяться для защиты информации:

- в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности
- в государственных информационных системах до 1 класса защищенности включительно
- в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных
- значимых объектах критической информационной инфраструктуры 1 категории значимости
- в информационных системах общего пользования 2 класса

Соответствует требованиям следующих нормативных документов:

- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) — по 4 уровню доверия
- «Требования по безопасности информации к средствам контейнеризации» (ФСТЭК России, 2022) — по 4 классу защиты
- «Требования по безопасности информации к средствам виртуализации» (ФСТЭК России, 2022) — по 4 классу защиты

3.2 Средства защиты

Протестирована совместимость с наложенным средствами защиты:

3.2.1 Kaspersky Security для виртуальных сред 6.2 Легкий агент

Машина Скала^р МДИ.О совместима с антивирусным средством защиты **Kaspersky Security для виртуальных сред 6.2 Легкий агент** (сертификат ФСТЭК 4846 от 04.09.2024, действует до 04.09.2029), которое соответствует следующим документам:

- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) — по 4 уровню доверия
- «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012)

- «Профиль защиты средств антивирусной защиты типа Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ» (ФСТЭК России, 2012)
- «Профиль защиты средств антивирусной защиты типа В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ» (ФСТЭК России, 2012)
- «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014)
- «Профиль защиты средств контроля съемных машинных носителей информации (контроля подключения съемных машинных носителей информации) четвертого класса защиты. ИТ.СКН.П4.ПЗ» (ФСТЭК России, 2014)

Kaspersky Security для виртуальных сред 6.2 Легкий агент, как и **Kaspersky Endpoint Security для Linux** могут применяться:

- в государственных информационных системах до 1 класса защищенности включительно
- в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных
- значимых объектах критической информационной инфраструктуры 1 категории значимости
- в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности

3.2.2 Kaspersky Endpoint Security для Linux

Сертифицированное антивирусное средство защиты **Kaspersky Endpoint Security для Linux** (сертификат ФСТЭК 2534 от 27.12.2011, действует до 27.12.2030) соответствует документам:

- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) по 2 уровню доверия
- «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012)
- «Профиль защиты средств антивирусной защиты типа класса защиты. ИТ.САВЗ.Б2.ПЗ» (ФСТЭК России, 2012)
- «Профиль защиты средств антивирусной защиты типа класса защиты. ИТ.САВЗ.В2.ПЗ» (ФСТЭК России, 2012)
- «Профиль защиты средств антивирусной защиты типа класса защиты. ИТ.САВЗ.Г2.ПЗ» (ФСТЭК России, 2012)
- «Требования к средствам контроля носителей (СКН)»
- «Профиль защиты средств контроля носителей информации (контроля подключения съемных машинных носителей информации) второго класса защиты. ИТ.СКН.П2.ПЗ»

3.2.3 Avanpost FAM

Машина динамической инфраструктуры Скала^р МДИ.О совместима и может включать в себя при поставке сертифицированное средство единой аутентификации **Avanpost FAM** (сертификат ФСТЭК 4492 от 13.12.2021, действует до 13.12.2026), которое может быть применено в следующих информационных системах, не предназначенных для обработки сведений государственной тайны:

- для применения в государственных информационных системах 1 класса защищенности

- для применения в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных
- для применения в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности

Avanpost FAM соответствует требованиям следующих нормативных документов:

- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020, приказ № 76) по 1 уровню доверия.

3.2.4 «Соболь» версия 4

При помощи опционального сертифицированного средства доверенной загрузки ПАК «Соболь» версия 4 (сертификат ФСТЭК №4043 от 05.12.2018, действует до 05.12.2028), на узлах **Машины** может осуществляться контроль целостности программного обеспечения, а на этапе загрузки ОС – защита от несанкционированной загрузки ОС со съемных носителей. Соответствует требованиям руководящих документов к средствам доверенной загрузки, а также 2 уровню доверия средств технической защиты безопасности и обеспечения безопасности информационных технологий и допускает возможность использования в ИСПДн до УЗ1 включительно, в ГИС до 1 класса защищенности включительно и в ЗОКИИ до 1 категории включительно.

4. ПРИНЦИПЫ СОЗДАНИЯ МАШИНЫ

Машина динамической инфраструктуры Скала^р МДИ.О создана для работы с виртуальной динамической инфраструктурой

Целью разработки было создание программно-аппаратного комплекса (ПАК), специально адаптированного для ПО **Basis Dynamix Enterprise** в целях создания высокопроизводительной платформы динамической инфраструктуры, позволяющей управлять хостами виртуализации и виртуальными серверами с разнородной нагрузкой. В **Машине** использованы преимущества тонкой настройки всех компонентов под функции и потребности конкретного ПО и тем самым обеспечен максимум ее производительности.

Комплексное размещение компонентов, применение высокопроизводительных протоколов и устройств хранения также способствуют достижению этой цели.

Использование **Машины динамической инфраструктуры Скала^р МДИ.О** обеспечивает:

- контроль — за счет быстрого развертывания инфраструктуры и готовым инструментам для управления виртуальным дата-центром и сетевыми функциями
- быстродействие — за счет блочного хранения с настраиваемой производительностью и интеграционным модулям к инструментам CI/CD и DevOps
- эффективность — за счет авторизации и аутентификации через отдельный брокер безопасности, а также полнофункционального REST API
- управление и адаптацию — за счет возможности создания и управления шаблонами, а также индивидуальной адаптации **Машины** под требования конкретного заказчика

Технологические принципы

- дублирование критичных компонентов
- применение высокопроизводительных компонентов
- разделение систем вычисления и хранения
- горизонтальное масштабирование вычислительных ресурсов
- сохранение работоспособности при отказе отдельных элементов системы
- комплексный подход к безопасности и защите данных

Технические решения

- архитектура основана на модулях и подсистемах
- специальное ПО для управления и мониторинга ПАК
- многоуровневое тестирование ПАК, его узлов и компонентов при производстве
- глубокая адаптация компонентов для совместной работы в составе **Машины**

Надежность на уровне архитектуры

- система управления развернута на трех узловом кластере Kubernetes
- система управления отделена от вычислительной нагрузки, что повышает безопасность и доступность системы управления
- разделение ресурсов на узлы вычисления и узлы хранения

Высокая производительность на уровне архитектуры

- благодаря выделенной сети внутреннего взаимодействия, все узлы взаимодействуют между собой с одинаковой высокой скоростью

Проработанность всех программных компонентов

Основные программные элементы **Скала^р МДИ.О**:

- операционная система
- ПО Basis Dynamix Enterprise
- Basis Virtual Security (при включении в состав **Машины** Модуля безопасности)
- ПО **Скала^р Геном** (включая компонент мониторинга **Визион**)

В **Машине** обеспечены оптимизация, тонкая настройка и доработка перечисленных компонентов для обеспечения их наибольшей производительности и функционального соответствия потребностям заказчика.

Практическое применение тиражируемых экземпляров **Скала^р МДИ.О** продемонстрировало высокую производительность и обозначило области для дальнейшего развития.

В ходе развития была разработана методика оптимизации настройки ядра ОС каждого из необходимых вычислительных узлов **Машины** под конкретный вариант ее применения. заказчик получает **Машину**, настроенную под проект. Инсталляция **Машин** на производстве осуществляется при помощи разработанного **Скала^р** специального ПО, что исключает риск человеческой ошибки.

Команда инженеров и архитекторов **Скала^р** продолжают работу по оптимизации алгоритмов восстановления узлов при возможных отказах. Аналогичная деятельность постоянно ведется и по развитию систем мониторинга и управления.

В комплексе все перечисленные направления формируют целостную архитектуру **Машины динамической инфраструктуры Скала^р МДИ.О**.

Сопровождение и поддержка

Важным дополнением ко всему перечисленному является полная ответственность производителя за **Машину** в целом, включая все программные и аппаратные компоненты. Это означает не только уверенность в работоспособности изделия в целом, но и последующую поддержку от единого поставщика в режиме одного окна, а не от нескольких разных поставщиков, как бывает при самостоятельном подборе, развертывании и настройке компонентов в случае традиционного подхода.

5. СОСТАВ МАШИНЫ

Ниже приведены термины, используемые для комплектации **Машины динамической инфраструктуры Скала^р МДИ.О**.

Машина — это набор аппаратного и программного обеспечения в виде Модулей **Скала^р**, соединенных вместе для обеспечения определенного метода обработки данных или предоставления ИТ-сервисов с заданными характеристиками.

Модуль — это единица поставки **Машин**, выполняющая определенные функции в соответствии с ее назначением. Модуль является единым и неделимым элементом спецификации **Машины** и содержит набор аппаратных узлов и ПО.

Узел — это элемент, выполняющий определенную задачу в составе Модуля.

Подсистема — логическое объединение компонентов (Модулей, Узлов) по функциональному признаку, с целью пояснения состава и принципов действия ПАК.

Машина динамической инфраструктуры Скала^р МДИ.О (базовый комплект) состоит из Модулей, представленных на рисунке 1.

Рисунок 1. Машина динамической инфраструктуры Скала^р МДИ.О

5.1 Комплекты поставки

Скала^р МДИ.О поставляются в виде функционально полного набора Модулей **Скала^р** и комплектуются в соответствии с показателями назначения, полученными от заказчика.

Машина включает в себя базовый комплект, и в случае необходимости дополняется комплектом Модулей расширения и/или специальными Модулями.

Базовый комплект — это набор Модулей **Скала^р**, минимально-необходимый для функционирования всех подсистем, обеспечивающих выполнение основного функционала **Машины**.

Комплект Модулей расширения — это набор Модулей **Скала^р**, позволяющий масштабировать ПАК, например, когда не хватает портовой емкости, или есть необходимость увеличить производительность и объем хранения данных. Кроме того, можно добавить специальные Модули **Скала^р**, позволяющие расширить функциональность ПАК.

На диаграмме ниже (Рисунок 2) представлена комплектация **Машины динамической инфраструктуры Скала^р МДИ.О** (базовый комплект и комплект Модулей расширения), а также соответствие Модулей **Машины** функциональным подсистемам.

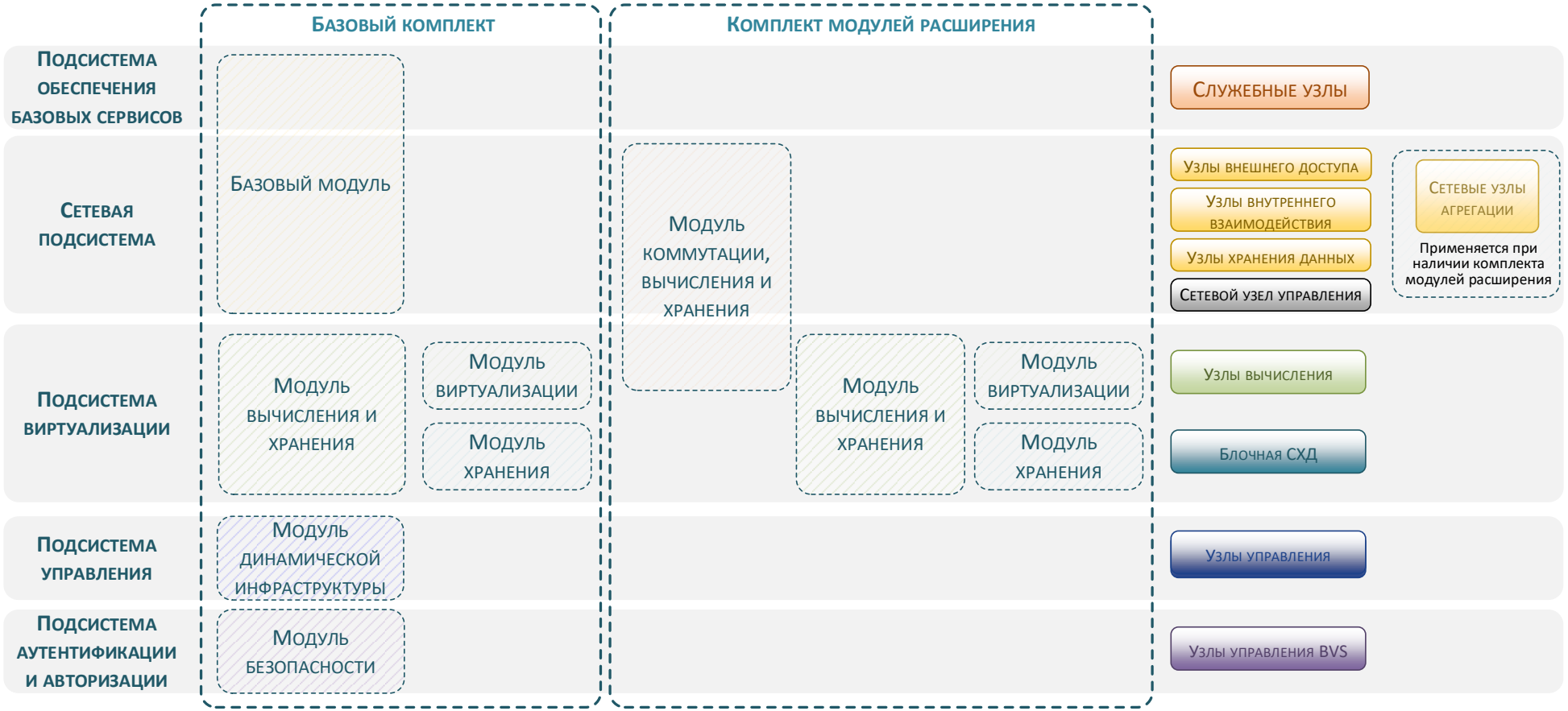

Рисунок 2. Комплектация Машины динамической инфраструктуры Скала^р МДИ.О

5.2 Подсистемы

Функции **Машины динамической инфраструктуры Скала^р МДИ.О** логически объединены в подсистемы. Часть подсистем обеспечивают основной функционал и всегда включены в **Машину**, а часть — предоставляют дополнительный функционал и могут быть добавлены по требованию заказчика.

