скала^р

Машина динамической инфраструктуры Скала^р МДИ.О

Масштабируемый и отказоустойчивый ПАК
для динамической облачной инфраструктуры виртуализации

Технический обзор

версия 1.88 от 08.12.2025

skala-r.ru info@skala-r.ru

Оглавление

Уведомление

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

Информация в настоящем документе относится к **Машине динамической инфраструктуры Скала^р МДИ.О**, в том числе поставляемой под прежним названием (до сентября 2025 года) как **Машина виртуализации Скала^р МВ.ДИ**.

Технические характеристики, приведенные в документе — справочные и не могут служить основанием для претензий.

Технические характеристики могут отличаться от приведенных вследствие модификации изделий.

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

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

Перечень терминов и сокращений

Термин, сокращение	Определение
ERP	(англ. Enterprise Resource Planning) — планирование ресурсов предприятия
IaaS	(англ. Infrastructure as a Service, Infrastructure as Code) — 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 развёртывание в противовес развёртыванию с использованием интерактивного взаимодействия и ручного редактирования конфигурационных файлов
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
NFS	(англ. Network File System) — протокол сетевого доступа к файловым системам
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
SSD	(англ. Solid-State Drive) запоминающее устройство на основе микросхем памяти
БД	База данных
ВМ	Виртуальная машина
ГИС	Государственные информационные системы — системы, которые создаются для реализации полномочий государственных органов и обеспечения обмена информацией между ними, а также в иных установленных федеральными законами целях
ЗОКИИ	Значимый объект критической информационной инфраструктуры
ИСПДн	Информационные системы персональных данных. Совокупность информации, содержащейся в базах данных, и обеспечивающих её обработку с использованием информационных технологий и технических средств

Термин, сокращение	**Определение**
Кластер	Отказоустойчивая архитектура функционала Машины
Машина	Автономный масштабируемый модульный программно-аппаратный комплекс (изделие с кодом ОКПД 26.14.20.160 из реестра 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
Модуль	Функционально завершенный комплект сконфигурированного 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. Зарегистрирован в ЕРРРП
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Подсистема	Логическое объединение компонентов по функциональному признаку, с целью пояснения состава и принципов действия ПАК
СХД	Система хранения данных
СУБД	Система управления базами данных
Узел	Вычислительный узел (сервер) или сетевой узел (коммутатор) в составе Модуля, в зависимости от контекста

1. Предисловие

1.1 Описание документа

Настоящий документ дает концептуальный и архитектурный обзоры **Машины динамической инфраструктуры Скала^р МДИ.О** (далее **Скала^р МДИ.О**).

Обзор раскрывает, как оптимизированные программно-аппаратные комплексы **Скала^р** отвечают современным вызовам, и фокусируется на **Машине динамической инфраструктуры Скала^р МДИ.О**.

1.2 Аудитория

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

1.3 Обратная связь

Скала^р и авторы этого документа будут рады обратной связи по нему.

Свяжитесь с командой **Скала^р** по электронной почте info@skala-r.ru.

2. 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 подход «Инфраструктура-как-Код» для создания часто меняющихся или непостоянных сред (например, сред разработки и тестирования) и обеспечить более быстрое и надёжное 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 сверхскоростную сетевую среду и систему интеллектуального управления.

Конструктивно **Скала^р МДИ.О** 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.

Машина динамической инфраструктуры Скала^р МДИ.О обеспечивает:

- высокую производительность — благодаря проработанной интеграции аппаратного и программного обеспечения, оптимизации алгоритмов для используемых технологий, применению широкого спектра методов обеспечения надёжности;
- отказоустойчивость — за счёт применения надёжных комплектующих и специализированного программного обеспечения, резервирования критических компонентов и использования устойчивых сетевых протоколов;
- катастрофоустойчивость — благодаря наличию специальных технологий;
- снижение затрат — за счёт комплексности продукта и специальных условий лицензирования;
- надежную основу для динамической инфраструктуры частного или публичного облака;
- автоматизированное развертывание сред виртуализации, что значительно снижает операционные затраты;
- динамическое управление ресурсами, что повышает гибкость инфраструктуры;
- удобный графический интерфейс администрирования;
- встроенный REST API, провайдер Terraform и модуль Ansible;
- развитую экосистему вендорских и партнерских решений;
- широкий спектр поддерживаемых ОС;
- быстрое масштабирование благодаря модульной платформе;
- встроенные средства мониторинга и управления эксплуатацией.

Машина динамической инфраструктуры Скала^р МДИ.О содержит все необходимые элементы для функционирования высоконагруженной системы на основе платформы

виртуализации Базис 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.

Машина динамической инфраструктуры Скала^р МДИ.О впервые была представлена в 2023 году и активно развивается.

Машины динамической инфраструктуры Скала^р МДИ.О успешно используются в крупных коммерческих, финансовых и государственных организациях.

Программно-аппаратные комплексы **Скала^р** включены в Единый реестр российской радиоэлектронной продукции и реестр российской промышленной продукции Минпромторга и работают на ПО, включённом в реестр Минцифры РФ.

3. Отличительные черты

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

Высокая доступность

- Механизмы распределения нагрузки;
- Система мониторинга и анализа состояния **Машины** собственной разработки **Скала^р**;
- Система хранения данных (СХД) с двумя контролерами, работающими в режиме symmetric active-active, что обеспечивает высокую доступность данных и низкое время переключения путей доступа;
- Защита от отказа единичных аппаратных компонентов, установленных в физические серверы (жёсткие 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

- Надёжные 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;
- 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 развёртывании

- Оптимальность настроек подтверждена значительным количеством установок;
- Автоматизированное развёртывание снижает риск человеческой ошибки;
- Стандартизация развёртывания гарантирует соответствие продукта заявленным характеристикам.

Непрерывный контроль состояния Машины

- 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;
- Сокращённые сроки ввода в эксплуатацию;
- Только обоснованно необходимые компоненты.

Альтернатива VMware и Microsoft

- Полностью российское решение;
- Отлаженные инструменты и процессы миграции;
- Высокие надёжность и производительность;
- Качество, подтверждённое опытом практического применения.

4. Подтвержденная безопасность

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

ОС может применяться для защиты информации:

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

ОС 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 сертифицированным средством виртуализации **Базис Virtual Security** (сертификат ФСТЭК 4348 от 24.12.2020, действует до 24.12.2025).

Базис Virtual Security может применяться для защиты информации:

- 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-ой категории значимости;
- в информационных системах общего пользования 2 класса.

Базис Virtual Security соответствует требованиям следующих нормативных документов:

- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11.02.2013 г. №17 с изменениями, внесенными приказом ФСТЭК России от 15.02.2017 г. № 27 и приказом ФСТЭК России от 28.05.2019 г. №106;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» введенным в действие приказом ФСТЭК России

№21 от 18.02.2013 г. с изменениями, внесенными приказом ФСТЭК России от 23.03.2017 г. №49 и приказом ФСТЭК России от 14.05.2020 г. №68;

- «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», введенным в действие приказом ФСТЭК России № 239 от 25.12.2017 г. с изменениями, внесенными приказом ФСТЭК России от 09.08.2018 г. №138, приказом ФСТЭК России от 26.03.2019 г. №60 и приказом ФСТЭК России от 20.02.2020 г. №35;
- «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», утвержденным приказом ФСТЭК России от 14.03.2014 г. №31 с изменениями, внесенными приказом ФСТЭК России от 23.03.2017 г. №49, приказом ФСТЭК России от 09.08.2018 г. №138 и приказом ФСТЭК России от 15.03.2021 г. №46;
- «Требования по защите информации, содержащейся в информационных системах общего пользования», введенным в действие приказом ФСТЭК России №489 от 31.08.2010 г.

