скала^р

Машина управления технологическими процессами Скала^р МСП.ТП

Модульная платформа для промышленной автоматизации и задач АСУ ТП

Технический обзор

Релиз МСП.ТП 2026

версия 1.1 от 29.07.2026

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

ОГЛАВЛЕНИЕ

Перечень терминов и сокращений 4
1 Предисловие 10
2 Введение 11
3 Отличительные черты 13
4 Подтвержденная безопасность 16
4.1 Операционные системы 16
4.2 Гипервизор и хранилище 16
4.3 Средства защиты 17
5 Сценарии использования 19
6 Принципы создания Машины 23
7 Варианты исполнения Машины 26
8 Состав Машины 27
8.1 Подсистемы Машины 28
8.2 Модули Машины 29
9 Архитектура Машины 33
9.1 Кластер управления (HA) 34
9.2 Кластер вычисления 34
9.3 Виртуальные машины служебных компонентов 35
9.4 Сетевое взаимодействие 35
10 Программные компоненты 38
10.1 Размещение программных компонентов 38
10.2 Basis vControl 40
10.3 Basis Workplace 43
10.4 Программная платформа Скала^р Геном 43
10.5 Р-Виртуализация 45
10.6 Р-Хранилище 45
11 Высокая доступность и защита данных 46
11.1 Кластер высокой доступности 46
11.2 Высокая доступность данных программно-определяемого хранилища 46
12 Поставка и лицензирование ПО в составе Машины 49
13 Гарантированное качество 51

14 Требования к размещению 52
15 Техническая поддержка 53
О Компании 55

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Термин, сокращение	Определение
API	(англ. Application Programming Interface) Интерфейс программирования приложений
APT-атака	(англ. Advanced Persistent Threat) Долгосрочная, целенаправленная кибератака, в которой злоумышленники методично проникают в систему, закрепляются в ней и ведут скрытую деятельность
Avanpost FAM (Federated Access Manager)	ПО для единой аутентификации сотрудников в корпоративных ресурсах организации
BACnet	(англ. Building Automation and Control network) Открытый сетевой протокол передачи данных, разработанный для систем автоматизации зданий и управления инженерными сетями
CentOS	(англ. Community Enterprise Operating System) Серверная операционная система семейства Linux с открытым кодом
ClickHouse	Колоночная аналитическая система управления базами данных с открытым исходным кодом, предназначенная для быстрой обработки аналитических запросов на больших объёмах данных в режиме реального времени
ClickHouse Keeper	Сервис координации, разработанный специально для кластеров ClickHouse
CloudLinux	Специализированный зарубежный коммерческий дистрибутив Linux, разработанный для сред совместного (виртуального) хостинга
CMDB	(англ. Configuration Management Database) Централизованный репозиторий, который хранит информацию о компонентах ИТ-инфраструктуры и их взаимосвязях
DCS	(англ. Distributed Control System) Компьютеризированная система управления технологическим процессом или установкой, в которой функции управления распределены по нескольким узлам или контроллерам, распределённым по всей системе
DDoS-атака	(англ. Distributed Denial of Service) Попытка вывести из строя сервис, массово отправляя на него запросы с множества устройств
Debian	Операционная система (дистрибутив Linux) с открытым исходным кодом
DPI	(англ. Deep Packet Inspection) Технология анализа сетевого трафика, которая позволяет детально изучать содержимое сетевых пакетов, включая их структуру, поведение и признаки приложений

Термин, сокращение	Определение
Erasure Coding	Технология в области информационных технологий, которая обеспечивает отказоустойчивость хранения данных за счет делением блоков информации на фрагменты с добавлением вычисляемых контрольных сумм (как правило, по алгоритму Рида-Соломона) и разнесением их на различные носители.
EtherNet/IP	(англ. Ethernet Industrial Protocol) Стандартный протокол связи в промышленных сетях
ERP	(англ. Enterprise Resource Planning) Система управления ресурсами предприятия
FINS	(англ. Factory Interface Network Service) Проприетарный сетевой протокол, разработанный японской компанией Omron для промышленной автоматизации
GUI	(англ. Graphical User Interface) Графический пользовательский интерфейс, способ взаимодействия человека с компьютерной системой или приложением через визуальные элементы
HA	(англ. High Availability) Свойство ИТ-систем оставаться работоспособными даже при отказе отдельных компонентов инфраструктуры
IAM	(англ. Identity and Access Management) Управление идентификацией и контролем доступа — совокупность технологий, операций, методов и политик для управления доступом пользователей к инфраструктуре
ICMP	(англ. Internet Control Message Protocol) Сетевой протокол, который используется для передачи диагностических и управляющих сообщений в сетях на основе TCP/IP
IEC 61850 MMS	Протокол передачи данных, определённый в международном стандарте IEC 61850
IEC 60870-5-104 Client, Server	Стандарт, который определяет протоколы для телеуправления и сбора данных в электротехнике и энергетике, особенно в системах SCADA
IP CIP	Объектно-ориентированный коммуникационный протокол, разработанный для промышленной автоматизации
IPMI	(англ. Intelligent Platform Management Interface) Стандартизированный интерфейс для удалённого управления и мониторинга серверного оборудования на аппаратном уровне
iSCSI	(англ. Internet Small Computer System Interface) Сетевой протокол, который позволяет передавать команды SCSI через IP сети
ISIM, PT ISIM	(англ. Integrated Security Incident Manager, SIM) Программно-аппаратный комплекс для защиты промышленных инфраструктур (АСУ ТП) от киберугроз, разработанный компанией Positive Technologies.
KVM	(англ. Kernel-based Virtual Machine) Гипервизор уровня ядра Linux, который позволяет создавать виртуальные машины и управлять ими

Термин, сокращение	Определение
LFF	(англ. Large Form Factor) Тип жёстких дисков, используемых в серверах и системах хранения данных для хранения данных
LTS	(англ. Long-Term Support) Модель выпуска программного обеспечения, при которой определённые версии получают расширенный период поддержки по сравнению со стандартными релизами
MES	(англ. Manufacturing Execution System) Система управления производственными процессами. Специализированное прикладное программное обеспечение, предназначенное для решения задач синхронизации, координации, анализа и оптимизации выпуска продукции в рамках какого-либо производства.
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
Modbus RTU	Разновидность промышленного протокола для обмена данными между устройствами автоматизации
Modbus RTU Over TCP/IP	Гибридный вариант протокола Modbus, который объединяет преимущества Modbus RTU (двоичный формат данных, компактность, эффективность передачи) и возможности TCP/IP для работы в сетях Ethernet
Modbus TCP/IP	Расширение протокола Modbus, предназначенное для работы в сетях Ethernet с использованием стека протоколов TCP/IP
MQTT	(англ. Message Queuing Telemetry Transport) Лёгкий сетевой протокол обмена сообщениями, разработанный специально для интернета вещей
NL-SAS	(англ. Near Line SAS) Гибридный тип жёстких дисков, который сочетает в себе характеристики SATA-дисков и интерфейс SAS
OEE	(англ. Overall Equipment Effectiveness) Система анализа общей эффективности работы оборудования
OEM-соглашение	(англ. Original Equipment Manufacturer agreement) Юридический договор между производителем (OEM-производителем) и компанией-заказчиком, который использует продукцию производителя для создания собственных продуктов, продаваемых под своим брендом
OPC AE	(англ. Open Platform Communications Alarms & Events) Стандарт в рамках семейства OPC, который предназначен для обмена данными о сигналах тревоги и событиях между промышленными системами управления и корпоративными приложениями
OPC DA	(англ. Open Platform Communications Data Access) Стандарт из семейства OPC, который используется в промышленной автоматизации для обмена данными в реальном времени между различными устройствами и программными приложениями
OPC HDA	(англ. Open Platform Communications Historical Data Access) Стандарт в рамках семейства технологий OPC