Основной функционал обеспечивается набором подсистем, необходимых **Машине** для выполнения задач прямого назначения.

Дополнительный функционал предоставляется набором подсистем из Модулей, обеспечивающих расширение функций **Скала^р МДИ.О**.

5.2.1 Подсистема обеспечения базовых сервисов

Подсистема обеспечения базовых сервисов отвечает за мониторинг и управление аппаратными и программными компонентами **Скала^р МДИ.О**. В нее включены вычислительные узлы Базового модуля, на которых предустановлена программная платформа **Скала^р Геном**, выполняющая следующие функции:

- сбор, хранение и отображение данных мониторинга
- настройка правил оповещения
- отправка оповещений о состоянии ПАК
- управление аппаратными компонентами
- настройка программных компонентов
- настройка интеграции со сторонним ПО

Архитектура подсистемы обеспечения базовых сервисов обеспечивает отказоустойчивый режим работы.

Подсистема обеспечения базовых сервисов реализуется в Базовом модуле (см. 5.3.1).

5.2.2 Сетевая подсистема

Сетевая подсистема выполняет функций организации сетевой связанности между всеми вычислительными узлами, входящими в состав **Машины,** и представляет собой набор сетевых узлов, которые организуют изолированные высокоскоростные сети:

- внутреннего взаимодействия (в зависимости от требований заказчика 25 Гбит/с или 100 Гбит/с) — для организации интерконнекта между всеми компонентами ПАК, включая организацию сети хранения для доступа к СХД в составе ПАК
- внешнего доступа (в зависимости от требований заказчика 25 Гбит/с или 100 Гбит/с) — для организации внешнего доступа
- управления (1 Гбит/с) — для организации управления оборудованием и передачи сервисной информации в подсистему обеспечения базовых сервисов

Стартовый комплект сетевых узлов всегда размещается в Базовом модуле (см. 5.3.1).

5.2.3 Подсистема виртуализации

Основные функции подсистемы виртуализации связаны с работой системы динамической инфраструктуры: формирование вычислительные мощностей для системы виртуализации и хранение данных. Подсистема отвечает за предоставление вычислительных ресурсов системе в рамках виртуальной инфраструктуры и хранения данных.

Подсистема реализуется Модулем вычисления и хранения (см. 5.3.3) и/или Модулями виртуализации (см. 5.3.4) и Модулями хранения (см. 5.3.5).

5.2.4 Подсистема управления

Подсистема управления выполняет функции управления динамической инфраструктуры, обеспечивает отказоустойчивый режим работы всех функциональных сервисов платформы динамической инфраструктуры.

Подсистема отвечает за:

- управление платформой виртуализации
- настройку и управление сетевыми функциями
- настройку и управление системами хранения данных (со стороны платформы динамической инфраструктуры)
- предоставление функций IaaS/IaC и различных интерфейсов доступа и управления
- отслеживание и анализ состояния системы динамической инфраструктуры

Подсистема реализуется Модулем динамической инфраструктуры (см. 5.3.2).

5.2.5 Подсистема аутентификации и авторизации

Подсистема аутентификации и авторизации выделяется в случае использования сертифицированной ФСТЭК версии ПО Basis Dynamix и отвечает за обеспечение безопасности системы управления и системы виртуализации и предназначен для использования в государственных информационных системах до 1 класса защищенности включительно, в информационных системах персональных данных до 1 уровня защищенности включительно, в автоматизированных системах до класса 1Г включительно. Подсистема отвечает за:

- идентификацию, аутентификацию и авторизацию пользователей в средстве виртуализации
- доверенную загрузку виртуальных машин средством виртуализации
- контроль целостности в средстве виртуализации
- регистрацию событий безопасности в средстве виртуализации
- управление доступом пользователей в средстве виртуализации
- управление потоками информации в средстве виртуализации
- ограничение программной среды

Подсистема реализуется Модулем безопасности (см. 5.3.6).

5.3 Модули Машины

В разрезе модульности, **Машина динамической инфраструктуры Скала^р МДИ.О** состоит из следующих функциональных модулей **Скала^р**, указанных на рисунке 2:

- Базового модуля
- Модуля вычисления и хранения
- Модуля динамической инфраструктуры
- Модуля виртуализации
- Модуля хранения
- Модуля безопасности
- Модуля коммутации, вычисления и хранения (используется для расширения)

Часть Модулей обеспечивают основной функционал и всегда включены в **Машину**, а часть — дополнительный функционал и могут быть добавлены по требованию заказчика.

5.3.1 Базовый модуль

Название в Едином реестре российской радиоэлектронной продукции — СКАЛА-Р Базовый модуль. Обеспечивает функционирование подсистемы обеспечения базовых сервисов и сетевой подсистемы.

Назначение

- обеспечение сетевой связанности между узлами
- организация выделенной сети управления **Машиной**
- организация подключения к сети заказчика
- исполнение функций мониторинга и управления компонентами **Машины**

Узлы

- два вычислительных узла мониторинга и регистрации, которые объединены в отказоустойчивый кластер и используются для служебных функций
- два или более сетевых узла 25 Гбит/с или 100 Гбит/с для организации внутреннего сетевого взаимодействия, включая сеть хранения
- два сетевых узла 25 Гбит/с для организации сети внешнего доступа (штатная комплектация)
- сетевой узел 1 Гбит/с для организации работы сети управления, также может быть выполнен в отказоустойчивом исполнении (как два узла)

Отказоустойчивость обеспечена

- резервированием вычислительных узлов, отвечающих за мониторинг и управление компонентами **Машины**
- технологией RAID для дисков вычислительных узлов
- резервированием сетевых коммутаторов (объединение сетевых узлов в MLAG-пару)

Применяемое программное обеспечение

- программная платформа **Скала^р Геном**
- система класса Identity & Access Management - Avanpost FAM (опция)

На служебных узлах Базового модуля предустановлено сервисное ПО **Скала^р Геном**, выполняющее следующие функции:

- сбор, хранение и отображение данных мониторинга
- настройка правил оповещения
- отправка оповещений о состоянии ПАК
- управление аппаратными компонентами
- настройка программных компонентов
- настройка интеграции со сторонним ПО

5.3.2 Модуль динамической инфраструктуры

Название в Едином реестре российской радиоэлектронной продукции — СКАЛА-Р Модуль динамической инфраструктуры. Обеспечивает функционирование подсистемы управления динамической инфраструктуры, отказоустойчивый режим работы всех функциональных

сервисов платформы динамической инфраструктуры. Схема узла управления показана на рисунке3.

Осуществляет управление узлами вычисления и хранения.

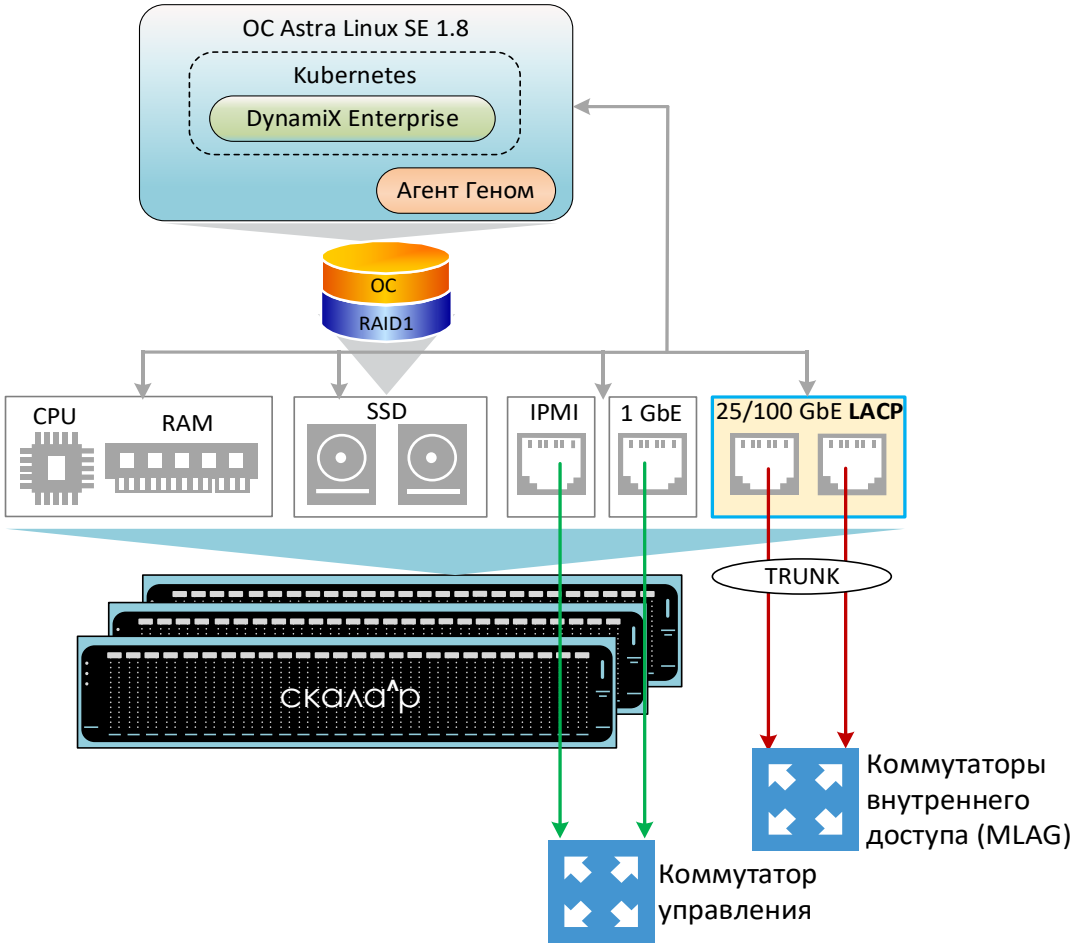

Рисунок 3. Схема узла управления

Назначение

- управление платформой виртуализации
- настройка и управления сетевыми функциями
- управление системами хранения данных
- предоставление функций IaaS/IaC и различных интерфейсов доступа и управления
- отслеживание и анализ состояния системы динамической инфраструктуры

Узлы

- три вычислительных узла, объединенные в кластер. Кластер построен на узлах с ОС Astra Linux 1.8 на базе Kubernetes с установленным программным продуктом Basis Dynamix Enterprise

Отказоустойчивость обеспечена

- выделением трех физических вычислительных узлов
- средствами Kubernetes

- ОС узлов разворачиваются на аппаратном RAID 1 – отказоустойчивом дисковом массиве из двух дисков

Применяемое программное обеспечение

- ОС Astra Linux 1.8
- Basis Dynamix Enterprise
- агенты управления и мониторинга программной платформы **Скала^р Геном**.
- Basis Cloud Control (опционально)
- Octopus (опционально)

5.3.3 Модуль вычисления и хранения

Название в Едином реестре российской радиоэлектронной продукции — СКАЛА-Р Модуль вычисления и хранения. Обеспечивает хранение данных и формируют вычислительные мощности для системы виртуализации. Содержит узлы вычислений и узлы хранения, объединяя функциональность Модуля виртуализации и Модуля хранения (описаны ниже).

5.3.4 Модуль виртуализации

Название в Едином реестре российской радиоэлектронной продукции — СКАЛА-Р Модуль виртуализации. Обеспечивает функционирование системы динамической инфраструктуры, формирует вычислительные мощности для системы виртуализации. Вычислительные узлы объединяются в единый кластер вычисления.

Кластер вычисления имеет возможность масштабирования количества узлов и изменения конфигурации узлов. Может включать до 180 вычислительных узлов. Схема вычислительных узлов приведена ниже (Рисунок 4).

Назначение

- предоставление вычислительных ресурсов в рамках виртуальной инфраструктуры

Узлы

- вычислительные узлы построены на с ОС Astra Linux 1.8 и гипервизоре QEMU/KVM
- минимально в Модуле один узел, но минимальное число узлов вычислений в **Машине** – 4

Отказоустойчивость обеспечена

- резервированием критических компонентов
- средствами виртуализации
- использованием устойчивых сетевых протоколов
- ОС узлов разворачиваются на аппаратном RAID 1 – отказоустойчивом дисковом массиве из двух дисков
- многоуровневым тестированием в лаборатории **Скала^р**.