- *Протестирована совместимость с наложенными средствами защиты*

Машина динамической инфраструктуры Скала^р МДИ.О использует антивирусное средство защиты **«Kaspersky Security для виртуальных сред 5.2 Легкий агент»** (сертификат ФСТЭК 3883 от 14.02.2018, действует до 14.02.2026), 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.САВ3.Б4.П3» (ФСТЭК России, 2012);
- «Профиль защиты средств антивирусной защиты тина В четвертого класса защиты. ИТ.САВ3.В4.П3» (ФСТЭК России, 2012).

Сертифицированное антивирусное средство защиты **Kaspersky Endpoint Security для Linux** (сертификат ФСТЭК 2534 от 27.12.2011, действует до 27.12.2025) 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 Б 2 класса защиты. ИТ.САВ3.Б2.13» (ФСТЭК России, 2012);
- «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВ3.В2.П3» (ФСТЭК России, 2012);
- «Профиль защиты средств антивирусной защиты типа Г второго класса защиты»

- При помощи 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.

5. Принципы создания Машины

Машина динамической инфраструктуры Скала^р МДИ.О создана для работы с 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 виртуальными серверами с разнородной нагрузкой. В **Машине** использованы преимущества тонкой настройки всех компонентов под функции и потребности конкретного ПО и тем самым обеспечен максимум её 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 счёт быстрого развёртывания инфраструктуры и готовым инструментам для управления виртуальным дата-центром и сетевыми функциями;
- быстродействие — за счёт блочного хранения с настраиваемой производительностью и интеграционным модулям к инструментам CI/CD и DevOps;
- эффективность — за счёт авторизации и аутентификации через отдельный брокер безопасности, а также полнофункционального REST API;
- управление и адаптацию — за счёт 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 трёх 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 **Машины динамической инфраструктуры Скала^р МДИ.О**:

- операционная система;
- ПО Basis Dynamix Enterprise;
- ПО **Скала^р Геном**.

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

Практическое применение тиражируемых экземпляров **Машин динамической инфраструктуры 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 её применения. Заказчик получает **Машину динамической инфраструктуры Скала^р МДИ.О**, 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 ведётся 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, развёртывании и настройке компонентов в случае традиционного подхода.

6. 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 её назначением. Модуль является единым и неделимым элементом спецификации 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.

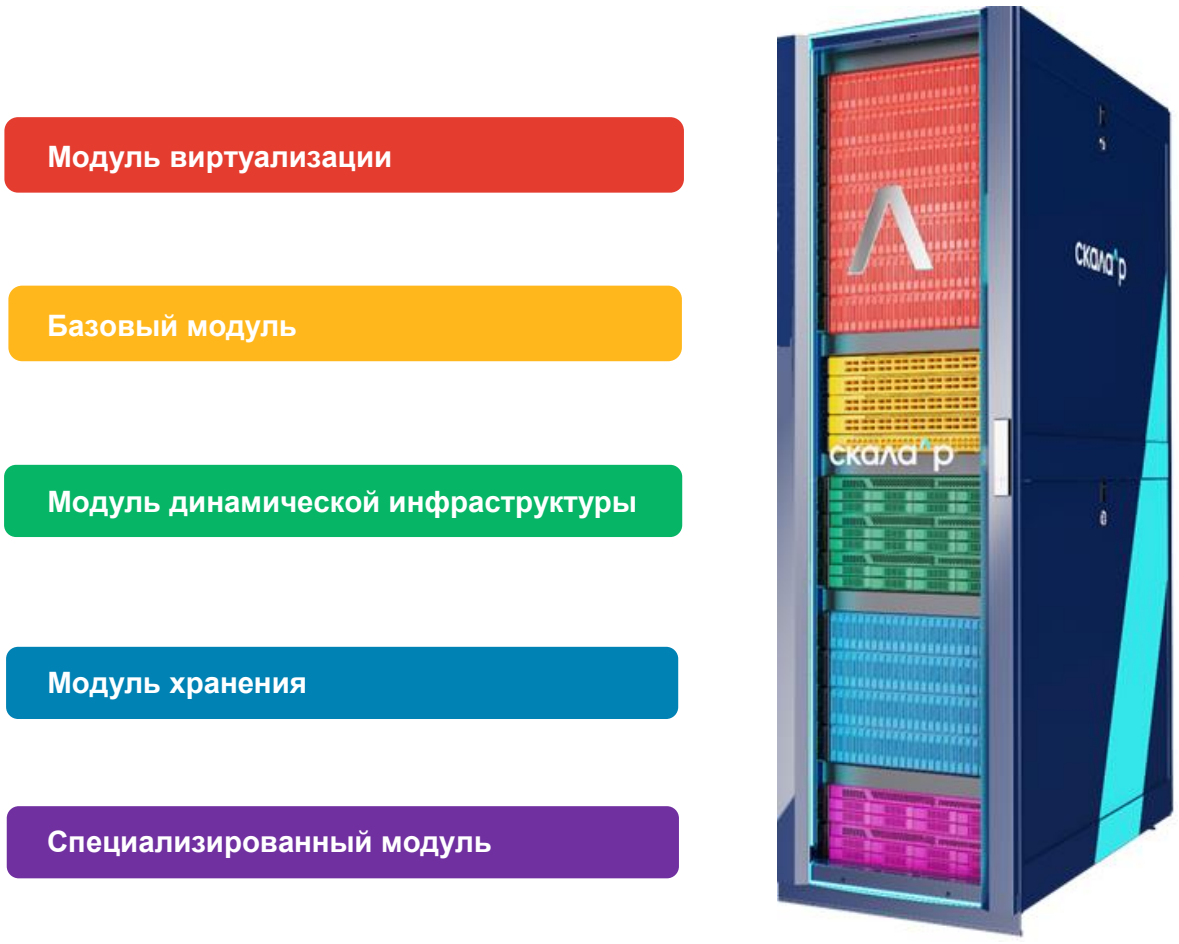

Рисунок 1. Машина динамической инфраструктуры Скала^р МДИ.О

Комплекты поставки

Машины динамической инфраструктуры 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 ёмкости, или есть необходимость увеличить производительность и объём 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**.