Термин, сокращение	Определение
OPC UA	(англ. Open Platform Communications Unified Architecture) Открытый кроссплатформенный стандарт для безопасного и надёжного обмена данными в промышленной автоматизации
PT NGFW	(англ. Next-Generation Firewall) Межсетевой экран нового поколения, разработанный российской компанией Positive Technologies
QEMU	Инструмент с открытым исходным кодом для эмуляции аппаратного обеспечения и виртуализации
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
RAID1	Массив из двух дисков, являющихся полными копиями друг друга и являющийся одним из уровней технологии RAID
RAM	(англ. Random Access Memory) Временное хранилище данных, которое обеспечивает быстрый доступ к информации для процессора
RAW	Формат данных, который содержит необработанные (или минимально обработанные) данные, что позволяет избежать потери информации
Redis	Система управления базами данных на основе открытого кода, которая хранит данные в оперативной памяти, а не на диске
Redis Sentinel	Специализированная система управления узлами Redis, которая обеспечивает высокую доступность за счёт автоматического обнаружения отказа и выбора новой реплики в качестве мастера
REST API	(англ. Representational State Transfer Application Programming Interface) Архитектурный стиль взаимодействия между клиентом и сервером через протокол HTTP
RX	Клиент-серверный протокол удалённой работы с виртуальным рабочим столом (терминалом) российской компании Ethersoft
R&D	(англ. Research and Development) Системный подход к научным исследованиям и технической разработке, направленный на создание новых продуктов, улучшение существующих решений и внедрение инноваций в бизнес-процессы
SAS	(англ. Serial Attached SCSI) Последовательный компьютерный интерфейс подключения жёстких или твердотельных дисков, иных накопителей, является развитием стандарта параллельного интерфейса SCSI
SCADA	(англ. Supervisory Control And Data Acquisition) Программно-аппаратный комплекс для диспетчерского управления и сбора данных в реальном времени
Service Desk	Централизованная система для управления запросами пользователей, связанная с ИТ-сервисами

Термин, сокращение	Определение
SNMP	(англ. Simple Network Management Protocol) Стандартный интернет-протокол для управления и мониторинга устройств в IP-сетях
SFF	(англ. Small Form Factor) Форм-фактор накопителей, который определяет их физические размеры
Syslog	Стандартизированный протокол для сбора, передачи и хранения сообщений журналов в компьютерных системах и сетях
S7	Программное обеспечение для программируемых логических контроллеров и систем управления
TREI	Программно-технические комплексы для автоматизации технологических процессов и информационно-измерительных систем
UNet	Сетевой фреймворк/стек на базе протокола UDP с поддержкой broadcast/multicast, резервирования каналов, и обеспечения качества передачи со стороны приложений
VDI	(англ. Virtual Desktop Infrastructure) Технология виртуализации рабочих столов, при которой рабочее место пользователя размещается не на локальном компьютере, а на удалённом сервере
VLAN	(англ. Virtual Local Area Network) Виртуальная локальная компьютерная сеть
VXLAN	(англ. Virtual Extensible LAN) Технология сетевой виртуализации, которая позволяет создавать масштабируемые виртуальные сети
WebUI	Графический интерфейс, реализованный с использованием веб-технологий и доступный через браузер
ZeroMQ	Высокопроизводительная асинхронная библиотека для обмена сообщениями между приложениями
ВС	Виртуальная среда
ГИС	Государственные информационные системы
ЗОКИИ	Значимый объект критической информационной инфраструктуры
Кластер	Отказоустойчивая архитектура совместно работающих узлов в программно-аппаратном комплексе
Машина Скала^р (Машина СКАЛА-Р)	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. Зарегистрирован в реестрах Минпромторга как программно-аппаратный комплекс (код ОКПД2 26.20.14.160)
ОСРВ	Тип специализированной операционной системы, основное назначение которой — предоставление необходимого и достаточного набора функций для проектирования, разработки и функционирования систем реального времени на конкретном аппаратном оборудовании

Термин, сокращение	Определение
ПАЗ	Противоаварийная автоматическая защита
ПЛК	Программируемый логический контроллер — цифровая электронная система, предназначенная для управления технологическими процессами в режиме реального времени.
Подсистема	Логическое объединение компонентов по функциональному признаку, с целью пояснения состава и принципов действия ПАК
РЗА	Релейная защита и автоматика
РСУ	Комплекс программно-аппаратных средств, предназначенный для автоматизации и управления технологическими процессами на промышленных объектах
СУУТП	Система усовершенствованного управления технологическим процессом
Система ТОиР	ТОиР — сокр. от «техническое обслуживание и ремонт». Система ТОиР — это комплекс программных и организационных инструментов для управления техническим обслуживанием и ремонтом оборудования, направленный на повышение надежности, сокращение простоев и оптимизацию затрат
Узел	Узел вычисления (сервер) или сетевой узел (коммутатор) в составе Модуля, в зависимости от контекста

1 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

Настоящий документ дает концептуальный и архитектурный обзоры **Машины управления технологическими процессами Скала^р МСП.ТП** (далее **Скала^р МСП.ТП**, **Машина, МСП.ТП**), название в реестрах Минпромторга РФ «Машина специализированная СКАЛА-Р МСП.ТП».

Документ раскрывает, как оптимизированные программно-аппаратные комплексы отвечают современным вызовам в задачах построения АСУ ТП и фокусируется на **Машине Скала^р МСП.ТП.**

Аудитория

Документ предназначен для партнеров **Скала^р** и заказчиков, перед которыми ставятся задачи разработки, закупки, управления или эксплуатации **Машины** при модернизации или построении АСУ ТП.

Целевая аудитория заказчика:

- служба главного метролога
- служба главного технолога
- служба главного инженера
- службы директора / руководителя по производству
- иные заинтересованные технологические и производственные подразделения

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 является программно-аппаратным комплексом, предназначенным для автоматизации управления, контроля, диагностики и оптимизации технологических и производственных процессов/операций в реальном времени при помощи создания горизонтально масштабируемой и отказоустойчивой среды серверной виртуализации, а также инфраструктуры для виртуальных рабочих мест пользователей.

Машина является базовой ИТ-инфраструктурой для эксплуатации ключевых систем автоматизации технологических и производственных процессов (АСУ ТП, СУУТП, SCADA, MES, ПЛК и РСУ), включая ПАЗ и версии исполнения систем для опасных производств (в соответствующем варианте исполнения, включая требования к варианту исполнения шкафа).

В состав **Машины** входят унифицированные узлы вычисления и сетевые узлы.

Конструктивно **Машина** собирается из служебных и функциональных **Модулей Скала^р**, каждый из которых, 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 и необходимые сетевые узлы.

Машина обеспечивает следующие преимущества:

- гарантия совместимости компонентов — **Скала^р** проводит R&D работы по выбору и валидации оборудования вместе с используемым программным обеспечением. Узлы вычисления, контроллеры, накопители, сетевые узлы, программное обеспечение виртуализации, управления тестируются в соответствии с разработанными архитектурой и технологическими картами **Машины** именно в той комбинации, которая будет поставляться заказчикам
- **Машина** поставляется с предварительно установленным системным, служебным и функциональным платформенным ПО и готова к эксплуатации немедленно после ее монтажа и подключения у заказчика
- серийное производство позволяет создать легко тиражируемое решение с регламентными сроками доступности к поставке. Оборудование из состава **Машины** является не только технически валидированным, но и подтвержденным OEM-соглашениями с ведущими поставщиками узлов и компонентов
- собственная сервисная служба позволяет обеспечить техническую поддержку «из одного окна» по всем составляющим комплекса. Инциденты, даже на стыке аппаратных и программных компонентов, будут разбираться службой поддержки **Скала^р**, специалисты которой, при необходимости, уже сами обратятся в поддержку производителя конкретного компонента
- получение новых функций с обновлениями системы. Функциональность реализована не в аппаратном, а в программном обеспечении, поэтому добавление новых функций не будет ограничено тем, что «приобретен комплекс предыдущего поколения»
- быстрая адаптация к требованиям бизнеса. **Машина** базируется на типовом серверном и сетевом оборудовании с широкой доступностью на российском рынке, с возможностью гибкого подбора его конфигураций
- надежная производительная работа **Машины** при больших нагрузках. Гиперконвергентная программно-определяемая система хранения данных поддерживает масштабирование производительности как вертикально (выбором более быстрых накопителей и интерфейсов их подключения), так и горизонтально