Применяемое программное обеспечение

- ОС Astra Linux 1.8
- QEMU/KVM
- агенты управления и мониторинга программной платформы **Скала^р Геном**

- **агенты BVS** (опционально, при включении в состав **Машины** Модуля безопасности)

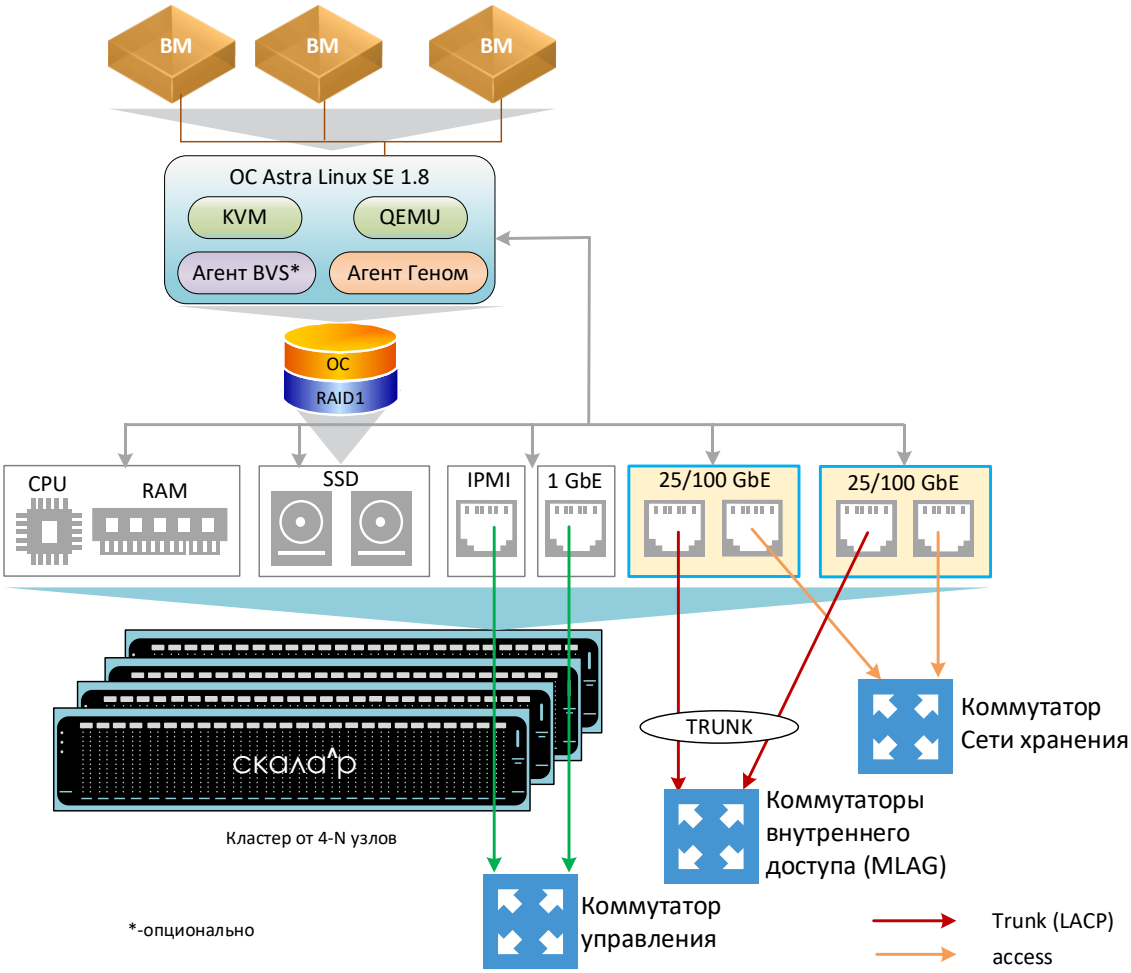

Рисунок 4. Схема вычислительного узла виртуализации

5.3.5 Модуль хранения

Название в Едином реестре российской радиоэлектронной продукции — СКАЛА-Р Модуль хранения. Обеспечивает хранение данных системы динамической инфраструктуры.

Назначение

- хранение данных виртуальной инфраструктуры (образов виртуальных машин и их виртуальных дисков)

Узлы

- СХД YADRO TATLIN.UNIFIED Gen2

5.3.6 Модуль безопасности

Название в Едином реестре российской радиоэлектронной продукции — СКАЛА-Р Модуль безопасности. Обеспечивает безопасность системы управления и системы виртуализации и предназначен для использования в государственных информационных системах до 1 класса защищенности включительно, в информационных системах персональных данных до 1 уровня защищенности включительно, в автоматизированных системах до класса 1Г включительно.

Применяется для соответствия требованиям ФСТЭК к системам виртуализации и при аттестации ИТ-систем. В общем случае – опционален. Схема узлов безопасности приведена на рисунке 5.

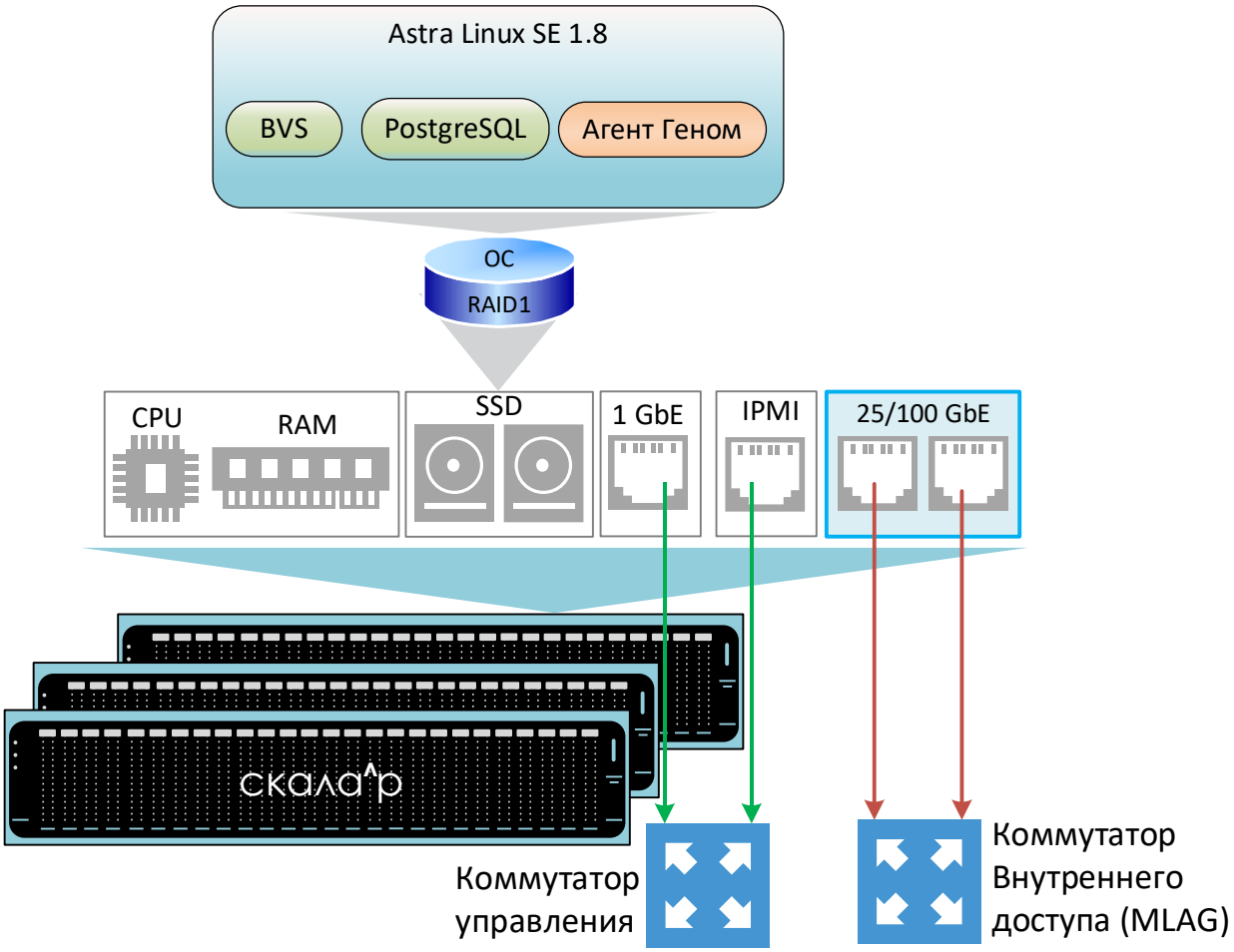

Рисунок 5. Схема узла безопасности

Назначение

- идентификация, аутентификация и авторизация пользователей в средстве виртуализации
- доверенная загрузка виртуальных машин средством виртуализации
- контроль целостности в средстве виртуализации
- регистрация событий безопасности в средстве виртуализации
- управление доступом пользователей в средстве виртуализации
- управление потоками информации в средстве виртуализации
- ограничение программной среды

Узлы

- состоит из трехузлового кластера с ОС Astra Linux 1.8 на базе программного продукта **Basis Virtual Security**

Отказоустойчивость обеспечена

- выделением трех физических вычислительных узлов

- технологией RAID для дисков вычислительных узлов

Применяемое программное обеспечение

- ОС Astra Linux 1.8
- Программная платформа **Basis Virtual Security**, включая специализированный пакет Java Development Kit
- Агенты управления и мониторинга программной платформы **Скала^р Геном**

6. АРХИТЕКТУРА

Основные компоненты **Машины динамической инфраструктуры Скала^р МДИ.О** и их взаимодействие представлены на схеме (Рисунок 6).

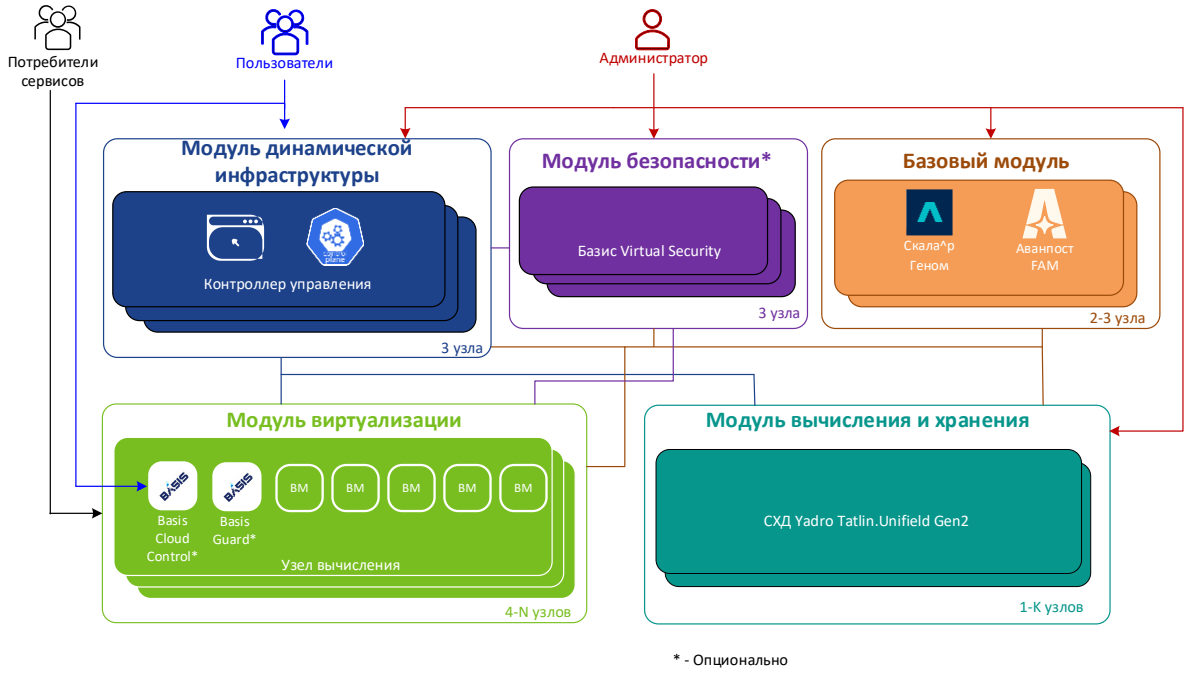

Рисунок 6. Общая архитектура Машины динамической инфраструктуры Скала^р МДИ.О

6.1 Кластер управления: назначение и характеристики

Кластер построен на узлах с ОС Astra Linux 1.8 на базе Kubernetes с установленным программным продуктом Basis Dynamix Enterprise (Рисунок 7) и агентами мониторинга. Отказоустойчивость и балансировка нагрузки кластера управления осуществляется штатными средствами Kubernetes.

В случае потери (отключения, фатального программного сбоя и т.п.) всего управляющего кластера, система виртуализации на вычислительных узлах продолжит функционировать в рабочем режиме (включая виртуальные машины), однако кластер-образующие компоненты системы виртуализации на вычислительных узлах (такие, как, например, механизм High Availability) работать не будут, как не будут доступны все сервисы управления виртуализацией.

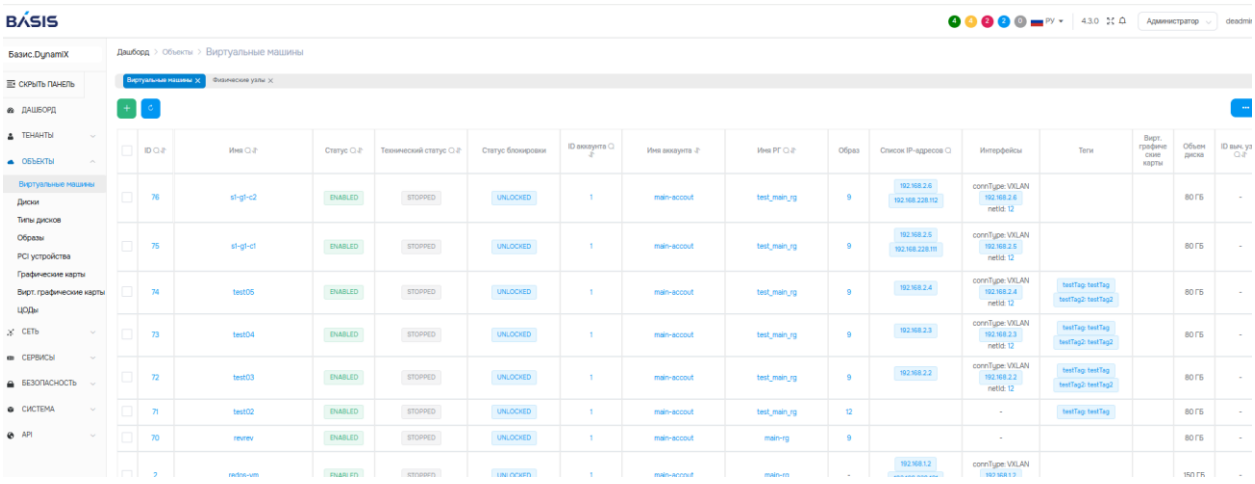

Рисунок 7. Пример интерфейса ПО Basis Dynamix Enterprise

6.2 Кластер вычисления: назначение и характеристики

Кластер вычисления предоставляет вычислительные ресурсы для виртуальных машин в рамках виртуальной инфраструктуры. Состоит из вычислительных узлов, которые формируют вычислительные мощности для системы виртуализации (ЦПУ/Память). Вычислительные узлы объединяются в единый кластер, организованный посредством гипервизора QEMU/KVM.