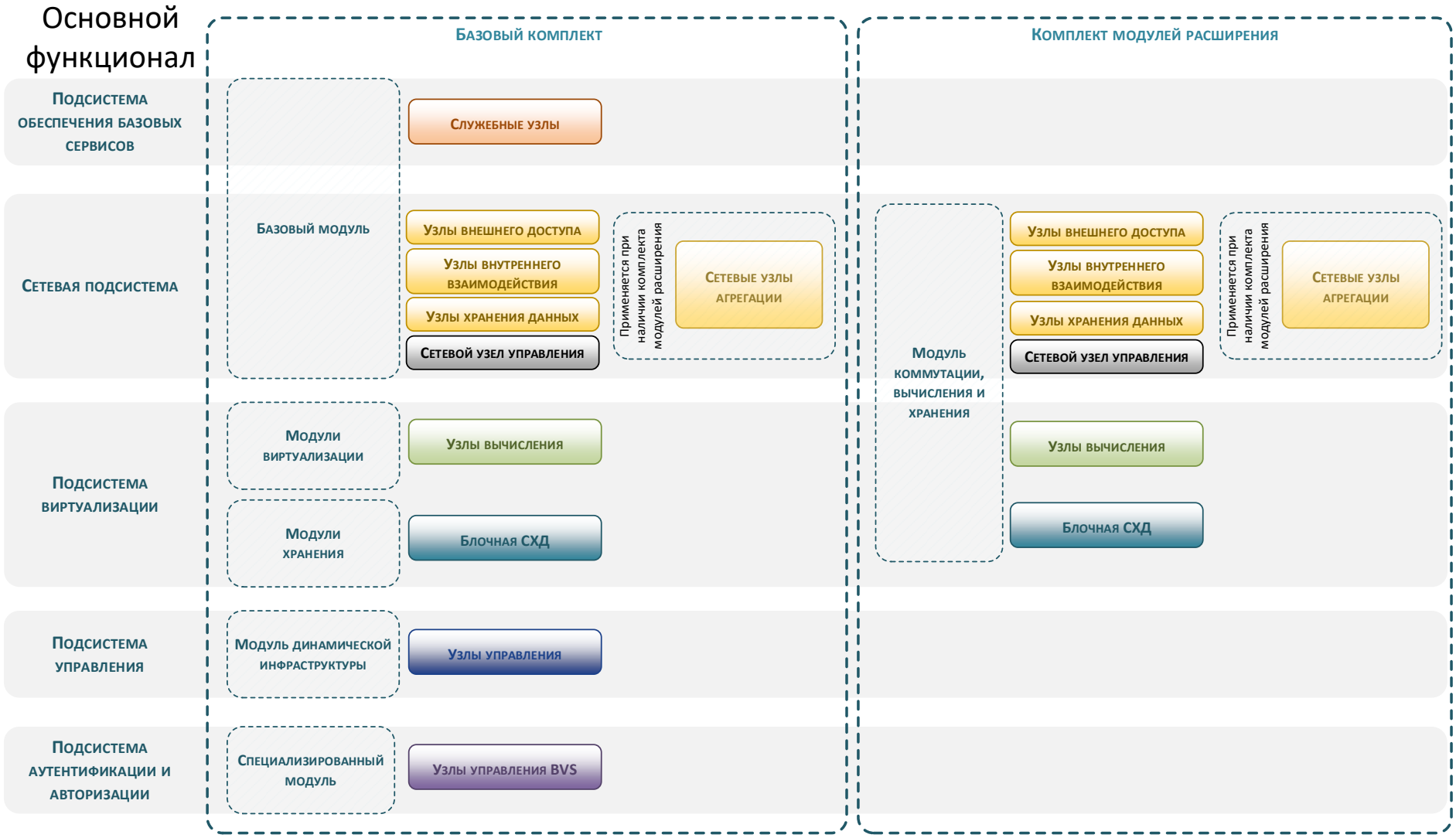

Рисунок 2. Комплектация Машины динамической инфраструктуры Скала^р МДИ.О

6.1 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 динамической инфраструктуры Скала^р МДИ.О** для выполнения задач прямого назначения.

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

6.1.1 Подсистема обеспечения базовых сервисов

Подсистема обеспечения базовых сервисов отвечает за мониторинг и управление аппаратными и программными компонентами **Машины динамической инфраструктуры Скала^р МДИ.О**. В неё 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. 6.2.1).

6.1.2 Сетевая подсистема

Сетевая подсистема выполняет функций организации сетевой связанности между всеми вычислительными узлами, входящими в состав **Машины динамической инфраструктуры Скала^р МДИ.О,** 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;
- 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 и передачи сервисной информации в подсистему обеспечения базовых сервисов.

Стартовый комплект сетевых узлов всегда размещается в **Базовом модуле** (см. 6.2.1).

6.1.3 Подсистема виртуализации

Выполняет основные функции, связанные с функционирование системы динамической инфраструктуры, формируют вычислительные мощности для системы виртуализации и

хранение данных. Отвечает за предоставление вычислительных ресурсов системе в рамках виртуальной инфраструктуры.

Подсистема реализуется **Модулем виртуализации** (см. 6.2.3).

6.1.4 Подсистема хранения

Выполняет основные функции, связанные с функционирование системы динамической инфраструктуры, обеспечивает хранение данных. Отвечает за хранение данных (образов виртуальных машин, шаблонов).

Подсистема реализуется **Модулем хранения** (см. 6.2.4).

6.1.5 Подсистема управления

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

- 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. 6.2.2).

6.1.6 Подсистема аутентификации и авторизации

Подсистема аутентификации и авторизации 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. Отвечает за:

- идентификация, аутентификация и авторизация пользователей в средстве виртуализации;
- доверенную загрузку 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.

Подсистема реализуется **Специализированным модулем** (см. 6.2.5).

6.2 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 динамической инфраструктуры;

- Модуля коммутации, вычисления и хранения (необходим для расширения);
- Модуля виртуализации;
- Модуля хранения;
- Специализированного модуля.

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

6.2.1 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 сетевых узла 100 Гбит/с для организации внутреннего сетевого взаимодействия;
- 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.

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 - Аванпост FAM (опция).

На служебных узлах базового модуля предустановлено сервисное ПО **Скала^р**, 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.

6.2.2 Модуль динамической инфраструктуры

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

Осуществляет управление узлами вычисления и хранения.

Назначение

- управления 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 Базис Dynamix Enterprise.

Отказоустойчивость обеспечена

- выделением трёх физических вычислительных узлов;
- средствами Kubernetes;
- технологией RAID для дисков вычислительных узлов.

Применяемое программное обеспечение

- ОС Astra Linux 1.8;
- Базис Dynamix Enterprise;
- Агенты мониторинга программной платформы **Скала^р Геном**.

6.2.3 Модуль виртуализации

Название в Едином реестре российской радиоэлектронной продукции — СКАЛА-Р Модуль виртуализации. Обеспечивает функционирование системы динамической инфраструктуры, формируют вычислительные мощности для системы виртуализации. Вычислительные узлы объединяются в единый кластер вычисления.
Кластер вычисления имеет возможность масштабирования количества узлов и изменение конфигурации узлов. Может включать до 180 вычислительных узлов.

Назначение

- предоставление вычислительных ресурсов системе в рамках виртуальной инфраструктуры.

Узлы

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

Отказоустойчивость обеспечена

- резервирования критических компонентов;
- использования устойчивых сетевых протоколов;
- ОС узлов разворачиваются на аппаратном RAID 1 – отказоустойчивом дисковом массиве из двух дисков;
- многоуровневое тестирование.

Применяемое программное обеспечение

- ОС Astra Linux 1.8;
- QEMU/KVM;
- Агенты мониторинга программной платформы **Скала^р Геном**;
- Агенты BVS (опционально).

6.2.4 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.Unifield Gen2.

6.2.5 Специализированный модуль

Название в Едином реестре российской радиоэлектронной продукции — СКАЛА-Р Специализированный модуль. 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.

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 трёхузлового кластера с ОС Astra Linux 1.8 на базе программного продукта **Базис Virtual Security**.

Отказоустойчивость обеспечена

- Выделением трёх физических вычислительных узлов;
- Технологией RAID для дисков вычислительных узлов.

Применяемое программное обеспечение

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

7. Архитектура Скала^р МДИ.О

Основные компоненты **Машины динамической инфраструктуры Скала^р МДИ.О** и их взаимодействие представлены на схеме (Рисунок 3).