— выбором большего числа накопителей/узлов хранения. Кроме того, такая система состоит из большого числа равнозначных узлов хранения и архитектурно не имеет единственного компонента, который мог бы стать узким местом или единой точкой отказа всего хранилища

- возможность вывести из эксплуатации любой элемент (или даже несколько) системы — узел вычисления или узел хранения — без существенного влияния на общую работоспособность и производительность системы
- нечувствительность к единичным отказам
- более низкие требования к широте экспертизы специалистов, эксплуатирующих решение, за счет меньшей номенклатуры компонентов
- возможность гибкого и почти мгновенного перераспределения ресурсов между задачами
- удобное централизованное управление вычислительными ресурсами из единого интерфейса с назначением приоритетов и правил общего доступа
- возможность переноса работающих виртуальных машин между узлами вычисления без остановки
- все функции сервера управления средствами виртуализации доступны через программный интерфейс (API), что дает возможность реализации полной автоматизации операций над инфраструктурой и, как следствие, возможность встраивания в частные и гибридные облачные решения
- механизмы сетевой изоляции, непрерывности и высокой доступности для запущенных виртуальных машин, автоматической балансировки вычислительной нагрузки в рамках одного вычислительного кластера
- мониторинг текущего состояния и утилизации ресурсов как аппаратных, так и программных компонентов **Машины**, с возможностью настройки длительности хранения собираемых метрик и их пороговых значений и параметров оповещения
- управление полным жизненным циклом **Машины**: установка и обновление всех программных компонентов в составе **Машины**, автоматическое формирование отчетов о версиях установленного ПО

3 ОТЛИЧИТЕЛЬНЫЕ ЧЕРТЫ

Главными отличительными чертами **Машины** являются поставка программно-аппаратного комплекса «под ключ» и ориентация на высокую надежность и высокую производительность на уровне архитектуры:

- как гипервизор, так и программно-определяемая система хранения данных создавались и развиваются с упором на надежность и безотказную работу
- резервирование данных на хранилище гибко настраивается под задачу: для особо критичных виртуальных машин можно повысить количество копий при резервировании данных с рекомендуемых «трех копий» до требуемого значения. При деградации хранилища ниже определенного заданного числа копий, хранилище автоматически перейдет в режим «только чтение», чтобы не допустить возможные полные потери данных или переход в неконсистентное состояние. В случае защиты данных помехоустойчивым кодированием (Erasure Coding) можно также выбрать оптимальные параметры кода Рида-Соломона, отдавая предпочтение или более высокой производительности или уменьшению накладных расходов полезного объема хранилища
- для всех виртуальных машин доступен кластер высокой доступности, минимизирующий время простоя при отказах узлов вычисления
- реализовано единое управление виртуальными ресурсами и мониторинг для многокластерной архитектуры решения
- надежность и гибкость варианта исполнения в соответствии с требованиями существующих систем и отечественных решений АСУ ТП, СУУТП, SCADA, MES, ПЛК и РСУ на базе принципов открытого АСУ ТП https://openapc.ru/resolution
- возможность обмена данными по промышленным протоколам, поставки контроллера отечественного производства в составе решения, совместимого с отечественным ОСРВ

Также, все комплектующие и составные части оборудования **Машины** проходят всестороннее тестирование и валидацию еще на этапе R&D, затем на этапе входного тестирования на производстве и на этапе выходного тестирования готовой **Машины**. При этом, конфигурация **Машины** предусматривает резервирование всех потенциальных единых точек отказа. Это не только узлы вычисления и накопители, но и сетевые контроллеры и сетевые узлы в составе **Машины**.

Последнее по порядку, но не по значению — служба технической поддержки «из одного окна».

Подробный перечень отличительных свойств по категориям приводится ниже.

Высокая доступность и производительность

- защита от отказа единичных узлов и аппаратных компонентов, установленных в узлы вычисления (жесткие диски, блоки питания и т.п.) обеспечивается их дублированием и схемами программной защиты данных
- высокоскоростные сети внутренней и внешней связности
- архитектурная оптимизация производительности
- специальные настройки программного обеспечения
- встроенная система мониторинга и анализа состояния **Машины** собственной разработки **Скала^р**

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
- коэффициент готовности составляет 0,9999
- интенсивность отказов — 0,0002 отказа в час
- ПАК соответствует классу готовности А3 (ГОСТ МЭК 60870-4-2011), классу МЦ-1 (ГОСТ Р 70139-2022) и уровню Tier III по классификации Uptime Institute

Гибкая система управления

- централизованное управление из единого web-интерфейса
- расширения функций опциональным интегрированным ПО

Линейная масштабируемость

- компоненты **Машины** подобраны и сбалансированы для раскрытия всего потенциала масштабируемости
- наращивание количества узлов вычисления 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 своевременного обнаружения слабых мест в защите и предотвращения возможных атак
- применение специальных промышленных профилей защиты операционных систем и сервисов (hardening) при производстве **Машин**

Обеспечение качества при развертывании

- оптимальность настроек подтверждена значительным количеством установок
- автоматизированное развертывание **Машины** на производстве **Скала^р** снижает риск человеческой ошибки
- стандартизация развертывания 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 **Машины**
- выпуск предварительно проверяемых патчей
- консультационная поддержка заказчиков и партнёров
- рекомендации по трекам обучения и проведение заказных вебинаров от вендора

Экономическая эффективность

- специальные условия лицензирования
- минимальные сроки проектирования решения
- сокращенные сроки ввода комплекса и решения в эксплуатацию
- только обоснованно необходимые компоненты

Альтернатива VMware vSphere, Microsoft Hyper-V, Citrix Hypervisor

- полностью российское решение для виртуализации и размещения специального технологического ПО и ПО АСУ ТП
- отлаженные инструменты и процессы миграции с иных систем виртуализации и с физических узлов вычислений
- высокая надежность и производительность
- качество, подтвержденное опытом практического применения

4 ПОДТВЕРЖДЕННАЯ БЕЗОПАСНОСТЬ

4.1 Операционные системы

Машина с сертифицированной **ОС Альт 8 СП** (сертификат ФСТЭК 3866 от 10.08.2018 г., действует до 10.08.2028 г.). ОС используется в качестве гостевой в служебных виртуальных машинах комплекса или основной для выделенных узлов вычисления.

ОС Альт 8 СП

ОС 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

ОС 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

4.2 Гипервизор и хранилище

Гипервизор и хранилище (в зависимости от исполнения ПАК) **Машины**, также обладают актуальной сертификацией ФСТЭК России и соответствует **4-му уровню доверия** по требованиям ФСТЭК России согласно нормативным документам:

- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (приказ ФСТЭК России от 2 июня 2020 г. №76)
- «Требования к средствам виртуализации» (приказ ФСТЭК России от 27 октября 2022 г. №187)

4.3 Средства защиты

Avanpost FAM

Машина может включать в себя при поставке сертифицированное средство единой аутентификации «Avanpost FAM» (сертификат ФСТЭК 4492 от 13.12.2021 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

«Соболь» версия 4

Машина совместима и может включать в себя при поставке сертифицированное средство доверенной загрузки ПАК «Соболь» версия 4 (сертификат ФСТЭК №4043 от 05.12.2018, действует до 05.12.2028), которое может быть применено для защиты информации:

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

ПАК «Соболь» 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 2 уровню доверия
- «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013)
- «Профиль защиты средства доверенной загрузки уровня платы расширения второго класса защиты. ИТ.СДЗ.ПР2.ПЗ» (ФСТЭК России, 2013)

Протестирована совместимость
с наложенными средствами защиты

Машина совместима и может использовать средства защиты информации:

PT ISIM (Positive Technologies Industrial Security Incident Manager) — это программно-аппаратный комплекс для глубокого анализа технологического трафика (DPI) и

мониторинга безопасности промышленных систем (АСУ ТП). Он выявляет кибератаки, вредоносное ПО и неавторизованные действия на ранних стадиях, помогая обеспечивать кибербезопасность критической инфраструктуры (КИИ).