Кластер вычисления имеет возможность масштабирования количества узлов и изменения конфигурации узлов. Может включать до **180** вычислительных узлов.

Кластер вычисления построен на узлах с ОС Astra Linux 1.8 и гипервизором QEMU/KVM с установленными агентами мониторинга.

Опционально на кластере вычисления могут быть установлены программные продукты Basis Guard (п. 6.2.1), Basis Cloud Control (п. 6.2.2) и Octopus (п. 6.2.3), которые взаимодействуют с кластером управления.

6.2.1 Basis Guard

ПО Basis Guard – опциональный продукт, предназначенный для асинхронной репликации виртуальных машин между различными группами серверов. Может применяться для создания резервных сред между различными площадками.

Технология Basis Guard объединяет функциональность клонирования и непрерывной синхронизации сложных прикладных систем в единый удобный механизм, с помощью которого настройка и управление резервными средами значительно упрощаются, что позволяет обеспечивать аварийное восстановление работоспособности приложения в заданные временных рамках. При этом Basis Guard может поддерживать standby среды на инфраструктуре, отличной от основной среды.

Принцип работы отображен на рисунке 8. Администрирование через графический интерфейс задает параметры доступа к исходной среде и будущей standby-среде, а также выбирает параметры аварийного восстановления, которые определяют целевой режим синхронизации.

Basis Guard анализирует среды, подтверждает техническую выполнимость задачи и строит оптимальный план первичного создания standby копии прикладной среды.

После создания standby копии Basis Guard продолжает реплицировать на нее изменения, которые происходят в процессе работы приложения в исходной среде. Пользователь может контролировать статус standby среды и ожидаемые параметры восстановления (текущий показатель RPO с учетом объема изменений в ВМ плана и пропускной способности канала репликации) в графическом интерфейсе Basis Migration Assistant.

В случае отказа исходной среды Basis Guard прекращает репликационные процессы, а пользователь может активировать приложение в резервной среде. Переключение прикладной нагрузки на standby происходит в соответствии с заданными параметрами восстановления.

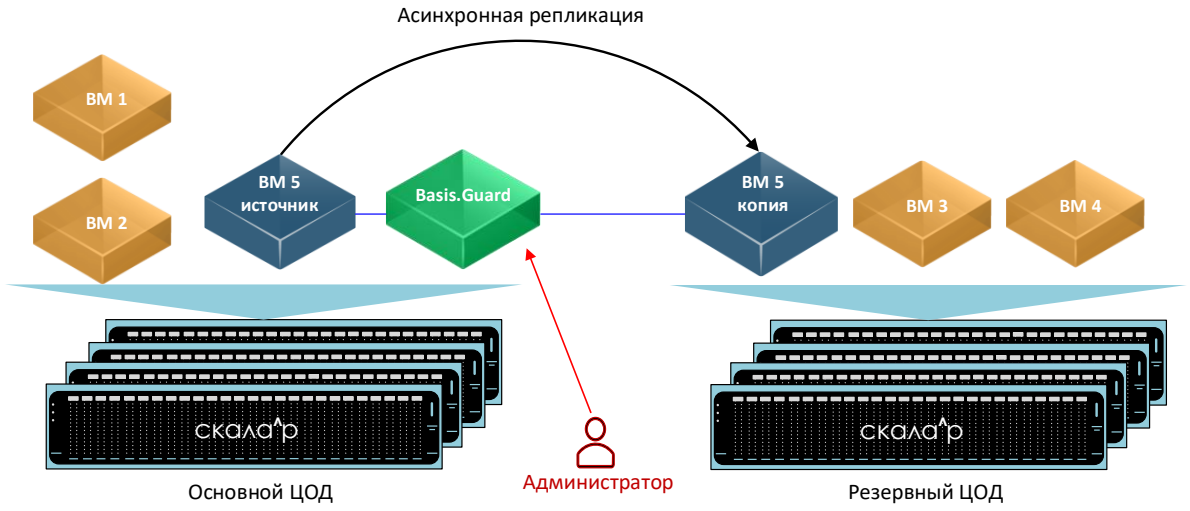

Рисунок 8. Принцип работы Basis Guard

6.2.2 Basis Cloud Control

ПО Basis **Cloud Control** – опциональный продукт, оркестратор для автоматизации облачных вычислений, предназначенный для управления частными и публичными облаками, позволяющий управлять несколькими ПАК **МДИ.О** из одного окна, автоматизировать бизнес-процессы от регистрации клиента и согласования заявок до биллинга и самообслуживания конечных пользователей (Рисунок 9).

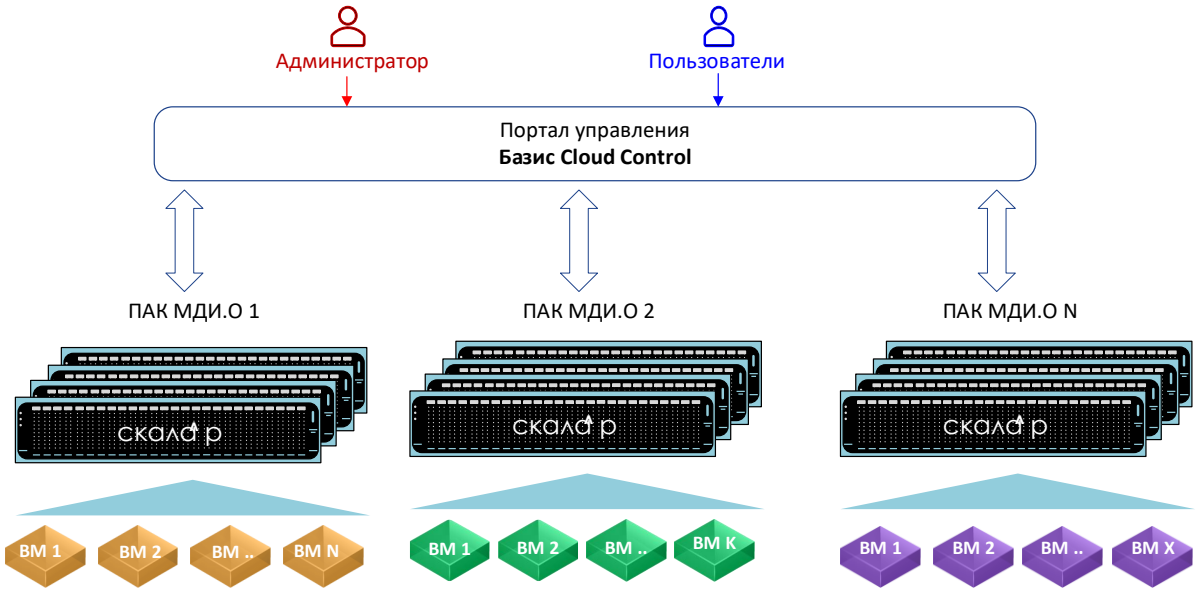

Рисунок 9. Управление Cloud Control

6.2.3 Октопус

ПО Октопус (Octopus) – опциональный компонент, выполняющий функции балансировки виртуальных машин на вычислительных узлах.

Позволяет существенно сократить финансовые затраты на расширение ЦОД за счет повышения эффективности использования серверного оборудования (путем динамического перераспределения ресурсов).

Повышает надежность бизнес-критичных приложений за счет оперативного предоставления недостающих ресурсов при пиковых нагрузках. По статистике, реальная утилизация серверного оборудования «полностью загруженного» ЦОД, использующего гипервизоры, обычно находится в диапазоне от 50% до 60%. Благодаря Октопус, реальную утилизацию можно довести до целевых 70-80%, освободив существенные мощности ЦОД

под новые задачи, либо выделив освободившиеся ресурсы наиболее ресурсоемким сервисам.

Система позволяет производить автоматическую или полуавтоматическую (с подтверждением оператора) балансировку таких ресурсов, как процессоры, оперативная память, дисковое пространство. Балансировка происходит на уровне виртуальных машин, физических хостов и хранилищ.

6.3 Узел хранения: назначение и характеристики

Узел хранения обеспечивает хранения данных системы динамической инфраструктуры **Скала^р МДИ.О,** построен на базе систем хранения данных YADRO TATLIN.UNIFIED Gen2**.**

Подключение узлов вычисления к СХД происходит по выделенной сети хранения данных и выполняется в режиме «Driver mode» по протоколу iSCSI. Для режима «Driver mode» в TATLIN требуется с управляющих узлов Dynamix доступ к API TATLIN по протоколам https и ssh.

Использование режима «Driver mode» поддерживается только для **томов с косвенной адресацией.** Том с косвенной адресацией — это том с картой указателей на блоки данных, сохраненной в области метаданных. Карта содержит статус каждого блока данных логического тома и его физический адрес, если блок занят. При создании пустой том с косвенной адресацией не занимает места в области данных. В области метаданных при этом записан минимальный объем, где отражено наличие тома и отсутствие у него занятых блоков. По мере записи информации из пула свободных блоков в области данных выделяются новые блоки. После записи в них карта указателей обновляется. В томах с косвенной адресацией размер блока равен 4 КиБ, а значит, они занимают в хранилище ровно столько места, сколько данных в них записали — с точностью до 4096 байт.

При повторной записи в уже занятые блоки данных оригинальные данные не перезаписываются. Вместо этого запись осуществляется в новые блоки с соответствующим обновлением метаданных тома. А освобожденные после перезаписи оригинальные блоки становятся доступны для последующих записей. Эта схема обеспечивает высокую производительность при записи данных «случайным» паттерном. Множество разных записей объединяется в одну последовательную запись, которая гораздо эффективнее с точки зрения быстродействия. Такой способ записи также упрощает реализацию мгновенных снимков.

Мгновенный снимок (снапшот) — это компактная с точки зрения дискового пространства копия данных, созданная в определенный момент времени. Снапшот способен моментально зафиксировать состояние тома, в отличие от резервной копии, создание которой при большом объеме данных может занять длительное время и требовать остановки записи для сохранения консистентности. Снапшот же не создает независимую копию данных, а лишь обеспечивает возможность обратиться к данным тома на момент создания снапшота.

В TATLIN.UNIFIED снапшоты создаются путем копирования карты блоков данных оригинального тома. Сами данные не копируются, поэтому снапшоты создаются очень быстро и не занимают дополнительного места в области данных.

Функциональность **клонирования дисков** доступна только для томов с косвенной адресацией. Как и снапшот, клон создается мгновенно за счет копирования карты блоков данных оригинального тома и не занимает дополнительного места в области данных. Клон доступен как для записи, так и для чтения. Блоки, на которые ссылается клон, сохраняются в области данных. Клон также может иметь снапшоты, для которых, в свою очередь, можно создавать другие клоны.

Тонкие диски для СХД TATLIN.UNIFIED Gen2 в текущем релизе не поддерживаются.

Для подключения каждого СХД к гипервизору не рекомендуется использовать количество путей, превосходящее 4 или 8 (данные числа являются оптимальными). В случае

подключения нескольких СХД, количество iSCSI сессий будет увеличиваться, что может привести к нестабильной работе iSCSI транспорта в момент частичной доступности путей.

Не следует использовать балансировщики нагрузки для iSCSI трафика, т.к. это сильно увеличивает задержки сети (latency).

Для iSCSI трафика необходимо использовать каналы данных с MTU 9000.

Необходимо избегать использования агрегированных LACP каналов передачи данных для iSCSI. Для обеспечения отказоустойчивости должна применяться технология доступа по нескольким путям (multipath).

Масштабируемость узла хранения рассчитывается исходя из потребностей заказчика (на 20 вычислительных узлов необходима 1 СХД TATLIN.UNIFIED Gen2).

6.4 Служебный узел: назначение и характеристики

Служебный узел выполняет функции обеспечения базовых сервисов, отвечает за мониторинг и управление аппаратными и программными компонентами **Скала^р МДИ.О.**

Установлены программная платформа **Скала^р Геном** и ПО **Avanpost FAM** (опция), выполняющие следующие функции:

- сбор, хранение и отображение данных мониторинга
- настройка правил оповещения
- отправка оповещений о состоянии ПАК
- управление аппаратными компонентами
- настройка программных компонентов
- настройка интеграции со сторонним ПО
- авторизация пользователей (опция FAM)

Для выполнения служебных функций, два сервисных вычислительных узла объединены в зеркальный кластер. Логическая схема работы сервисных узлов представлена на рисунке 10.