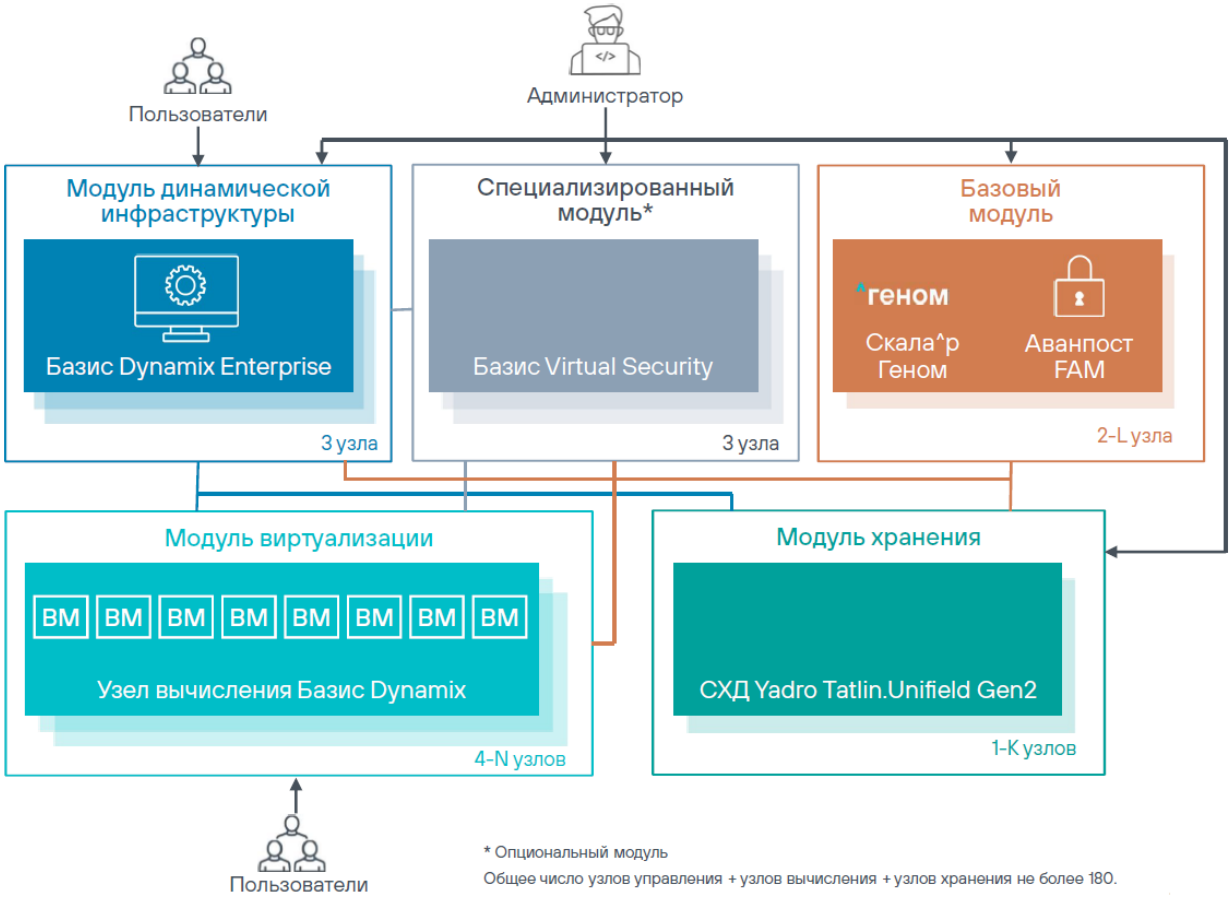

Рисунок 3. Общая архитектура Машины динамической инфраструктуры Скала^р МДИ.О

7.1 Назначение и характеристики кластера управления

Кластер управления – представляет собой выделенный кластер управления высокой доступности, развернутый на трёх узлах (контроллерах). Он обеспечивает отказоустойчивый режим работы всех функциональных сервисов платформы IaaS/IaC, различных интерфейсов доступа и управления, а также дополнительных инфраструктурных сервисов платформы виртуализации. Осуществляет управление узлами вычисления и хранения.

Кластер построен на узлах с ОС Astra Linux 1.8 на базе Kubernetes с установленным программным продуктом Базис Dynamix Enterprise (Рисунок 4) 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.

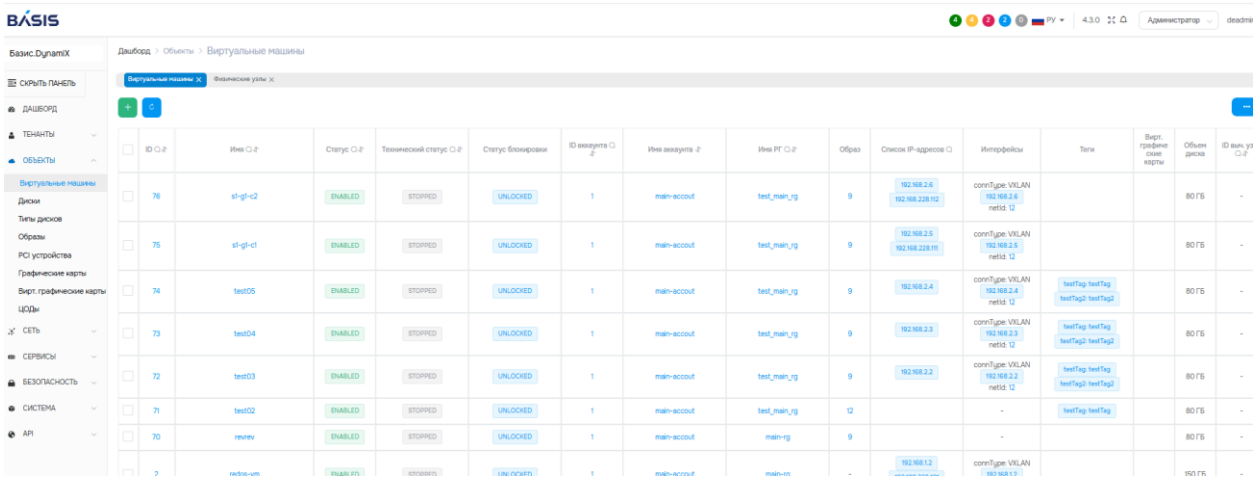

Рисунок 4. Пример интерфейса ПО Базис Dynamix Enterprise

7.2 Назначение и характеристики кластера вычисления

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 изменение конфигурации узлов. Может включать до **180** вычислительных узлов.

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

7.3 Назначение и характеристики узла хранения

Узел хранения – обеспечивает хранения данных системы динамической инфраструктуры **Скала^р МДИ.О**, построен на базе систем хранения данных Yadro Tatlin.Unifield 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.

Клонирование дисков функциональность томов с косвенной адресацией — это клоны. Снапшоты не поддерживают операции ввода-вывода, но от снапшота можно создавать клоны. Как и снапшот, клон создается мгновенно 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. Зависимости между клоном и родительским снапшотом нет: после создания клона снапшот вполне можно удалить. Клон также может иметь снапшоты, для которых, в свою очередь, можно создавать другие клоны.

Тонкие диски для СХД Tatlin.Unifield Gen2 в текущем релизе не поддерживаются.

Масштабируемость узла хранения рассчитывается исходя из потребностей Заказчика (на 20 вычислительных узлов необходима 1 СХД Tatlin.Unifield Gen2).

7.4 Назначение и характеристики служебного узла

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 **Аванпост 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).

Состоит из двух вычислительных узлов, объединенных в зеркальный кластер для выполнения служебных функций. Логическая схема работы сервисных узлов представлена на рисунке 5.