PT NGFW (от Positive Technologies) — это межсетевой экран нового поколения (Next Generation Firewall, NGFW), разработанный в России. Основные характеристики:

- сертификация: продукт сертифицирован ФСТЭК (сертификат № 4877) и включён в реестр российского ПО Минцифры. Соответствует требованиям 152-ФЗ и защиты КИИ
- производительность: до 300 Гбит/с в режиме распознавания пользователей и приложений (для модели PT NGFW 3040)
- архитектура: универсальная архитектура x86 — не требует специализированных аппаратных ускорителей
- глубина устройства до 600 мм, фронтальное размещение интерфейсов — упрощает установку без изменения существующей коммутации
- резервирование питания: все модели имеют два блока питания; старшие модели поддерживают горячую замену

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.ПЗ» (ФСТЭК России, 2012)
- «Профиль защиты средств антивирусной защиты типа В четвертого класса защиты. ИТ.САВ3.В4.ПЗ» (ФСТЭК России, 2012)

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 Б 2 класса защиты. ИТ.САВ3.Б2.13» (ФСТЭК России, 2012)
- «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВ3.В2.ПЗ» (ФСТЭК России, 2012)
- «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВ3.Г2.ПЗ.».

*Указанное в подразделе совместимое ПО наложенных средств защиты не входит в поставку **Машины**.*

5 СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

Машина является универсальным модульным решением для построения инфраструктурной платформы и может применяться в разнообразных сценариях и их комбинациях. Несколько примеров приведены ниже.

Миграция (модернизация) унаследованных систем в виртуальную среду

Промышленные предприятия сталкиваются с комплексом вызовов, связанных с эксплуатацией и развитием систем автоматизации. Резкое сокращение поддержки со стороны зарубежных производителей АСУ ТП, ускоренное моральное и физическое старение вычислительной инфраструктуры, кратное увеличение киберугроз, а также ужесточение требований в области кибербезопасности и импортозамещения создают значительные операционные и финансовые риски. Фактически, существует реальная угроза нарушения непрерывности технологических процессов из-за невозможности поддерживать работоспособность критически важных систем управления. При этом одномоментная замена всей существующей АСУ ТП на полностью отечественные решения на текущем этапе развития технологий практически невозможна или экономически нецелесообразна. Это приводит к необходимости совместной эксплуатации унаследованных зарубежных систем и новых российских разработок. Данная ситуация требует создания универсальной, отказоустойчивой и безопасной ИТ-платформы, которая стала бы основой для планомерной модернизации без остановки производства.

Машина обеспечивает гарантированную совместимость с системами ведущих производителей, позволяя эксплуатировать даже устаревшие версии ОС и ПО в современной защищенной среде.

Новые проекты внедрений АСУ ТП

Внедрение **Машины** позволяет консолидировать вычислительные ресурсы и приводит к сокращению количества физических серверов на 30-40% за счет виртуализации. Таким образом существенно снижаются затраты на электроэнергию, охлаждение и занимаемые площади. Централизованное управление всей ИТ-инфраструктурой АСУ ТП сокращает операционные расходы на администрирование и техническое обслуживание.

Машина включена в дорожную карту развития Национальной платформы промышленной автоматизации (О-АСУ ТП) и рекомендована для использования в проектах импортозамещения рабочей группой по вопросу разработки открытой автоматизированной системы управления технологическими процессами (АНО «Открытые системы автоматизации»).

Во всех сценариях важное значение имеют такие преимущества **Машины**, как подтвержденная совместимость программных и аппаратных компонентов, быстрый и простой ввод в эксплуатацию за счет поставки полностью предустановленного решения, единая техническая поддержка и доступ к новым функциям путем обновления программной части **Машины**.

Универсальная серверная инфраструктура предприятия

Машина как платформа может стать надежным фундаментом для инфраструктуры серверной виртуализации предприятия. Платформа может содержать от четырех до нескольких десятков узлов вычисления, объединенных в один или несколько отказоустойчивых вычислительных кластеров, с управлением из одного окна единой системы управления. Оптимальное количество узлов вычисления в одном кластере составляет 4-16 узлов.

В зависимости от требований это может быть как единая **Машина**, так и несколько **ПАК Скала^р** (например, обслуживающих организационно разные задачи под управлением различных отделов). При этом различные ПАК могут быть включены в единый контур мониторинга средствами ПО **Скала^р**.

Инфраструктура виртуальных рабочих мест

Машина является отличным фундаментом и для инфраструктуры виртуальных рабочих мест, во многом благодаря полностью разработанному в России продукту Basis Workplace в своем составе. Продукт реализует всё необходимое для виртуальных рабочих мест поверх платформы серверной виртуализации от **Скала^р** — подключение к VDI, к терминальным серверам, публикацию приложений, доступ к физическим ПК и др.

Системы и средства промышленной автоматизации

На базе платформы **Машины** функционируют распределённые системы управления (DCS), служащие фундаментом для построения комплексных цифровых решений на производстве.

В промышленной автоматизации (АСУ ТП), это обеспечивает:

- сбор данных с датчиков, станков с ЧПУ, производственных линий и консолидацию в единую информационную систему
- управление исполнительными механизмами: выдачу управляющих команд на основе заданных технологических параметров
- надёжность: поддержка заданных параметров, отказоустойчивость, «горячее» и «холодное» резервирование для бесперебойной работы
- расчёт ключевых показателей эффективности (OEE) и выявление «узких мест» производства
- внедрение систем ТОиР: переход от планово предупредительных ремонтов к предиктивной аналитике (прогнозирование износа узлов)
- оперативный контроль производства: инструменты для расследования инцидентов и генерации отчётности

Интеграция IT и OT-контуров

На базе платформы **Машины** возможно:

- создание единой платформы, где данные с оборудования (OT) напрямую поступают в корпоративные системы управления производством (MES) и предприятием (ERP)
- поддержка edge вычислений: обработка данных на периферии для снижения нагрузки на центральную систему
- интеграция с российскими системами управления

Промышленная роботизация и ИИ

Использование в **Машине** ИИ-инструментов позволяет добиться следующих преимуществ:

- техническое зрение и адаптивная роботизация: определение пространственного положения объектов (например, железнодорожных вагонов) и передача данных в **Машину** для управления манипуляторами
- гибкая автоматизация «бесконвейерного» производства: работа роботов в динамической среде, высокоточные операции на движущихся объектах

- прогнозирование отказов (Predictive Maintenance): анализ данных с датчиков (вибрация, температура, ток) для предсказания поломок
- повышение энергоэффективности: оптимизация работы насосов, компрессоров и другого оборудования
- унификация оборудования разных производителей: применение универсальных ИИ моделей как контроллеров
- интеллектуальные помощники инженеров: AI ассистенты в формате чата для диагностики и ремонта оборудования

Обучение и подготовка кадров

На базе платформы **Машины** возможно:

- создание виртуальных сред, имитирующих реальную инфраструктуру (заводы), в том числе с применением цифровых двойников предприятия
- отработка навыков управления производственными процессами, приближённых к реальным
- тестирование сценариев реагирования на инциденты.

Информационная безопасность и кибериммуность

Машина поддерживает принцип кибериммунность - выполнение критических функций даже при компрометации отдельных компонентов.