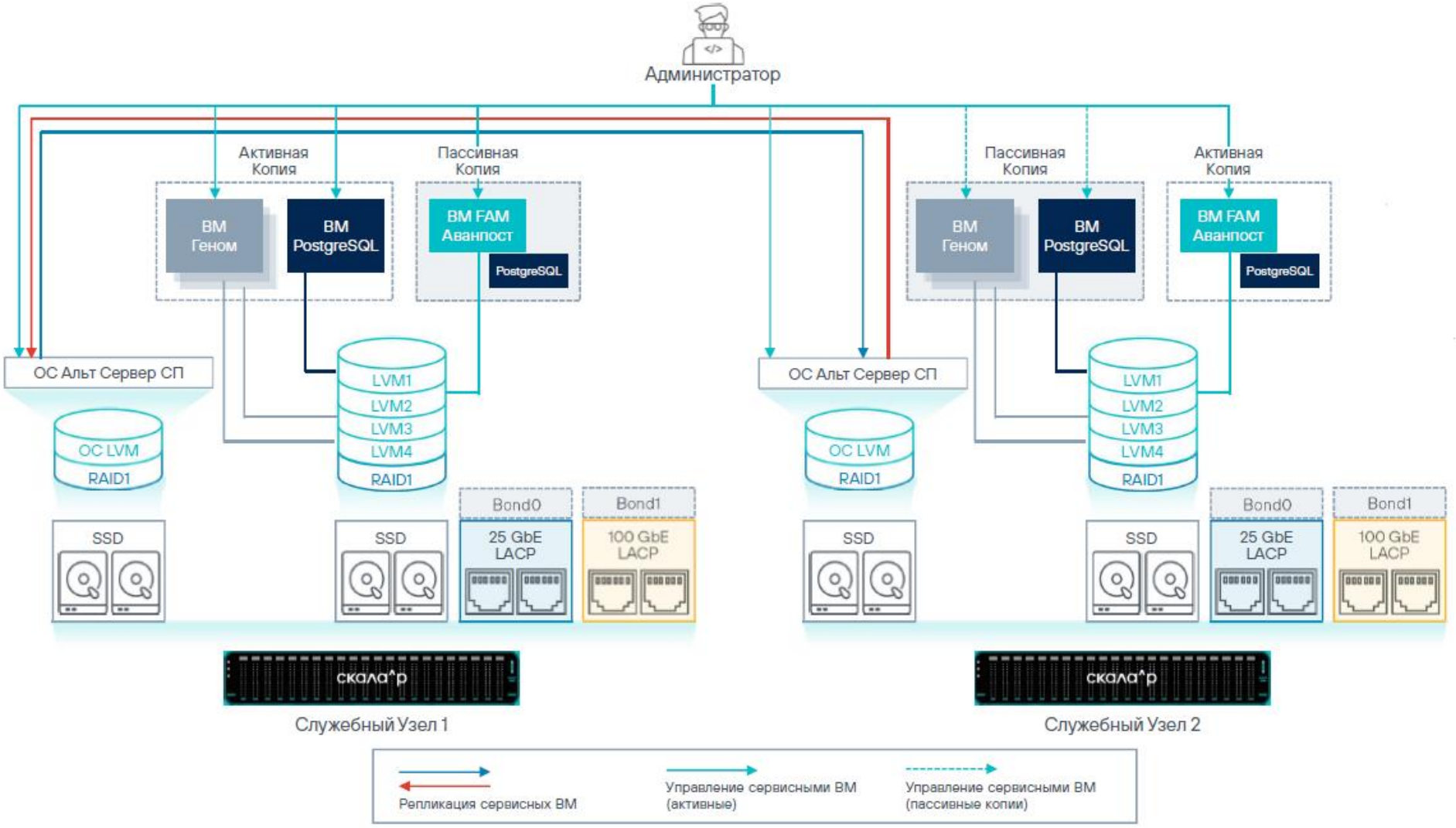

Рисунок 10. Логическая схема работы служебных (сервисных) узлов

В роли базовой операционной системы на каждом служебном узле используется ОС Альт Сервер 8 СП Release 10, сертифицированная ФСТЭК России и включенная в Единый реестр российских программ для электронных вычислительных машин и баз данных. В качестве гипервизора используется связка из программного модуля ядра KVM и эмулятора ввода-вывода QEMU из дистрибутива базовой ОС.

Отказоустойчивость работы служебных ВМ с ПО **Скала^р Геном** и Avanpost FAM на служебных узлах достигается размещением двух копий каждой сервисной виртуальной машины на разных сервисных узлах, при этом одна из них активна, другая работает в пассивном режиме.

В каждой из этой пары сервисных машин в качестве дискового устройства используется прямое подключение неформатированного логического раздела (RAW), расположенного на программном массиве RAID1 (зеркало) на двух SSD дисках. Логический раздел активной сервисной виртуальной машины реплицируется, в свою очередь в логический раздел пассивной копии (выключенной) сервисной виртуальной машины. Синхронизация данных между локальным и удаленными разделами идет через протокол TCP (без шифрования и аутентификации), по умолчанию используется порт TCP/3260 (может быть изменен).

Основной логический диск и его реплика на удаленном сервисном узле работают в режиме соответственно первичного (primary) и вторичного (secondary) узлов. Вторичный (резервный) узел хранит реплику, но не позволяет осуществить к ней локальный доступ, первичный же позволяет осуществить локальный доступ. Как только происходит повышение роли логического диска до первичного, доступ открывается и сам диск больше не будет принимать реплику, а наоборот, будет отдавать свою реплику на удаленный узел.

6.4.1 Программная платформа Скала^р Геном

Программная платформа **Скала^р Геном** предназначена для управления жизненным циклом ПАК, диагностики, мониторинга, обслуживания и управления как отдельным ПАК, так и инфраструктурой, состоящей из множества различных ПАК **Скала^р**. **ПО Геном** обладает, в частности, следующим функционалом:

- ведение электронного паспорта **Машины**
- отслеживание состояния узлов
- предоставление доступа к IPMI всех узлов **Машины**
- вывод узла **Машины** в режим обслуживания
- загрузка и запуск обновления ПО
- сбор данных о конфигурации элементов **Машины**
- сбор данных, отображение, мониторинг элементов ПО, активных компонентов Модулей **Машины**, служебных сервисов и сервисов БД
- конфигурирование метрик мониторинга, настройка уведомлений
- конфигурирование графического отображения на информационных панелях в виде графиков, отдельных значений, диаграмм, таблиц
- хранение метрик с возможностью настройки глубины хранения и управления жизненным циклом хранимых данных
- отображение в пользовательском графическом интерфейсе данных о состоянии объектов мониторинга
- контроль изменений объектов мониторинга в режиме, близком к реальному времени
- сбор и мониторинг логов
- мониторинг сервисов, специфичных для различных типов **Машин**

Объектом мониторинга **Скала^р Геном** может быть любой физический или логический объект, например, память, процессор, файловая система, количество пользователей, очередь файлов на обработку, объем обработанного трафика, значение температуры и другие.

Отличительной особенностью ПО **Скала^р Геном** являются возможности мониторинга специфичных параметров ПАК, обеспечивающих его надежность и производительность, что позволяет выполнять быстрый и качественный анализ причин возникновения внештатных ситуаций, строить прогнозы развития ситуации в будущем.

Сбор данных с узлов ПАК осуществляется с помощью установленных агентов ОС и служебной СУБД.

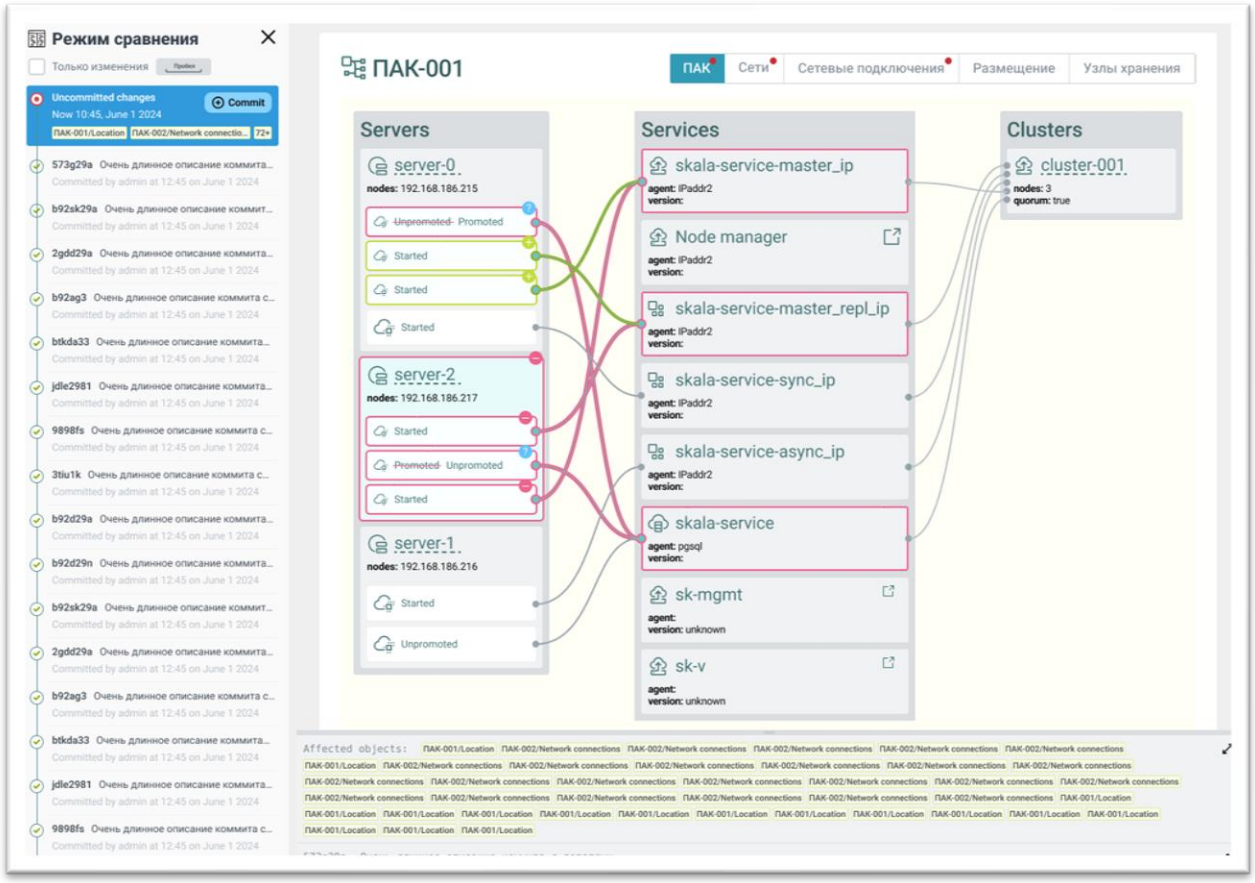

Рисунок 11. Пример интерфейса ПО Скала^р Геном (отображение схемы подключений узлов ПАК)

ПО **Скала^р Геном** позволяет проводить настройку появления новых критических уведомлений, условия их получения гибко настраиваются в соответствии с текущими потребностями (Рисунок 12). Имеется возможность управлять формированием почтовых уведомлений: регулировать их группировку, частоту отправки и т.д.

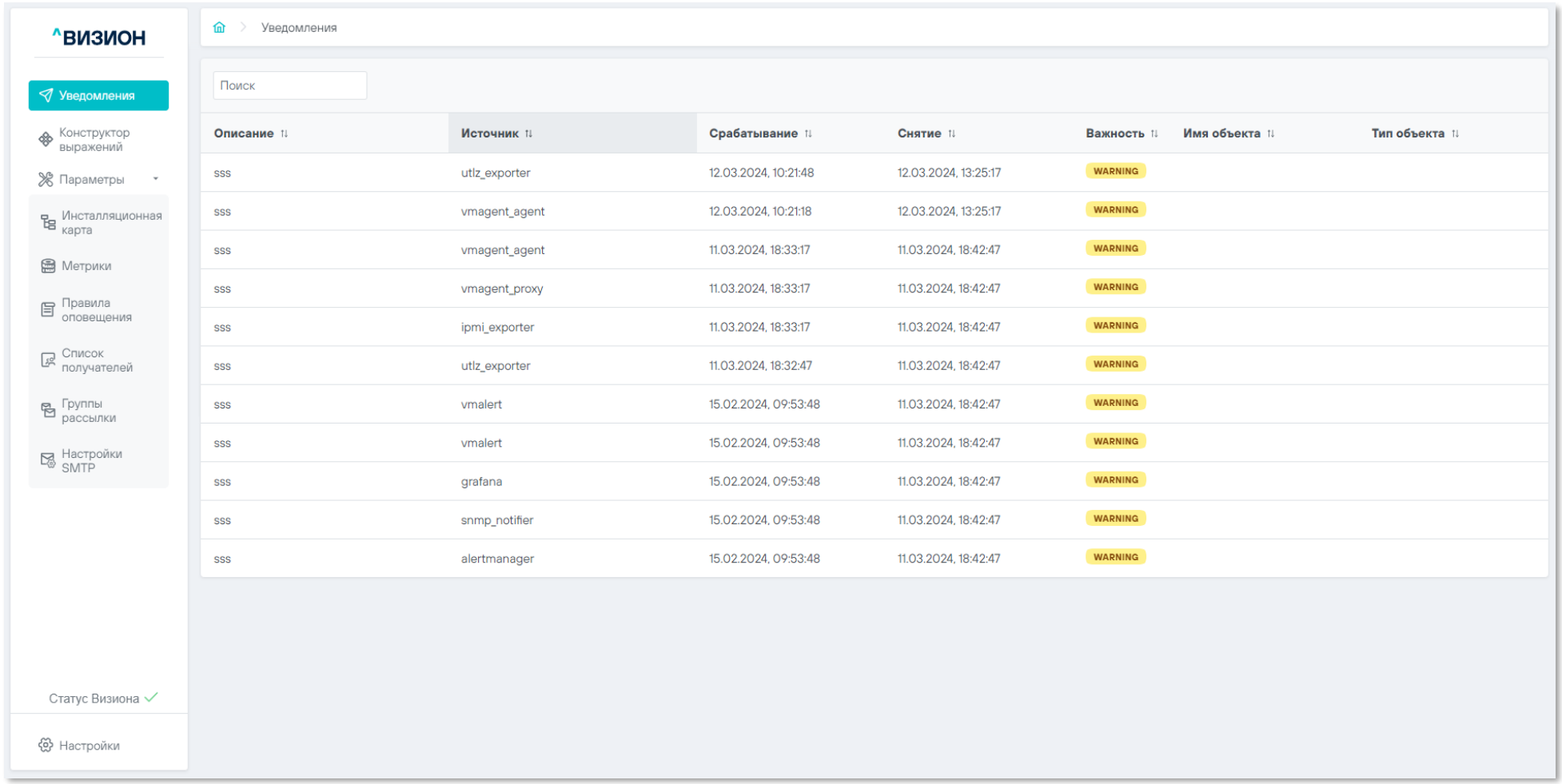

Рисунок 12. Пример интерфейса ПО Скала^р Геном (пример окна настройки уведомлений мониторинга)