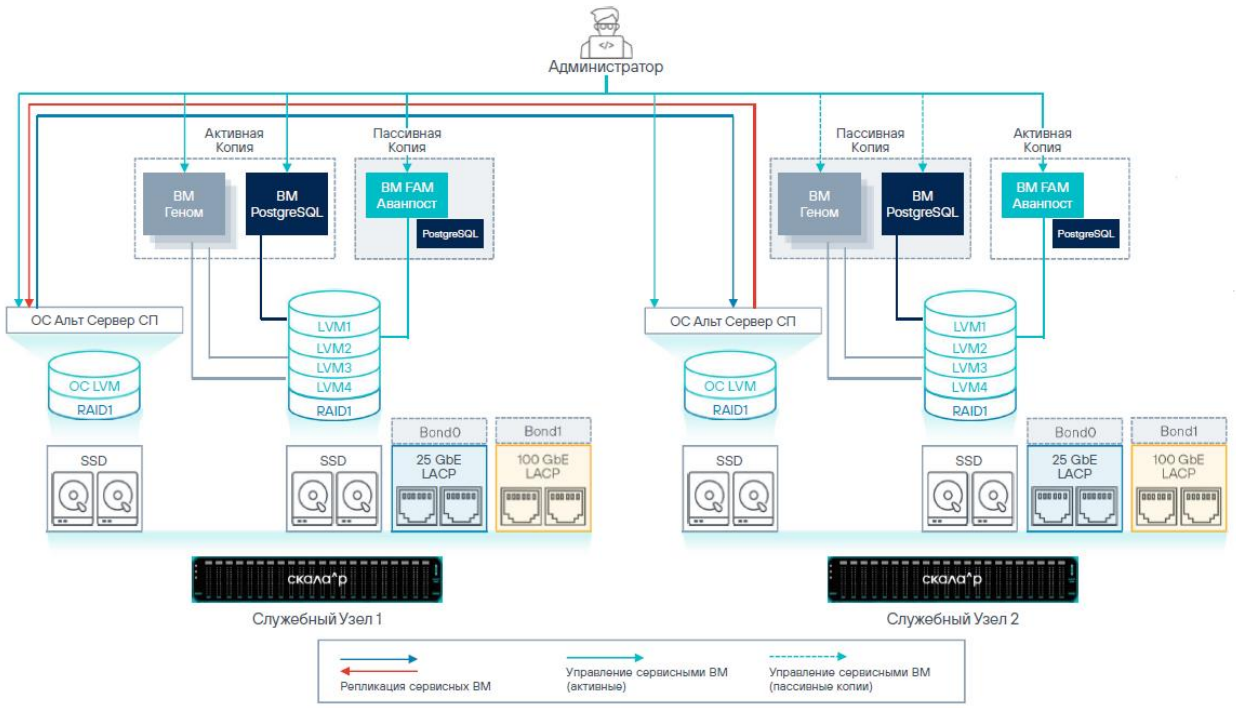

Рисунок 5. Логическая схема работы служебных (сервисных) узлов

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 Аванпост 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 сервисной машине 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 идёт 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) узла и вторичного (secondary). 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.

7.4.1 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, обладает 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 СУБД.

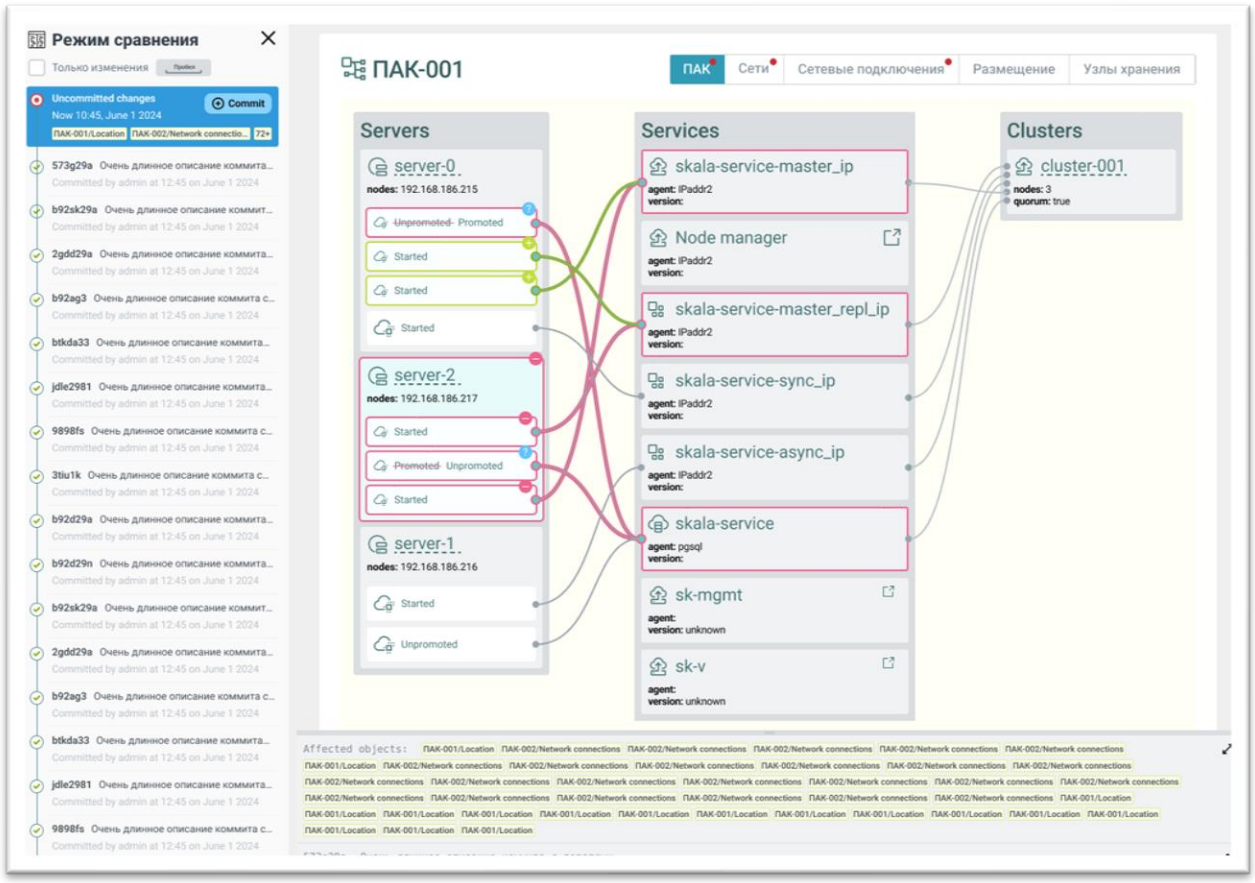

Рисунок 6. Пример интерфейса ПО Скала^р Геном (отображение схемы подключений узлов ПАК)

ПО **Скала^р Геном** позволяет проводить настройку появлении новых критических уведомлений, условия их получения гибко настраиваются в соответствии с текущими потребностями (Рисунок 7). Возможно управлять формированием почтовых уведомлений: регулировать их группировку, частоту отправки и т.д.

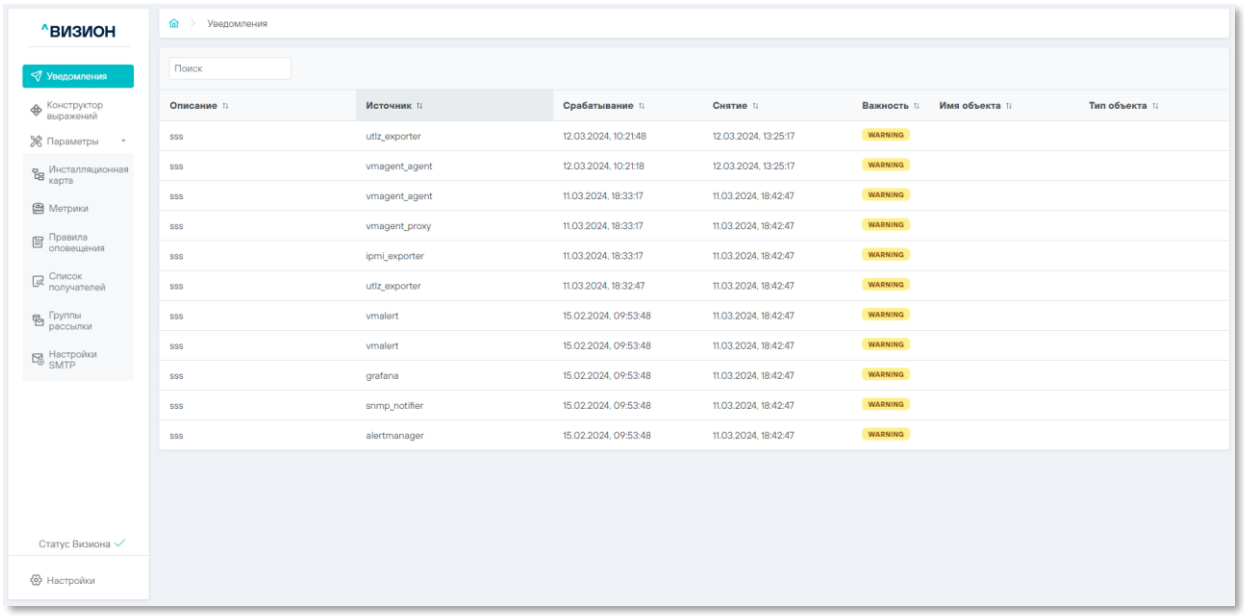

Рисунок 7. Пример интерфейса ПО Скала^р Геном
(пример окна настройки уведомлений мониторинга)

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 8).