В промышленной автоматизации (АСУ ТП) это обеспечивает:

- анализ копий сетевого трафика: выявление аномалий и угроз без влияния на технологический процесс
- безопасную передачу данных между контурами управления в критической информационной инфраструктуре (КИИ)
- фильтрацию трафика локально, без расшифровки SSL/TLS (защита от DDoS и ботов)
- гибридные схемы защиты от многовекторных DDoS атак
- технология «ловушек» и «приманок» для выявления целевых атак (APT) и уязвимостей нулевого дня
- создание кибериммуных терминалов релейной защиты и автоматики (РЗА), устойчивых к атакам

Доверенные ПАК

Ранее компании использовали технологии и ПО преимущественно иностранного происхождения ввиду их широкой доступности и технологической зрелости, но в сложившейся ситуации они уже не отвечают требованиям государственной безопасности и надежности ввиду рисков несанкционированного доступа к данным, отсутствия гарантий бесперебойности в работе и из-за использования в качестве инструмента для ослабления критически важных отраслей государства.

В ноябре 2023 года вышло Постановление Правительства РФ №1912, обязывающее перевести все значимые объекты критической информационной инфраструктуры (ЗОКИИ) на доверенные программно-аппаратные комплексы до 31 декабря 2029 года. С 1 сентября 2024 года субъекты КИИ не могут использовать недоверенные ПАК, приобретенные после этой даты.

Для признания ПАК доверенным необходимо выполнить ряд требований:

- ПАК находится в Реестре российской промышленной и радиоэлектронной продукции Минпромторга РФ
- программное обеспечение ПАК зарегистрировано в Реестре российского ПО Минцифры
- если программно-аппаратный комплекс реализует функцию защиты информации, то ПО, реализующее такую функцию, должно иметь сертификат ФСТЭК
- ПАК должен предоставлять функциональную устойчивость

Таким образом, доверенный ПАК должен представлять собой комплексное изделие из исключительно российского оборудования и программного обеспечения и быть признанным как промышленное изделие российского производства.

ПАК производства Скала^р соответствуют этим и иным критериям согласно ПП №1912.

Скала^р использует подход, позволяющий организациям любого масштаба и направленности, в том числе субъектам критической информационной инфраструктуры (КИИ), оперативно выстраивать высоконагруженный, обозримый и легко масштабируемый ИТ-ландшафт полностью на российских технологиях доверенных ПАК, обеспечивая при этом максимальную совместимость всех компонентов системы. В результате, сроки проектов по импортозамещению и созданию аттестованных контуров КИИ значительно сокращаются.

Команда профильных специалистов по регламентации производства и информационной безопасности Скала^р готова оказать предварительные консультации по таким вопросам.

6 ПРИНЦИПЫ СОЗДАНИЯ МАШИНЫ

Машина управления технологическими процессами Скала^р создана для работы с масштабируемой виртуальной инфраструктурой

Целью разработки **Машины** было создание программно-аппаратного комплекса (ПАК), специально адаптированного для исполнений с системным ПО **Basis vControl**, **Росплатформа (Р-Виртуализация, Р-Хранилище)** в целях создания высокопроизводительной платформы серверной виртуализации. 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** обеспечивает:

- горизонтальное масштабирование — наращивание ресурсов **Модулями Скала^р** без простоев
- высокую отказоустойчивость — кластер высокой доступности (HA) для ВМ, репликацию блоков данных и алгоритмы Erasure Coding на уровне программно-определяемого хранилища, технологии RAID при применении СХД
- гибкую подсистему хранения на основе гиперконвергентного программно-определяемого хранилища
- единое управление — web-интерфейс и REST API через **Basis vControl**, также через служебное ПО **Скала^р Геном** (который включает в себя компоненты ПО **Скала^р Визион**)

Технологические принципы

- дублирование критичных компонентов оборудования
- отсутствие единой точки отказа
- сохранение работоспособности при одновременном отказе отдельных элементов различных подсистем
- применение высокопроизводительных компонентов узлов
- горизонтальное масштабирование вычислительных ресурсов и ресурсов хранения
- многоуровневое тестирование Машины, ее узлов и компонентов при производстве
- комплексный подход к безопасности и защите данных

Технические решения

- архитектура основана на модулях и подсистемах и типизированных компонентах
- специальное ПО для управления и мониторинга **Машины**
- глубокая адаптация компонентов для совместной работы в составе **Машины**

Надежность на уровне архитектуры

- система управления виртуализацией может быть развернута на собственном выделенном кластере высокой доступности и, таким образом, отделена от вычислительной нагрузки в рамках **Машины**, что повышает ее безопасность и доступность

- система мониторинга и управления жизненным циклом **Машины** также может быть развернута на выделенных служебных узлах, чтобы исключить воздействие вычислительной нагрузки на показания регистрируемых метрик и ее зависимость в целом от работы продуктивных вычислительных кластеров

Высокая производительность на уровне архитектуры

- благодаря выделенной сети внутреннего взаимодействия все узлы взаимодействуют между собой с одинаково высокой скоростью
- физическое разделение технологической сети АСУ ТП, сети управления и сетей внутреннего взаимодействия и внешнего доступа гарантирует отсутствие задержек и удобство подключения к сетям заказчика

Проработанность всех программных компонентов

Основные программные элементы **Машины:**

- программная платформа обслуживания и мониторинга **Машины Скала^р Геном**

В ходе создания **Машины** была разработана методика оптимизации настройки ядра ОС каждого из узлов вычисления **Машины** под конкретный вариант ее применения. Заказчик получает **Машину**, настроенную под функциональные требования проекта.

Инсталляция узлов **Машин** на производстве осуществляется при помощи разработанного в **Скала^р** специального ПО, что исключает риск человеческой ошибки.

Практическое применение тиражируемых экземпляров **МСП.ТП** продемонстрировало высокую стабильность работы и производительность при эксплуатации.

Команда инженеров и архитекторов **Скала^р** изучает области для дальнейшего развития **Машин** и продолжает работу по оптимизации ПАК; кроме того, постоянно ведется деятельность по развитию систем мониторинга и управления собственной разработки.

Подтверждена поддержка гостевых ОС для виртуальных машин

- Windows Server 2008 R2 с SP 1, 2012, 2012 R2, 2016, 2019, 2022
- Windows 10
- Альт 9, 10, 11
- Astra Linux 1.7, 1.8
- РЕД ОС 7.3, 8
- Ubuntu 14.04 LTS (x64), 16.04 LTS (x64), 17.10 (x64), 18.04 (x64)

Следующие ОС также могут быть применены в качестве гостевых, но без гарантии работоспособности всех гостевых утилит (GuestTools):

- CentOS 6.x (x64), 7.x (x64)
- Debian 7.x (x64), 8.x (x64), 9.x (x64)
- openSUSE 42.x (x64)
- CloudLinux 6.x (x64), 7.x (x64)

Подтверждена совместимость в рамках дополнительного тестирования версий

- Windows XP, Vista, 7, 8, 10 Enterprise

Поддержка ключевых протоколов обмена данными при использовании соответствующего ПО

- OPC UA
- OPC DA, OPC AE, OPC HDA (на платформе Windows)
- Modbus TCP/IP, Modbus RTU, Modbus RTU Over TCP/IP
- IEC 60870-5-104 Client, Server
- IEC 61850 MMS
- MQTT
- BACnet
- S7 (Siemens)
- EtherNet/IP CIP (Rockwell Automation)
- FINS (Omron)
- UNet (TREI)
- SNMP
- ICMP
- Syslog

Все перечисленное формирует целостную архитектуру и динамику развития **Машины**.

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.

7 ВАРИАНТЫ ИСПОЛНЕНИЯ МАШИНЫ

Машины поставляются в виде функционально необходимого набора **Модулей Скала^р** и комплектуются в соответствии с показателями назначения, полученными от заказчика, и могут поставляться в двух вариантах исполнения.