Если при эксплуатации ПАК используются дополнительные каналы доставки уведомлений, возможна настройка их трансляции во внешнюю систему управления оповещениями об инцидентах. Эта настройка производится в пользовательском интерфейсе раздела мониторинга ПО **Скала^р Геном**:

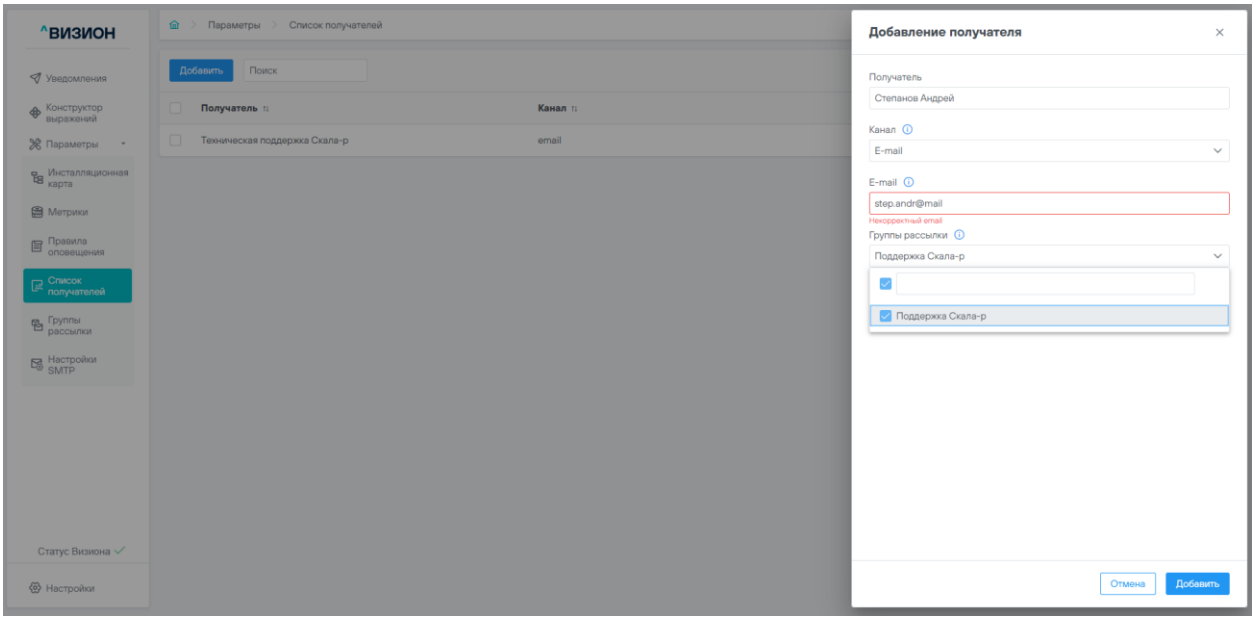

Рисунок 13. Пример интерфейса ПО Скала^р Геном (настройка пересылки сообщений)

Архитектурно, программная платформа **Скала^р Геном** состоит из следующих сервисных виртуальных машин, вместе образующие программную платформу обслуживания, управления и мониторинга **Скала^р Геном** (Рисунок 14): ВМ Платформы (сервер управления), ВМ Топологии (сервер топологии, CMDB) и ВМ Мониторинга (**Визион**).

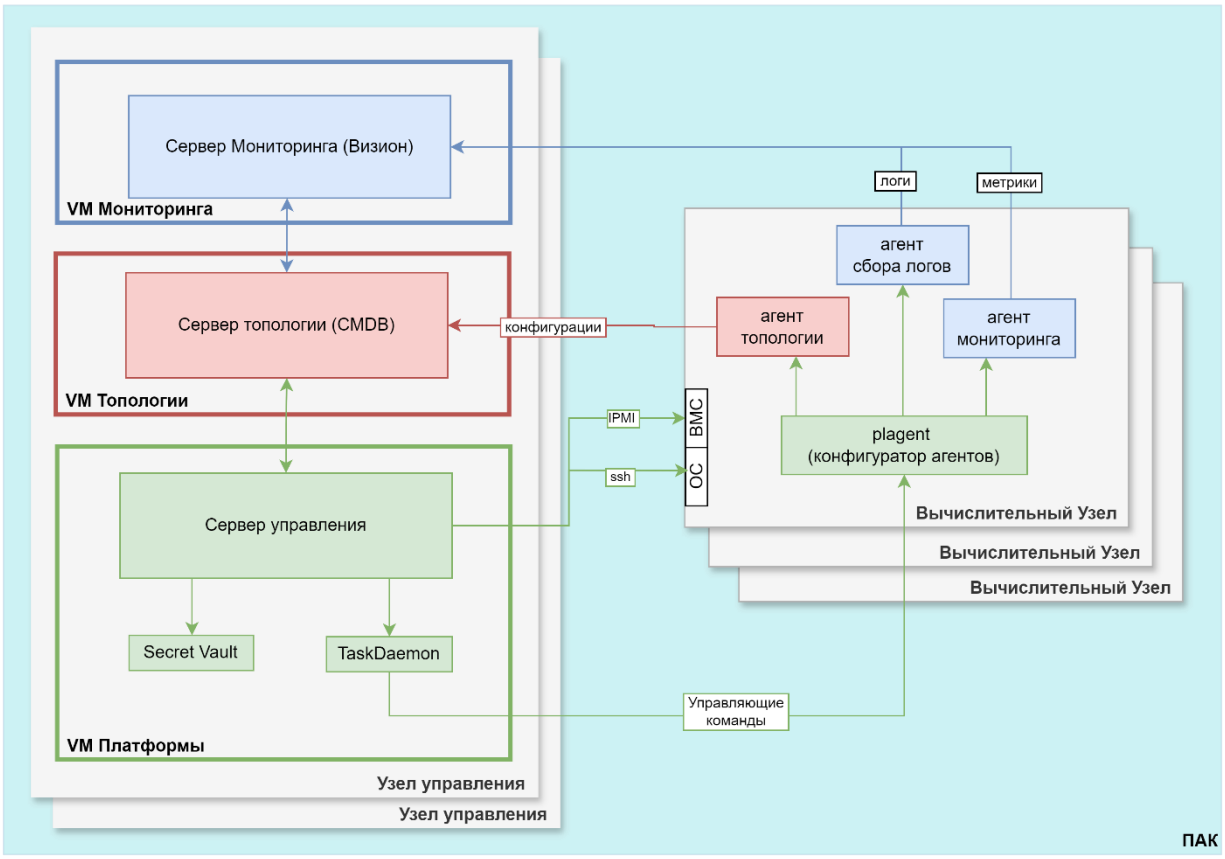

Рисунок 14. Основные компоненты программной платформы Скала^р Геном

Программная платформа **Скала^р Геном** может быть развернута как в режиме, обеспечивающем обслуживание одного ПАК (Рисунок 14), так и в режиме централизованного управления несколькими ПАК, обеспечивающем управление инфраструктурой, состоящей из множества ПАК **Скала^р** (Рисунок 15). В последнем случае, на служебных узлах подчиненных ПАК разворачиваются ВМ прокси-сервера топологии и ВМ прокси-сервера мониторинга, передающие соответствующие данные на служебные узлы основного ПАК. При этом сервер управления, развернутый на ВМ Платформы основного ПАК, обеспечивает непосредственное управление агентами, установленными на вычислительных узлах подчиненных ПАК.

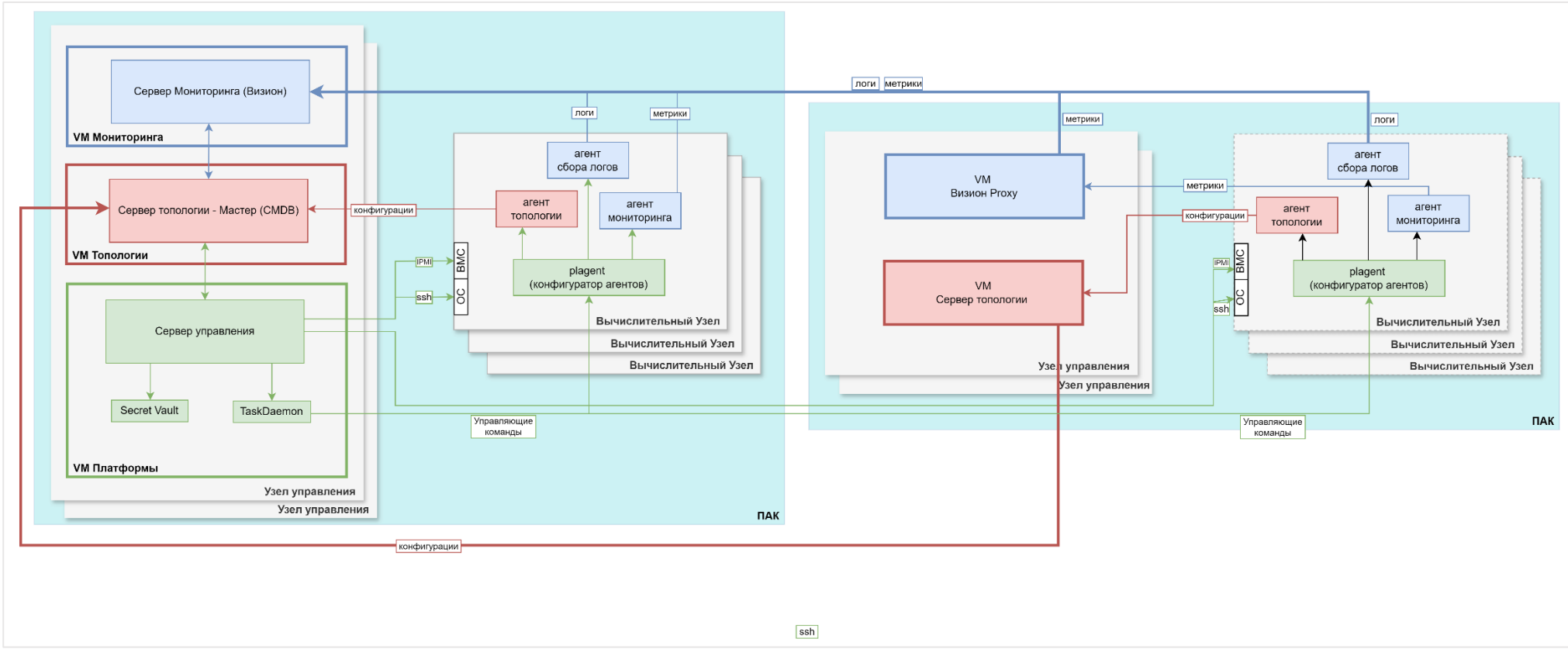

Рисунок 15. Программная платформа Скала^р Геном в режиме централизованного управления несколькими ПАК

6.5 Модуль безопасности: назначение и характеристики

Узлы управления Модуля безопасности – опциональный кластер, выполняет функции авторизации, обеспечения безопасности системы управления и системы виртуализации. Предназначен для использования в государственных информационных системах до 1 класса защищенности включительно, в информационных системах персональных данных до 1 уровня защищенности включительно, в автоматизированных системах до класса 1Г включительно.

Кластер состоит из трех вычислительных узлов с ОС Astra Linux 1.8 на базе программного продукта Basis Virtual Security (BVS, именование в реестре ПО Минцифры – Базис.Virtual Security).

Узел управления BVS обеспечивает выполнение следующих функций безопасности:

- идентификация, аутентификация и авторизация пользователей в средстве виртуализации
- доверенная загрузка виртуальных машин средством виртуализации
- контроль целостности в средстве виртуализации
- регистрация событий безопасности в среде виртуализации
- управление доступом пользователей в среде виртуализации
- управление потоками информации в среде виртуализации
- ограничение программной среды

Взаимодействует с кластером управления и кластером вычисления.

Схема взаимодействия компонентов Basis Virtual Security представлена ниже (Рисунок 16).