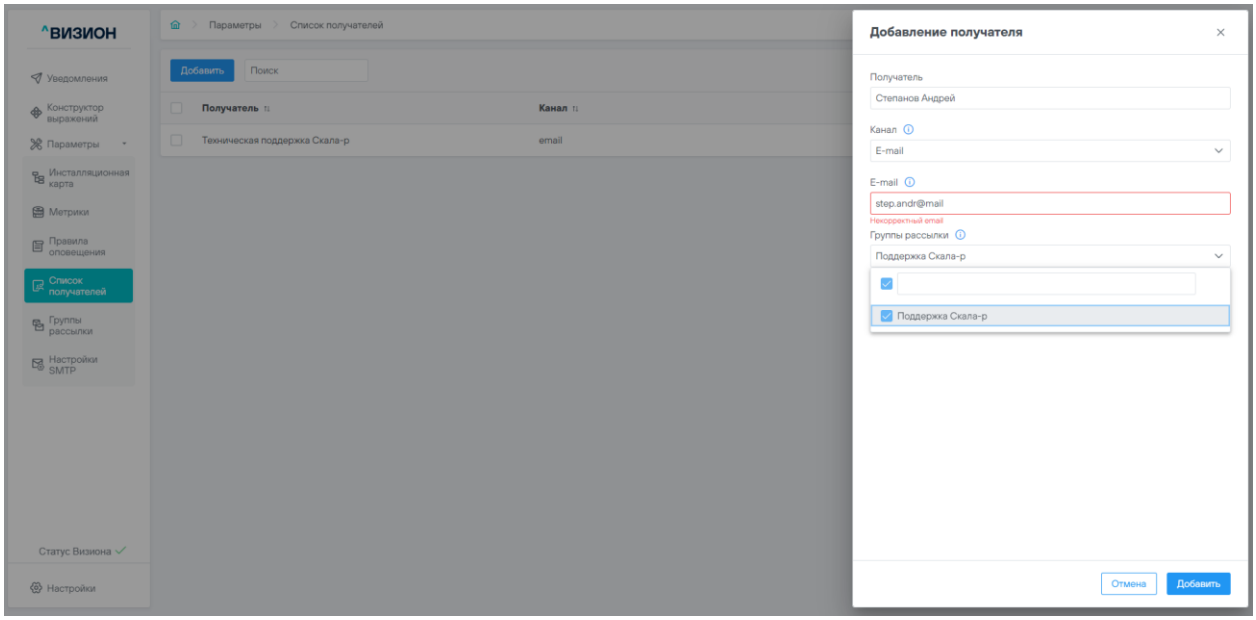

Рисунок 8. Пример интерфейса ПО Скала^р Геном (настройка пересылки сообщений)

Архитектурно, программная платформа **Скала^р Геном** состоит из следующих сервисных виртуальных машин, вместе образующие программную платформу обслуживания, управления и мониторинга **Скала^р Геном** (Рисунок 9): ВМ Платформы (сервер управления), ВМ Топологии (сервер топологии, CMDB) и ВМ Мониторинга (Визион).

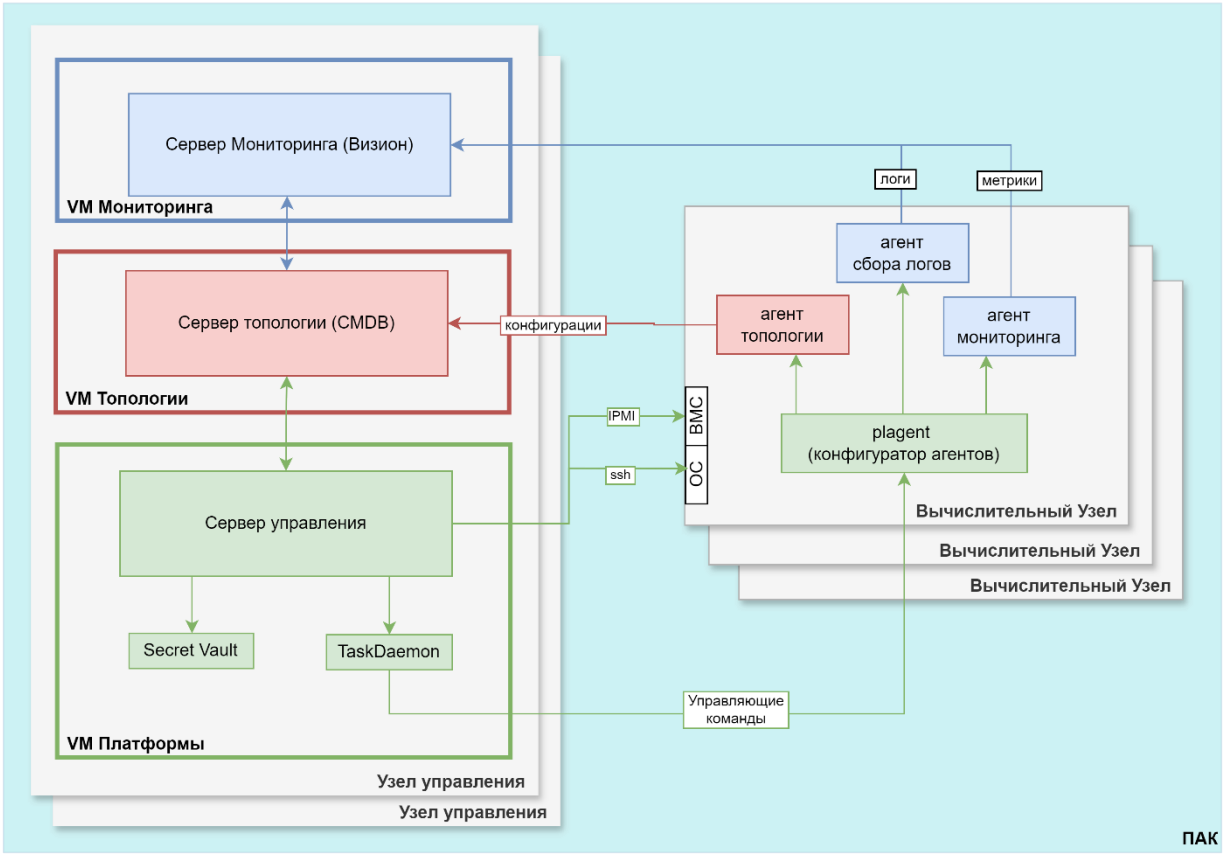

Рисунок 9. Основные компоненты программной платформы Скала^р Геном

Программная платформа **Скала^р Геном** может быть развернута как в режиме, обеспечивающем обслуживание одного ПАК (Рисунок 9), так и в режиме централизованного управления несколькими ПАК, обеспечивающим управление инфраструктурой, состоящей из множества ПАК СКАЛА-Р (Рисунок 10). 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.