Тип 1

Данное исполнение реализовано в виде Специализированного модуля **Машины**. На Специализированный модуль установлена ОС Альт 8 СП, гипервизор для виртуальных машин KVM и **ПО Скала^р Геном**, который является системой мониторинга и обслуживания **Машины**.

Тип 2

Данное исполнение реализовано в виде Базового модуля и модуля Виртуализации. В составе этого варианта исполнения **Машины** присутствует Основное функциональное ПО виртуализации Базис, гипервизор Р-Виртуализация, который обеспечивает разделение ресурсов сервера между виртуальными машинами, программно-определяемое хранилище Р-Хранилище, которое обеспечивает распределенный дисковый массив и **ПО Скала^р Геном**, которое является системой управления автоматизации обслуживания **Машины**.

Отличительные черты исполнений **Машины** представлены в таблице 1 и подробно описаны в разделе 9.

Таблица 1. Варианты исполнения Машины

Варианты исполнения	Сетевые узлы	Кластер управления (HA)	Узлы вычисления
Тип 1	■	□	■
Тип 2	■	■	■

8 СОСТАВ МАШИНЫ

Комплекты поставки

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 **Машину**, например, когда не хватает портовой емкости или есть необходимость увеличить производительность или объем хранения данных. Кроме того, можно добавить специальные **Модули Скала^р**, позволяющие расширить функциональность **Машины**.

На рисунках ниже (Рисунок 1 и Рисунок 2) представлены варианты исполнения **Машины** (Базовый комплект и Комплект модулей расширения), а также соответствие Модулей **Машины** функциональным подсистемам.

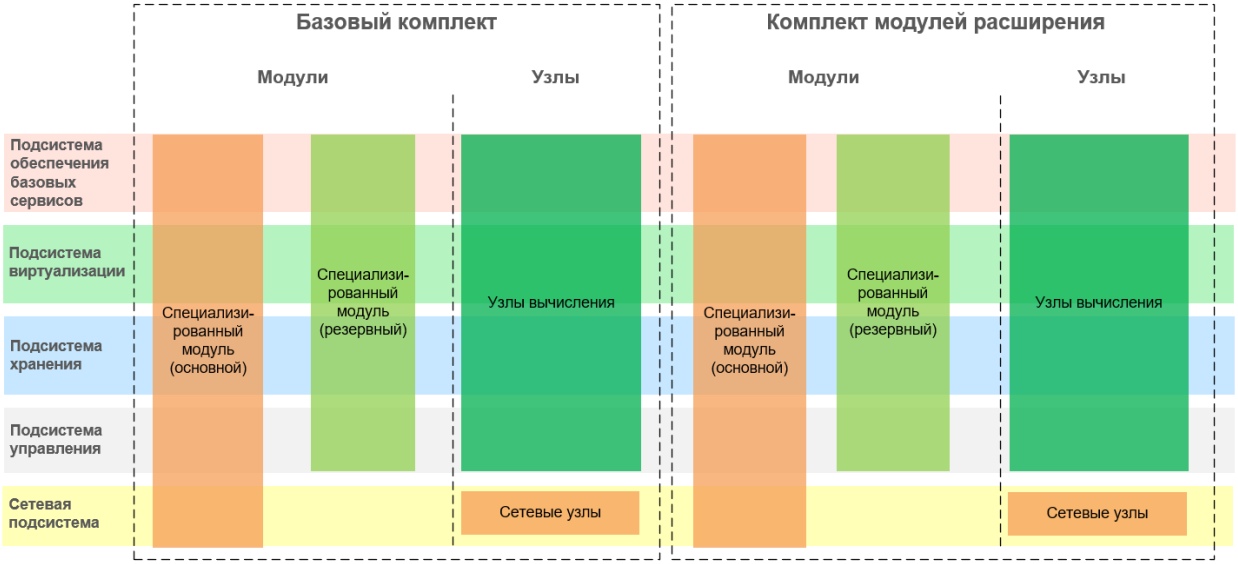

Рисунок 1. Вариант исполнения Машины (тип 1)

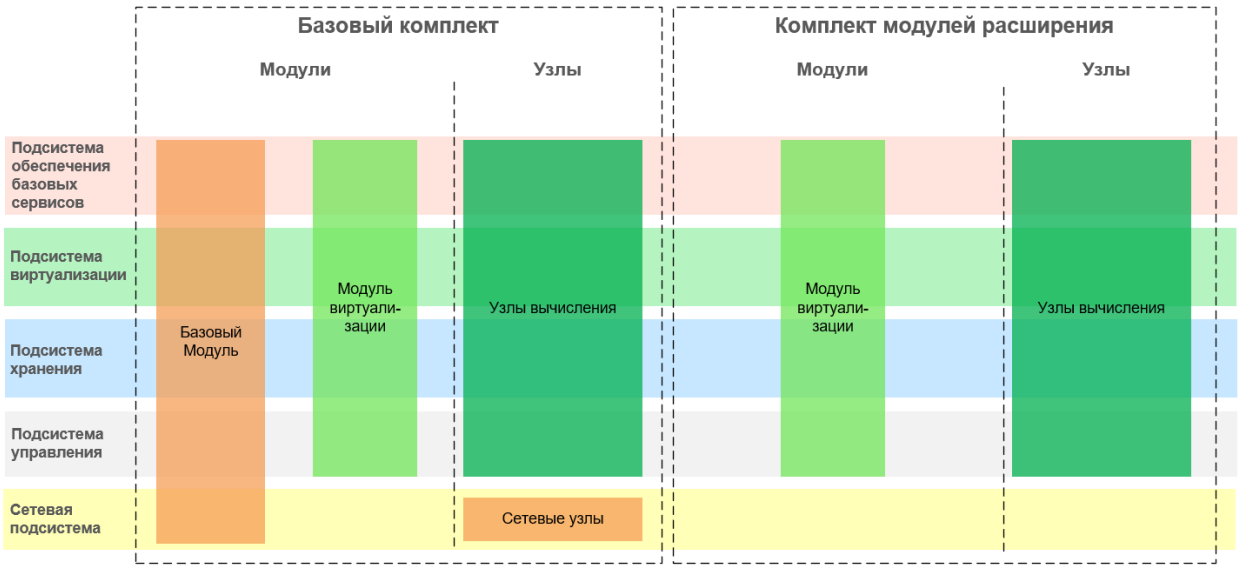

Рисунок 2. Вариант исполнения Машины (тип 2)

8.1 Подсистемы Машины

Функции **Машины** 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 **Машины**.

8.1.1 Подсистема обеспечения базовых сервисов

Подсистема обеспечения базовых сервисов отвечает за размещение служебных виртуальных машин с **ПО Скала^р Геном**, выполняющих функцию мониторинга аппаратных и программных компонентов **Машины** по обширному набору метрик, отслеживание состояния метрик, настройка оповещений при выходе за пределы нормальных значений, управление обслуживанием **Машины**:

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

8.1.2 Подсистема виртуализации

Подсистема виртуализации:

- объединяет в себе узлы вычисления с гипервизорами
- формирует виртуальную среду для последующего размещения продуктивных виртуальных машин с общими разделяемыми вычислительными ресурсами
- обеспечивает реализацию:
  - режима высокой доступности работы виртуальных машин
  - режима автоматической балансировки нагрузки между узлами вычисления в кластере с целью равномерной утилизации (насколько это возможно) их вычислительных ресурсов

8.1.3 Подсистема хранения

Подсистема хранения может объединять в себе унифицированные узлы хранения программно-определяемого хранилища и аппаратные системы хранения данных, предоставляя ресурс для хранения данных виртуальных машин.

8.1.4 Подсистема управления

Подсистема управления объединяет в себе узлы или виртуальные машины с управляющим виртуализацией ПО. Предоставляет администратору подсистемы виртуализации единый графический веб-интерфейс для управления виртуальной инфраструктурой, виртуальными машинами, виртуальными сетями, создания снэпшотов и резервных копий виртуальных машин.