Basis Virtual Security состоит из подсистем:

1. Подсистема проксирования, реализованная на прокси-сервере NGINX, с помощью которого реализуется проксирование запросов до сервисов Basis Virtual Security и реализуется поддержка TLS
2. Подсистема авторизации состоит из компонентов:

- virtual-security-admin – основной компонент, который реализовывает бизнес-логику, обеспечивает интеграцию между подсистемами программного модуля и предоставляет API
- virtual-security-web – программный компонент, который предоставляет графический интерфейс администратору для централизованного управления программным модулем и различными функциями безопасности, которые данный программный модуль реализует
- virtual-security-auth – сервис, который отвечает за реализацию функций безопасности, связанных с идентификацией, аутентификацией пользователей в средстве виртуализации и в других внешних системах с использованием протоколов OpenID Connect (OIDC), SAML 2.0, Kerberos, LDAP/Active Directory, FreeIPA, ALDpro
- ldap-server – LDAP-сервис, который обеспечивает реализацию протокола легковесного доступа к каталогам (LDAP, Lightweight Directory Access Protocol) и позволяет выполнять операции создания, хранения, изменения и удаления различных записей в указанных каталогах, в том числе управлять жизненным циклом учетных записей пользователей

- virtual-security-pg-pam – сервис, который обеспечивает аутентификацию по токену сессии, выданному в соответствии со стандартом OpenID Connect, при удаленном или локальном доступе систем, обращающихся к служебной СУБД Postgres Pro от имени ранее аутентифицированных пользователей

3. Подсистема СУБД, реализованная на Postgres Pro (сертифицированная ФСТЭК версия) как объектно-реляционная система управления базами данных
4. Подсистема взаимодействия с агентами, реализованная сервисом vcore-broker – это шина обмена сообщениями, которая выполняет транспортные функции в программном модуле и гарантирует доставку различных управляющих сигналов между программными компонентами серверной части и сервисом-агентом virtual-security-agent, который функционирует на вычислительных узлах
5. Подсистема агрегации системных журналов обеспечивает хранение и индексацию журналов событий программного модуля Базис.Virtual Security и других внешних систем

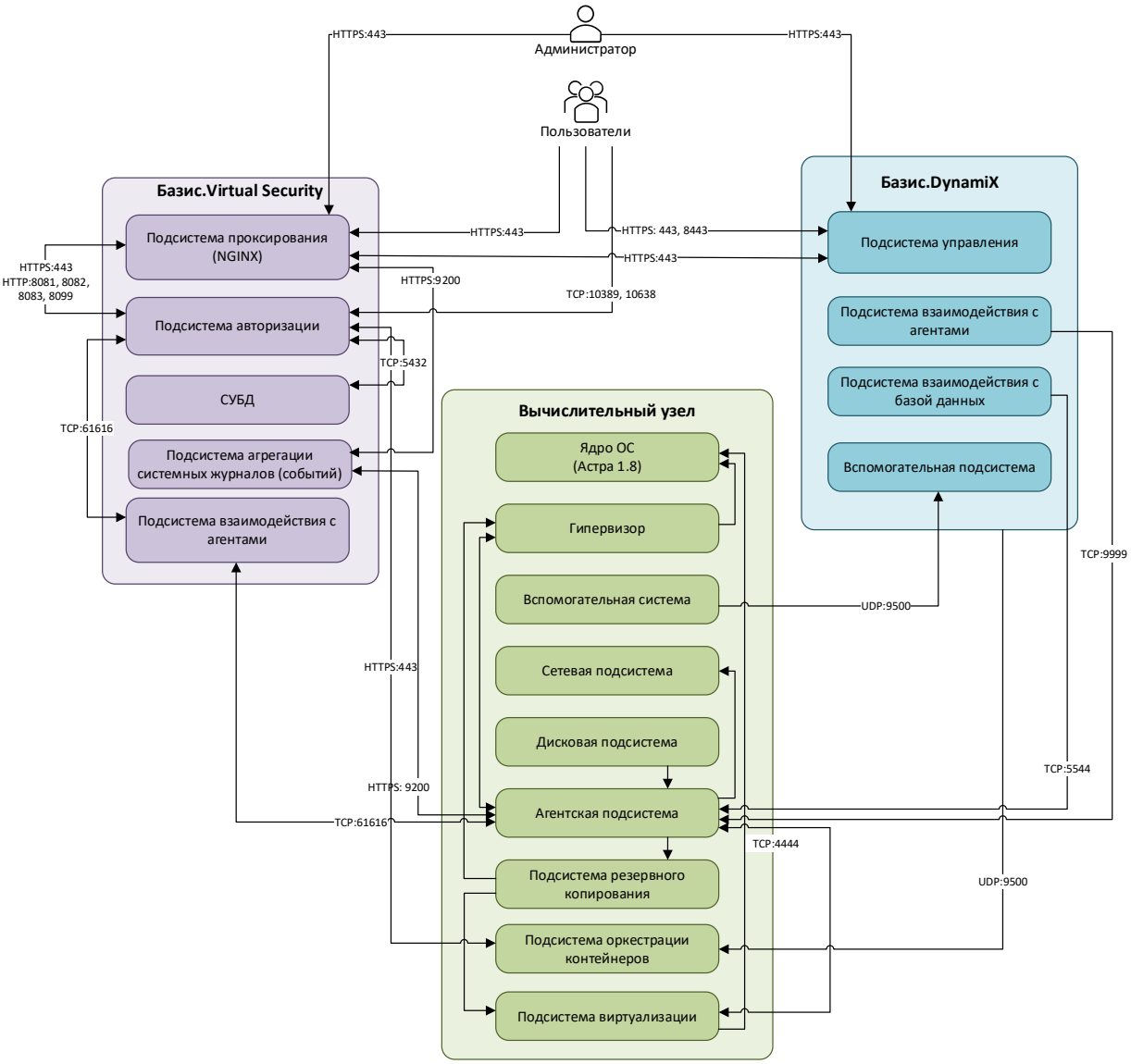

Рисунок 16. Схема взаимодействия компонентов Basis Virtual Security

6.6 Сетевое взаимодействие

Схема взаимодействия между компонентами **Скала^р МДИ.О** приведена на рисунке (Рисунок 17).

Сетевой узел управления подключается к сети управления заказчика и обеспечивает функционирование сетей управления административного доступа – **adm_mgmt** и сети управления оборудованием IPMI – **hw_mgmt**.

Сетевой узел внутреннего взаимодействия обеспечивает функционирование сетей:

- передачи данных между ресурсами платформы, миграции виртуальных машин – **backplane**
- управления ресурсами платформы – **mgmt**
- VXLAN туннелей для связи виртуальных машин – **vxbackend**
- управления виртуальными шлюзами (ViNS и LoadBalanced) – **gw_mgmt**
- управления ресурсами – **bvs_mgmt** (опционально)

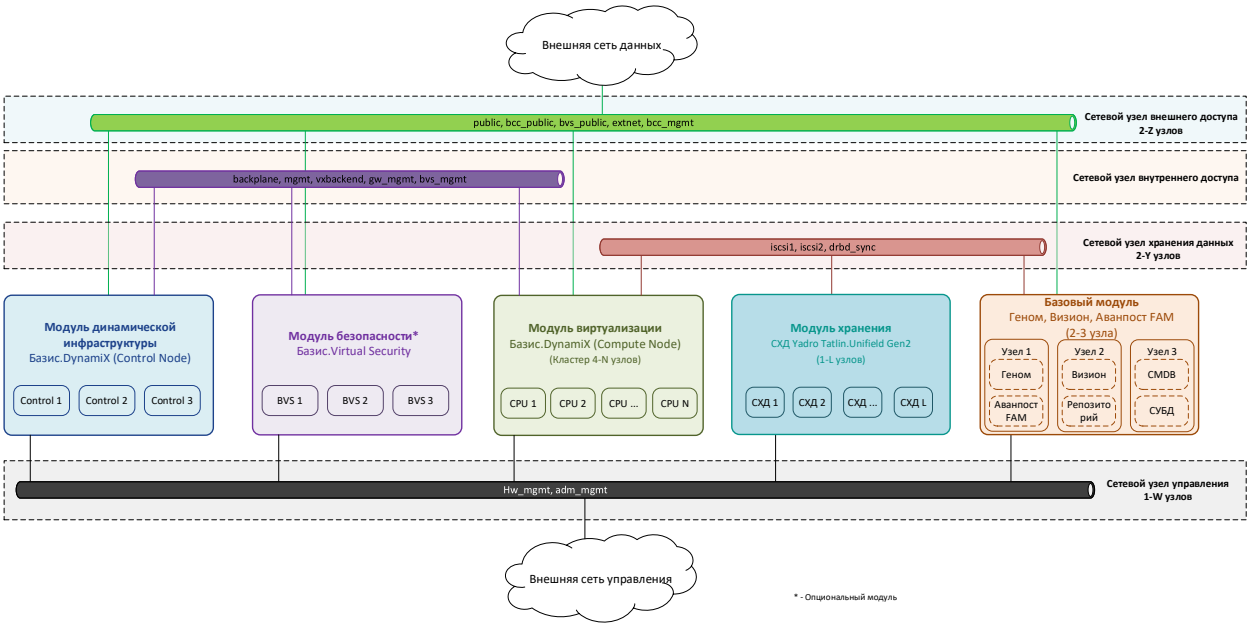

Рисунок 17. Схема взаимодействия узлов Машины динамической инфраструктуры

Сетевой узел внешнего доступа подключается к внешней сети заказчика, обеспечивает функционирование сетей:

- доступа к WEB интерфейсу – **public**
- доступа к Basis Cloud Control – bcc_public (опционально, при включении ПО в **Машину**)
- управления Basis Cloud Control – bcc_mgmt (опционально, при включении ПО в **Машину**)
- доступа к WEB интерфейсу Basis Virtual Security – **bvs_public** (опционально)
- доступа для потребителей сервисов (внешняя сеть для ВМ) – **extent**

На сетевом узле хранения данных организованы сети:

- хранения данных для взаимодействия вычислительных узлов с СХД **iscsi1** и **iscsi2**
- репликации DRBD трафика служебного узла **drbd_sync**

Один из вариантов эталонной коммутации **Машины** приведен на рисунке 18.

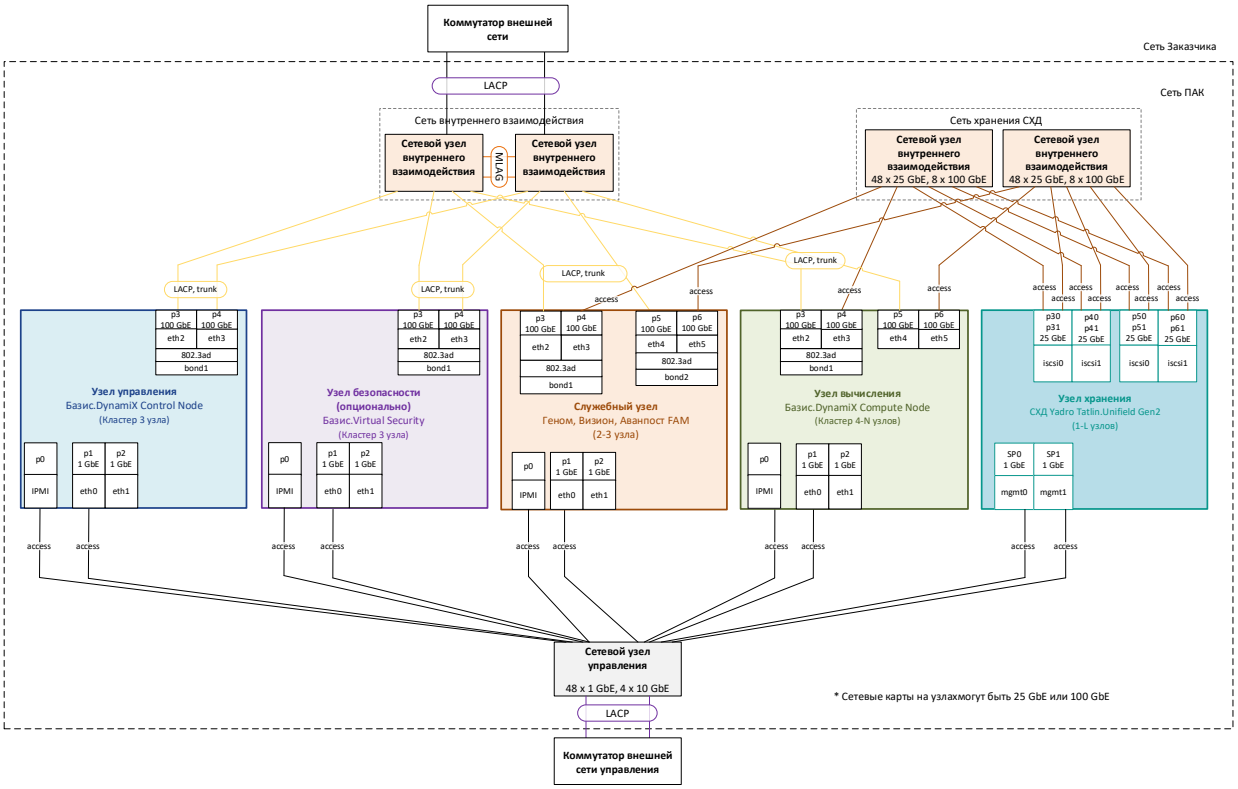

Рисунок 18. Схема коммутации Машины

Для подключения к внешним сетям в **Машине** используются два сетевых узла с портами 10/25 Гбит/с и uplink-портами 100 Гбит/с. Сетевые узлы собраны в отказоустойчивую группу MLAG, что позволяет подключать к паре сетевых узлов узлы и другие устройства, используя протокол LACP. На стеке сетевых узлов внешних сетей реализован сетевой сегмент External VLAN.

Для реализации сети интерконнекта используются два сетевых узла с портами 25 или 100 Гбит/с. Сетевые узлы собраны в отказоустойчивый кластер с использованием технологии MLAG, что позволяет подключать к паре сетевых узлов узлы и другие устройства, используя протокол LACP. На стеке сетевых узлов внешних сетей реализован сетевой сегмент Internal VLAN.

Для реализации сетей управления используется один сетевой узел с портами 1 Гбит/с и uplink-портами 10 Гбит/с. Сетевой узел управления подключен к виртуальному коммутатору внешних сетей двумя портами 10 Гбит/с, собранными в bond-интерфейс по протоколу LACP.

7. ТЕКУЩИЕ ОГРАНИЧЕНИЯ

В текущем релизе имеется ряд ограничений, которые описаны ниже.

7.1 Виртуальные ресурсы

Ограничения по переподписке виртуальных ресурсов:

- не рекомендуется выделять на одну виртуальную машину виртуальных процессоров больше, чем установлено на физическом сервере. Так, если в физическом сервере установлен один процессор с 10 ядрами и 20 потоками, то не рекомендуется использовать в одной виртуальной машине более 20 виртуальных процессоров
- соотношение суммарного количества виртуальных процессоров на всех виртуальных машинах к суммарному количеству ядер на физическом сервере не должно превышать 10:1, рекомендуется не более 3:1
- рекомендуется, чтобы общее количество виртуальных процессоров на виртуальной машине была ниже, а максимальная утилизация виртуальных процессоров была выше (например, использование 2-х виртуальных процессоров с максимальной утилизацией 80% лучше, чем 8-и виртуальных процессора и утилизацией 20%)

7.2 Узлы управления

При инсталляциях более 60 вычислительных узлов необходимо закладывать дополнительные ресурсы на узлах управления под журналы событий.