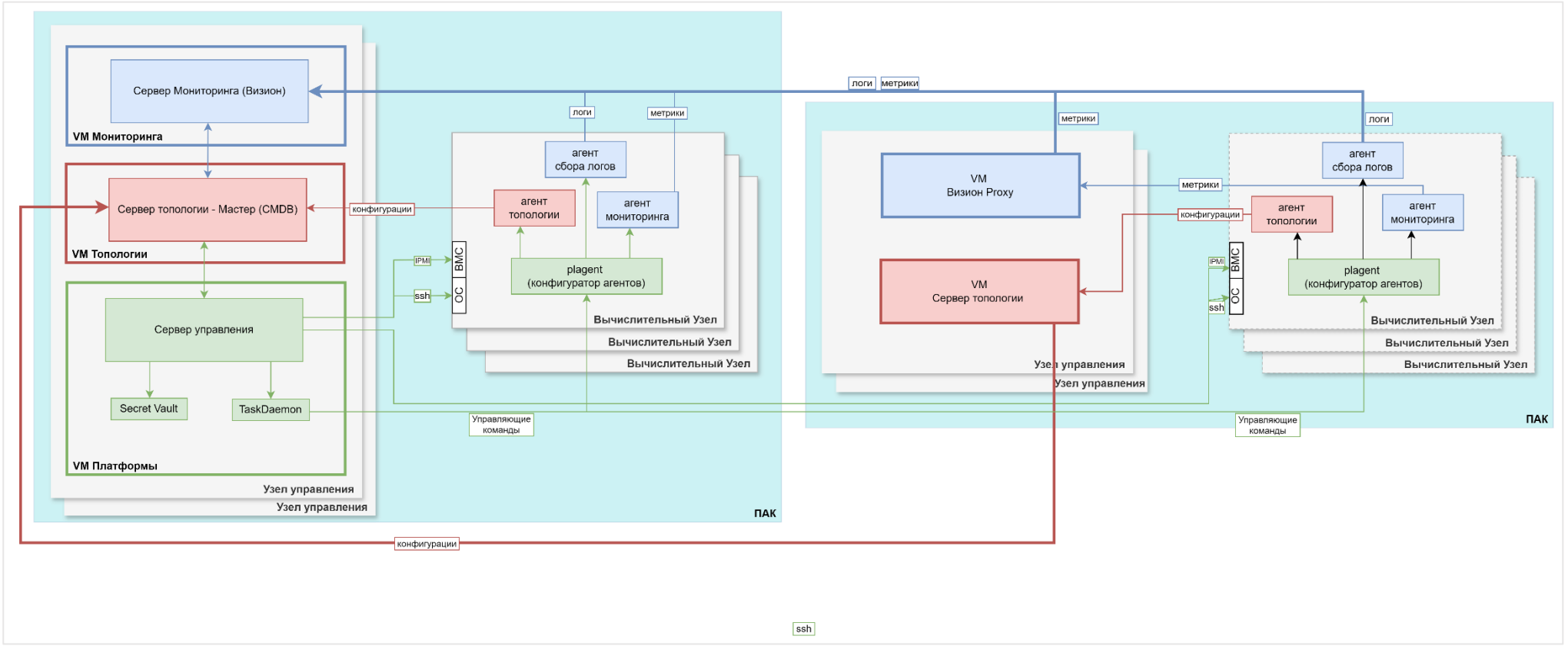

Рисунок 10. Программная платформа Скала^р Геном в режиме централизованного управления несколькими ПАК

7.5 Назначение и характеристики узлов управления BVS

Узлы управления BVS – 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 трёх вычислительных узлов с ОС Astra Linux 1.8 на базе программного продукта Базис Virtual Security (BVS).

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 Базис Virtual Security представлена ниже (Рисунок 11).

Базис Virtual Security состоит из подсистем:

1. Подсистема проксирования реализованной на прокси-сервере NGINX, с помощью которого реализуется проксирование запросов до сервисов Базис Virtual Security и реализуется поддержка TLS;
2. Подсистема балансировки нагрузки состоит из сервиса балансировки нагрузки basis-vbalancer, который реализует распределение запросов между нескольким узлами кластера управления программного модуля Базис Virtual Security;
3. Подсистема авторизации состоит из:
    a. virtual-security-admin – основной компонент, который реализовывает бизнес-логику, обеспечивает интеграцию между подсистемами программного модуля и предоставляет API;
    b. virtual-security-web – программный компонент, который предоставляет графический интерфейс администратору для централизованного управления программным модулем и различными функциями безопасности, которые данный программный модуль реализует;
    c. 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;
    d. virtual-security-proxy – сервис проксирования (интеграционный шлюз), который отвечает за управление доступом к API-интерфейсам защищаемых информационных и автоматизированных систем;
    e. 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 учётных записей пользователей;

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

4. Подсистема СУБД реализовано на PostgreSQL как объектно-реляционная система управления базами данных;
5. Подсистема взаимодействия с агентами реализована 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.