8.1.5 Сетевая подсистема

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

- интерконнекта (внутреннего взаимодействия) и внешнего доступа (25 Гбит/с) — для организации быстрой связности с минимальными задержками между всеми компонентами ПАК, в том числе для работы гиперконвергентного программно-определяемого хранилища, а также для организации доступа к виртуальным машинам и элементам управления виртуализацией и администрирования ПАК
- управления (1 Гбит/с) — для организации выделенной сети низкоуровневого управления всеми узлами ПАК

8.2 Модули Машины

8.2.1 Базовый модуль

Базовый модуль используется для обеспечения сетевой связанности между компонентами, функций управления виртуализацией, функций виртуализации, общего хранилища, служебных функций, а также для организации выделенной сети управления **Машиной**.

В составе Базового модуля есть необходимые компоненты для подключения **Машины** к вышестоящим сетевым узлам.

Типовой состав для продуктивной инсталляции ПАК:

- два узла вычисления, совмещающих следующие функции:
  - управление виртуализацией
  - виртуализация, вместе с виртуальными машинами заказчика
  - общее хранилище
  - служебные функции и исполнение Программной платформы **Скала^р Геном**, включая мониторинг ПАК
- два сетевых узла 25 Гбит/с внешнего доступа и интерконнекта для случаев использования программно-определяющего хранилища
- один сетевой узел 1 Гбит/с для выделенной сети управления

Типовые характеристики узлов вычисления Базового модуля представлены в таблице 2.

Таблица 2. Типовые характеристики узлов вычисления Базового модуля

Категория	Характеристика
Процессор	2x CPU (2.6 ГГц / 24 ядра - минимальная конфигурация) 2x CPU (2.6 ГГц / 26 ядра - средняя конфигурация) 2x CPU (2.5 ГГц / 32 ядра - максимальная конфигурация)
Оперативная память	256 - 1024 Гбайт
Диски (накопители)	2x 480 Гбайт SSD (SFF SATA) - os 2x 960 Гбайт SSD (M.2 NVMe) - mds > 4 1.92 Тбайт SSD (SFF SATA) - sds

Сетевые карты	2x 10/25 Гбит/с, dual port 1 Гбит/с RJ45 (на материнской плате) 1 Гбит/с RJ45 IPMI (на материнской плате) 2x 1/10 Гбит/с RJ45 (для подключения к Технологической сети АСУ ТП)

Характеристики сетевых узлов Базового модуля:

- сетевые узлы 25 Гбит/с – маршрутизирующие коммутаторы с 48 портами 25 GbE и 8 портами 100 GbE
- сетевой узел 1 Гбит/с снабжен 48 портами 1 GbE и 4 портами 10/25 GbE

Применяемое в Базовом модуле программное обеспечение:

- основное функциональное ПО виртуализации Базис
- ПО виртуализации Р-Виртуализация
- ПО управления хранением Р-Хранилище
- ПО **Скала^р Геном**
- ПО Avanpost FAM (опционально)

8.2.2 Модуль виртуализации

Узлы вычисления Модуля виртуализации и Базового модуля образуют единый кластер вычисления. Это физические узлы, которые формируют вычислительные мощности для системы виртуализации (ЦПУ / ОЗУ) и общее программно-определяемое хранилище, служебные функции и исполнение Программной платформы **Скала^р Геном**, включая мониторинг ПАК.

В состав **Машины** рекомендуется включать 4-16 узлов вычисления, формирующих вычислительный кластер определяющий максимально возможный домен обеспечения высокой доступности для ВМ.

В состав Модуля входит один или более узел вычисления.

Узлы вычисления в Базовых модулях, Модулях виртуализации имеют одинаковые характеристики. Если в Базовом модуле **Машины** применяется процессор в минимальной конфигурации, то в Модуле виртуализации этой **Машины** используются такие же процессоры в минимальной конфигурации. То же самое применимо и к средней и к максимальной конфигурации.

Типовые характеристики узлов вычисления Модуля виртуализации совпадают с характеристиками узлов Базового модуля и представлены в разделе 8.2.1.

Применяемое в Модуле виртуализации программное обеспечение:

- основное функциональное ПО виртуализации Базис
- ПО виртуализации Р-Виртуализация
- ПО управления хранением Р-Хранилище
- ПО **Скала^р Геном**

8.2.3 Специализированный модуль

Специализированный модуль предназначен для осуществления функций специализированных задач **Машины**, в том числе подходит для установки специализированных сетевых карт, создан с применением сконфигурированного для выполнения заданных функций оборудования и специализированного ПО.

В **Машине** для обеспечения необходимого уровня отказоустойчивости используется два Специализированных модуля (основной и резервный).

Состав основного Специализированного модуля:

- один узел вычисления, необходимый для функционирования прикладного ПО с правом использования виртуализации
- два сетевых узла 1 Гбит/с управления, внешнего доступа и интерконнекта

Характеристики узла вычисления Специализированного модуля совпадают с характеристиками узлов вычисления Базового модуля и описаны в разделе 8.2.1.

Характеристики сетевых узлов Специализированного модуля:

- сетевые узлы 1 Гбит/с снабжены 48 портами 1 GbE, 4 портами 10/25 GbE и 2 портами 40 GbE

Состав резервного Специализированного модуля:

- один узел вычисления, необходимый для функционирования прикладного ПО с правом использования виртуализации

Резервный Специализированный модуль выполняет функцию холодного резерва. То есть при выходе из строя любого основного Специализированного модуля и невозможности его быстрого восстановления, специализированные сетевые карты устанавливаются в резервный Специализированный модуль, после чего запускаются виртуальные машины.

Применяемое в Специализированном модуле программное обеспечение:

- операционная система **ОС Альт 8 СП (**в качестве гипервизора используется связка из программного модуля ядра KVM и эмулятора ввода-вывода QEMU из дистрибутива базовой ОС)
- ПО **Скала^р Геном**
- ПО Avanpost FAM (опционально)

8.2.4 Модуль резервного копирования

В качестве системы резервного копирования (СРК) может использоваться внешний Модуль резервного копирования из состава **Машин** производства **Скала^р**.

Модуль резервного копирования предназначен для организации целевого хранилища резервных копий в среде виртуализации. Он обеспечивает прием, хранение и восстановление данных виртуальных машин и приложений по протоколу файлового доступа NFS, используя встроенные средства резервного копирования платформы виртуализации.

Хранилище используется платформой виртуализации как NFS-ресурс (Network File System).

Резервное копирование и восстановление виртуальных машин выполняется штатными средствами СРК без необходимости установки дополнительных агентов на гостевые ОС.

ПО для построения программно-определяемых систем хранения данных RAIDIX 5 обеспечивает отказоустойчивость на уровне дисков (программный RAID, защита от потери данных при выходе из строя одного или нескольких накопителей), а также высокую скорость потоковой записи, критически важную для окон резервного копирования.

Узел вычисления укомплектован четырьмя портами Ethernet 10/25 Гбит/с и двумя служебными портами Ethernet 1 Гбит/с (включая IPMI).

На базе портов 10/25 Гбит/с создается группа агрегации в режиме 802.3ad LACP, которая представляет собой на уровне операционной системы один логический агрегированный

интерфейс. Этот интерфейс предназначен для подключения внешних систем к сервису NFS.

Состав Модуля резервного копирования:

- один узел вычисления, совмещающий функции узла вычисления и системы хранения данных (СХД) на основе одноконтроллерной конфигурации программно-определяемой платформы RAIDIX 5

Типовые характеристики узлов вычисления Модуля резервного копирования представлены в таблице 3.