7.3 Вычислительные узлы

Ограничения в отношении вычислительных узлов:

- максимальное количество вычислительных узлов – 180 штук
- максимальное количество виртуальных машин на физический сервер – 250
- максимальное количество ядер или потоков на физический сервер – 768
- максимальный объем памяти на одну виртуальную машину – 4 Тбайт
- максимальный объем памяти на один физический сервер – 12 Тбайт

7.4 СХД TATLIN.UNIFIED Gen2

- Максимальное количество ресурсов на 1 СХД TATLIN.UNIFIED Gen2 в составе ПАК – 700
- Рекомендуемое подключение 20-23 вычислительных узлов на 1 СХД

Основные отличия между Driver mode и Shared LUN представлены в таблице ниже.

Таблица 1. Основные отличия между Driver mode и Shared LUN

Driver mode	Shared LUN
Положительные особенности: ▪ действия с LUN выполняются с помощью API драйвера СХД	**Положительные особенности:** ▪ используется для любых СХД ▪ лицензируется только 50 Тбайт

Driver mode	Shared LUN
▪ диски напрямую пробрасываются в виртуальные машины ▪ стабильность работы ▪ скорость работы ▪ snapshot и clone средствами СХД (версия прошивки TATLIN –3.1.1 ▪ быстрое подключение при вводе в эксплуатацию	
Отрицательные особенности: ▪ лицензируется весь сырой объем	**Отрицательные особенности:** ▪ долго настраивается и подключается при вводе в эксплуатацию (сложность настройки, есть человеческий фактор)
Ограничения: ▪ количество снимков – 20	**Ограничения:** ▪ создание не более 30 пулов ▪ создание в пуле не более 4 LUN ▪ объем LUN не более 20 Тбайт ▪ подключение к СХД не более 50 вычислительных узлов ▪ количество снимков – 5 при миграции между ПАК ограничение для SHARED SEP pool allocation_type file: диск/диски размером более **30 Гбайт нельзя мигрировать в SHARED SEP File**. Из SHARED SEP File в любой другой тип СХД миграция возможна без ограничений.

7.5 Сеть

- Поддерживается только IPv4; IPv6 не поддерживается

7.6 Виртуальные машины

Максимально возможный объем памяти на одну виртуальную машину – 950 Гбайт.

Максимальное количество виртуальных процессоров на одну виртуальную машину – 256.

Для виртуальных машин на чипсете I440FX:

- допустимо использовать 4 виртуальные графические карты
- ограничения СХД: 9 дисков (1 загрузочный + 8 дисков с данными)
- ограничения сети: 8 сетевых интерфейсов

Для виртуальных машин на чипсете Q35:

- максимальное количество GPU – 36, рекомендовано не более 4

- максимальное количество дисков на одну ВМ 70 (1 загрузочный + до 69 дополнительных), рекомендованное – не более 8
- минимальный объем диска – 1 Гбайт (для загрузочного диска)
- максимальный объем диска – 60 Тбайт
- максимальное количество подключений к сетям на одну ВМ – 38, рекомендованное не более 8
- максимальное количество подключений ВМ к одной и той же сети – 1
- максимальная пропускная способность одного сетевого интерфейса – 3.5 Гбит

8. СПЕЦИФИЧНЫЕ ЧЕРТЫ

Проектирование и реализация **Машины динамической инфраструктуры Скала^р МДИ.О** осуществлялись с учетом ряда выбранных приоритетов, оказывающих непосредственное влияние на функциональные и эксплуатационные показатели. Наиболее значимые из них рассмотрены ниже.

Применение стандартного высоконадежного и производительного оборудования в качестве платформы для размещения компонентов взамен уникальных аппаратных разработок

Эффект:

- обеспечение стабильного уровня производительности (компоненты проверены временем)
- повышение надежности ПАК (нет уникальных элементов)
- снижение стоимости сопровождения (доступность элементов при выходе из строя)

Возможность интеграции типового и стороннего ПО для мониторинга и управления в дополнение к предустановленным

Эффект:

- сохранение ранее сделанных инвестиций в системы управления ИТ-инфраструктурой
- возможность построения сквозных систем управления, в которые интегрируются **Машины** и в которых **Скала^р МДИ.О** — лишь один из элементов

9. ГАРАНТИРОВАННОЕ КАЧЕСТВО

Качественные показатели **Машины динамической инфраструктуры Скала^р МДИ.О** обеспечиваются ее соответствием проверенному стандартному варианту, соблюдением установленных норм и требований по формированию, реализацией работ высококвалифицированными специалистами на всех этапах жизненного цикла.

Производство (комплектование и развертывание ПО)

- при производстве используются высококачественные комплектующие
- сборка продукции осуществляется строго в соответствии с утвержденным планом размещения компонентов
- развертывание и первичная конфигурация **Машины** осуществляются в автоматическом режиме
- дополнительные настройки ПО осуществляются в соответствии с утвержденной методикой и пошаговой инструкцией
- осуществляется функциональное тестирование сформированной **Машины**
- при необходимости возможны индивидуальные конфигурации **Машины Скала^р МДИ.О**

Передача в эксплуатацию

- **Машина** полностью сформирована, протестирована, готова к размещению в сети заказчика и подключению прикладного ПО
- в комплекте с **Машиной** передаются паспорт и сертификат на поддержку
- передается комплект документации, необходимый контролирующим организациям для аттестации **Машины** в контуре заказчика
- по запросу проводится обучение специалистов заказчика работе с **Машиной**

Поддержка

- **Скала^р МДИ.О** поставляется с годовой поддержкой (более выгодный вариант — на 3 или 5 лет), которая включает в себя решение вопросов, связанных с нарушениями работоспособности как комплекса в целом, так и его отдельных аппаратных компонентов и программного обеспечения
- первая и вторая линия поддержки предоставляются непосредственно производителем **Машины** или сертифицированным партнером **Скала^р**
- заказчик имеет возможность выбора варианта поддержки из актуальных на момент поставки (как минимум, из вариантов 9×5 или 24×7)
- в сложных случаях, в решении проблем на третьей линии поддержки участвуют архитекторы и инженеры, разработчики **Скала^р МДИ.О**

Сопровождение

По запросу возможна реализация дополнительных требований по модернизации или развитию **Машины**, в том числе:

- аппаратная модернизация ПАК
- горизонтальное или вертикальное масштабирование **Машины**

Работы выполняются с участием архитекторов и инженеров, разработчиков **Машины** и ПО **Скала^р**.

10. ТРЕБОВАНИЯ К РАЗМЕЩЕНИЮ МАШИНЫ

Машина динамической инфраструктуры Скала^р МДИ.О представляет собой комплект узлов для размещения в серверный монтажный шкаф 19”, высота 42U и больше, с дальнейшей возможностью модульной расширяемости до 14 стоек (или более).

Монтажный шкаф (стойка) может быть поставлен как опция.

Для подключения шкафа к системе электроснабжения должны быть предусмотрены два независимых входа электропитания.

Расчетная потребляемая мощность шкафа (задается параметрами ЦОД заказчика) определяет топологию размещения модулей и узлов в стойках ЦОД и учитывается при расчете **Машины**. От этого зависит количество дополнительного коммутационного оборудования в составе **Машины**.

В месте установки должны быть предусмотрены соответствующие мощности по отводу тепла.

Для подключения к локальной сети заказчика необходим резервированный канал до 4×100 Gigabit Ethernet или до 8×10/25 Gigabit Ethernet. Требуемые трансиверы определяются на этапе формирования спецификации **Машины**.

При развертывании будут выполнены настройки сетевых адресов в соответствии со структурой сети заказчика. Заказчик должен предоставить необходимые данные в соответствии с номенклатурой компонентов **Машины**.

В сети заказчика должны быть настроены соответствующие маршруты и права доступа.

Дальнейшие мероприятия по вводу в эксплуатацию осуществляются заказчиком путем настройки прикладных программных систем.

11. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Поставка **Машины динамической инфраструктуры Скала^р МДИ.О** осуществляется с предварительными сборкой, тестированием и настройкой оборудования согласно требованиям заказчика. Качественная поддержка обеспечивается едиными стандартами гарантийного и постгарантийного технического обслуживания:

- пакет услуг по технической поддержке на первый год включен в поставку
- заказчик может выбирать пакет 9×5 или 24×7 (вариант для комплексов критической функциональности)
- срок начально приобретаемой технической поддержки может быть увеличен до 3-х и 5-и лет, также доступна пролонгация поддержки

Состав типовых пакетов услуг по технической поддержке **Скала^р МДИ.О** представлен в таблице 2.

Таблица 2. Пакеты услуг по технической поддержке

Услуги	Пакет «9×5»	Пакет «24×7»
«Режим предоставления услуг 9×5» (в рабочее время по рабочим дням)	+	–
«Режим предоставления услуг 24×7» (круглосуточно)	–	+
Предоставление доступа к системе регистрации запросов/инцидентов Service Desk	+	+
Предоставление доступа к базе знаний по продуктам **Скала^р**	+	+
Предоставление обновлений лицензионного ПО **Скала^р**	+	+
Диагностика, анализ и устранение проблем в работе комплекса **Скала^р**, включая: устранение аппаратных неисправностей техническое сопровождение ПО	+	+
Консультации по работе комплекса **Скала^р**	+	+
«Защита конфиденциальной информации» (неисправные носители информации не возвращаются заказчиком)	Опция	Опция
Замена и ремонт оборудования по месту установки	+	+
Доставка оборудования на замену за счет производителя	+	+

Услуги	Пакет «9×5»	Пакет «24×7»
Расширенные параметры обслуживания	–	+
Времена реагирования и отклика, не более:		
Время регистрации обращений	30 минут, рабочие часы (9×5)	30 минут, круглосуточно (24×7)
Подключение специалиста к решению инцидентов критичного и высокого уровней	В течение 1 рабочего часа (9×5)	В течение 1 часа (24×7)

Примечание к срокам ремонта оборудования

Комплекс **Машина динамической инфраструктуры Скала^р МДИ.О** архитектурно является устойчивым к выходу из строя отдельных компонентов и даже узлов, поэтому нет необходимости в обеспечении дорогостоящего сервиса срочного восстановления оборудования в течение суток и менее. В комплексе предусмотрено как минимум двойное резервирование основных компонентов, позволяющее сохранять данные и работоспособность даже при выходе из строя нескольких дисков и/или серверов (узлов).

12. ПОСТАВКА И ЛИЦЕНЗИРОВАНИЕ ПО

Команда **Скала^р** активно занимается развитием программных продуктов **Машин динамической инфраструктуры Скала^р МДИ.О**. Направления развития формируются на основе анализа мирового опыта использования систем подобного класса и пожеланий заказчиков и партнеров. Новые функции реализуются в форме релизов, которые могут выходить несколько раз в год.

Лицензируемое программное обеспечение в составе **Машины динамической инфраструктуры Скала^р МДИ.О**:

- Basis Dynamix Enterprise
- Basis Virtual Security (опция)
- ОС «Astra Linux Special Edition»
- ОС «Альт СП» (на служебных узлах Базового модуля)
- СУБД Postgres Pro Standard Certified (служебная СУБД для **Геном**/Avanpost FAM – на служебных узлах Базового модуля)

Программное обеспечение **Скала^р Геном** поставляется исключительно в составе **Машин Скала^р** и лицензируется по метрикам комплекса в соответствии с количеством серверных узлов.

12.1 Политика обновления ПО

Команда **Скала^р** активно занимается развитием собственных программных продуктов. Направления развития формируются на основе анализа мирового опыта использования систем подобного класса и пожеланий заказчиков и партнеров. Новые функции реализуются в форме релизов. Обновления для **Машин**, находящихся в эксплуатации, производятся по согласованию с заказчиком.

Настоящий технический обзор описывает **Машину динамической инфраструктуры Скала^р МДИ.О** с версиями ПО, представленными в таблице3.

Таблица 3. Пакеты услуг по технической поддержке

Название ПО	Версия ПО
ОС «Astra Linux Special Edition»	1.8
ОС «Альт СП» (на служебных узлах базового модуля)	c10f2
Basis Dynamix Enterprise	4.4
Basis Virtual Security (опция)	4.0
Программная платформа Скала^р Геном	1.18.3
ПО класса Identity & Access Management «Avanpost FAM»	1.13.6

О КОМПАНИИ

Скала^р – модульная платформа для построения высоконагруженной ИТ-инфраструктуры (продукт Группы Rubytech).

Программно-аппаратные комплексы (**Машины**) **Скала^р** выпускаются с 2015 года и представляют широкий технологический стек для построения динамических инфраструктур и инфраструктур управления данными высоконагруженных информационных систем.

Продукты **Скала^р** включены в Реестр промышленной продукции, произведенной на территории Российской Федерации, и в Единый реестр российских программ для ЭВМ и БД. Соответствует критериям доверенности и использованию для объектов критической информационной инфраструктуры (КИИ).

Машины Скала^р являются серийно выпускаемыми преднастроенными комплексами, которые быстро развертываются и вводятся в эксплуатацию. Глубокая интеграция технических средств и программного обеспечения в ПАК **Скала^р** позволяет получить расширенные возможности и функциональность, которые недоступны при использовании отдельных компонентов.

Модульный принцип обеспечивает интеграцию разнородных компонентов ИТ-инфраструктуры в единую платформу предприятий, корпораций и ведомств. Единые поддержка и сервисное обслуживание для всех продуктов линейки **Скала^р** от производителя обеспечивают оперативное разрешение инцидентов на стыке технологий.

Дополнительная информация – на сайте www.skala-r.ru.