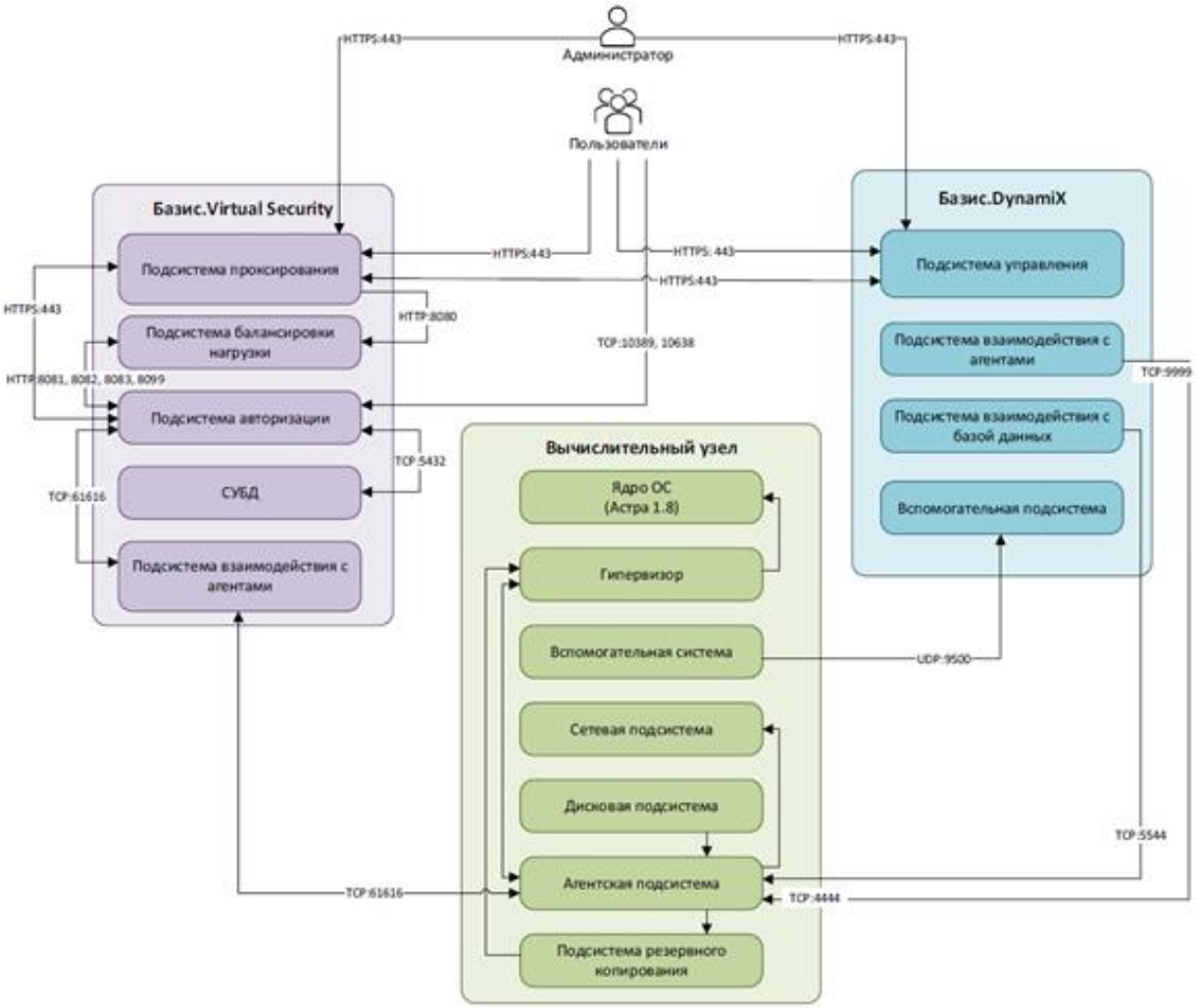

Рисунок 11. Схема взаимодействия компонентов Базис Virtual Security

7.6 Сетевое взаимодействие

Взаимодействие компонентов осуществляется через:

- сетевой узел управления;
- сетевой узел внутреннего взаимодействия;

- сетевой узел внешнего доступа;
- сетевой узел хранения данных.

Схема взаимодействия между компонентами **Скала^р МДИ.О** приведена на рисунке (Рисунок 12).

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 – **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).

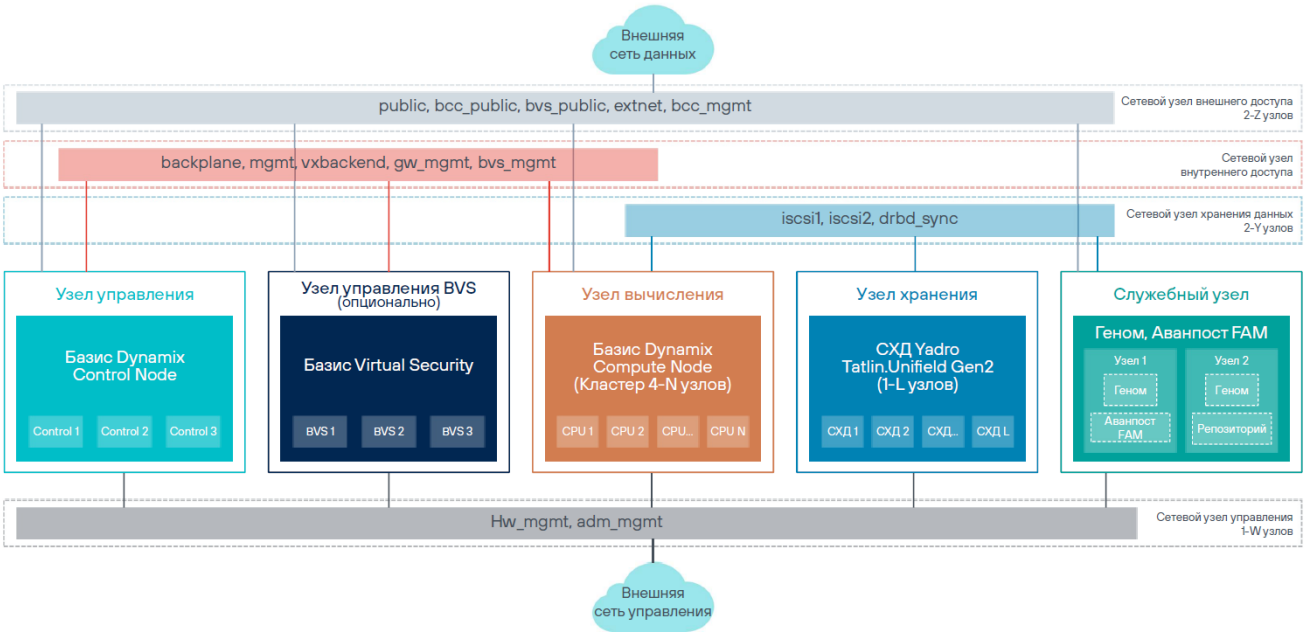

Рисунок 12. Схема взаимодействия узлов Машины динамической инфраструктуры Скала^р МДИ.О

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);
- управления Basis Cloud Control – **bcc_mgmt** (опционально);
- доступа к WEB интерфейсу Базис 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**.

8. Специфичные черты

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

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

Эффект:

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

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

Эффект:

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

9. Гарантированное качество

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

Производство (комплектование и развёртывание ПО)

- При производстве используются высококачественные комплектующие;
- Сборка продукции осуществляется строго в соответствии с утверждённым планом размещения компонентов;
- Развертывание и первичная конфигурация **Машины** осуществляются в автоматическом режиме;
- Дополнительные настройки ПО осуществляются в соответствии с утверждённой методикой и пошаговой инструкцией;
- Осуществляется функциональное тестирование сформированной **Машины**;
- При необходимости возможны индивидуальные конфигурации **Машины динамической инфраструктуры Скала^р МДИ.О**.

Передача в эксплуатацию

- **Машина динамической инфраструктуры Скала^р МДИ.О** полностью сформирована, протестирована, готова к размещению в сети Заказчика и подключению прикладного ПО;
- В комплекте с **Машиной** передаются паспорт и сертификат на поддержку;
- Передаётся комплект документации, необходимый контролирующим организациям для аттестации **Машины динамической инфраструктуры Скала^р МДИ.О** в контуре Заказчика;
- По запросу проводится обучение специалистов Заказчика работе с **Машиной динамической инфраструктуры Скала^р МДИ.О.**

Поддержка

- **Машина динамической инфраструктуры 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 партнёром **Скала^р**;
- У Заказчика есть 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 **Машины динамической инфраструктуры Скала^р МДИ.О**.

Сопровождение

По запросу возможна реализация дополнительных требований по модернизации или развитию **Машины динамической инфраструктуры Скала^р МДИ.О**, 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 поставлена 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 развёртывании будут выполнены настройки сетевых адресов в соответствии со структурой сети Заказчика. Заказчик должен предоставить необходимые данные в соответствии с номенклатурой компонентов **Машины динамической инфраструктуры Скала^р МДИ.О**.

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

Дальнейшие мероприятия по вводу в эксплуатацию осуществляются Заказчиком путём настройки прикладных программных систем.

11. Техническая поддержка

Поставка **Машин 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 **Машин динамической инфраструктуры Скала^р МДИ.О** представлен в таблице 1.

Таблица 1 — 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	+	+
Расширенные параметры обслуживания	—	+

Услуги	Пакет «9×5»	Пакет «24×7»
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. Лицензирование ПО в составе модулей

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**:

- Базис Dynamix Enterprise;
- Базис 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/Аванпост FAM – на служебных узлах базового модуля);
- среда разработки и исполнения BellSoft Java Axiom JDK Certified server или аналог (для BVS).

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 таблице 2.

Таблица 2 — Версии ПО, описанного в настоящем техническом обзоре

Название ПО	Версия ПО
ОС «Astra Linux Special Edition»	1.8.1
ОС «Альт СП» (на служебных узлах базового модуля)	c10f2
Базис Dynamix Enterprise	4.3
Базис Virtual Security (опция)	3.4
Среда разработки и исполнения BellSoft Java Axiom JDK Certified server (для BVS)	17.0.12+10
Программная платформа Скала^р Геном	1.18.1

13. О Компании

Скала^р — модульная платформа для построения высоконагруженной ИТ-инфраструктуры (продукт Группы Rubytech). Лидер российского рынка ПАК (по версии CNews Analytics, 2024).

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.