Таблица 3. Типовые характеристики узлов вычисления Модуля резервного копирования

Категория	Характеристика
Процессор	2x CPU (2.8 ГГц / 8 ядер)
Оперативная память	256 - 512 Гбайт
Диски (накопители)	2x 480 Гбайт SSD (SFF SATA) - os 2x 960 Гбайт SSD (M.2 NVMe) - mds > 4 20 Тбайт HDD (LFF NL-SAS) - sds
Сетевые карты	2x 10/25 Гбит/с, dual port 1x Гбит/с RJ45 (на материнской плате) 1x Гбит/с RJ45 IPMI (на материнской плате)

Применяемое в Модуле резервного копирования программное обеспечение:

- RAIDIX 5

9 АРХИТЕКТУРА МАШИНЫ

Конфигурация **Машины** (тип 1) представлена на рисунке 3.

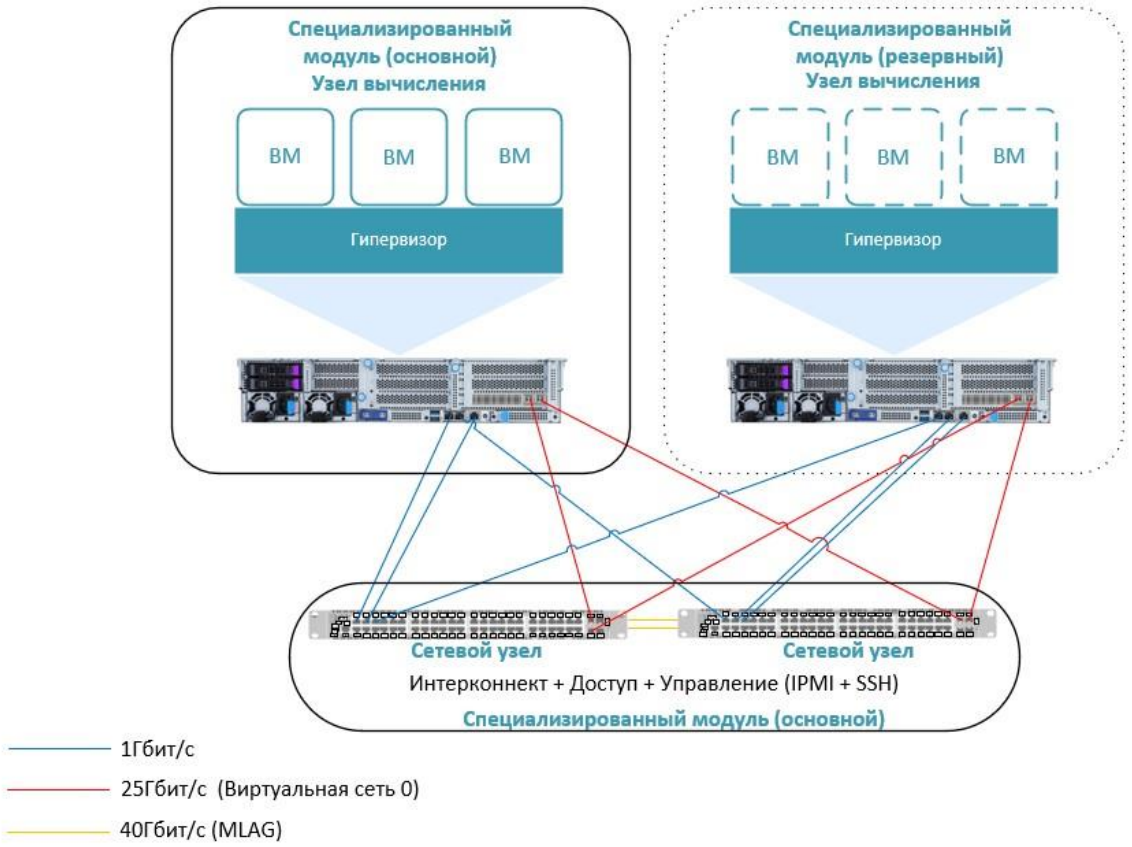

Рисунок 3. Конфигурация Машины (тип 1)

Конфигурация **Машины** (тип 2) представлена на рисунке 4.

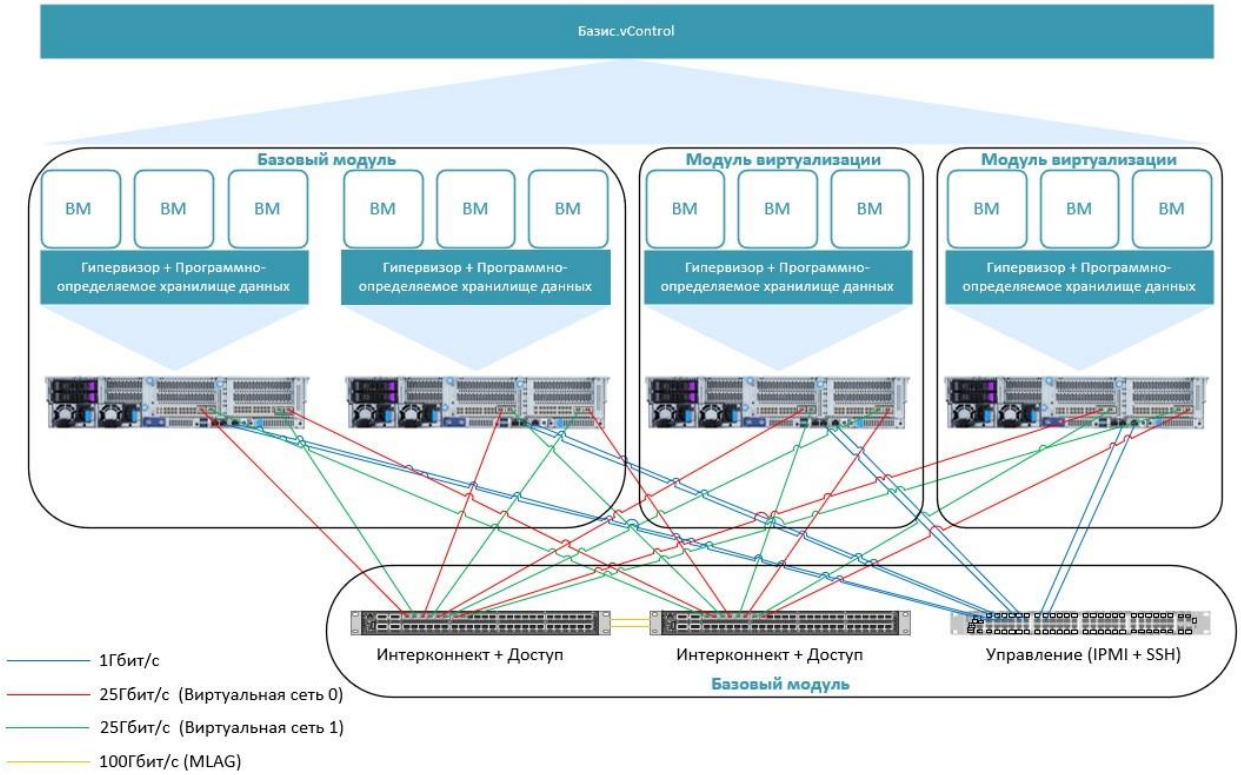

Рисунок 4. Конфигурация Машины (тип 2)

9.1 Кластер управления (HA)

Кластер управления – логический компонент виртуальной инфраструктуры, развернутый на четырех узлах вычисления. В кластере управления запускается все программное обеспечение, отвечающее за работоспособность платформы виртуализации, внутренние служебные базы данных, интерфейсы управления, включая GUI и REST API, которые управляют всеми узлами вычисления кластера.

Кластер управления подсистемы управления представляет собой кластер высокой доступности (HA) и разворачивается на общих с кластером вычисления узлах вычисления, с гипервизором Р-Виртуализация и общей разделяемой системой хранения данных (аппаратной или гиперконвергентной программной - Р-Хранилище) под единым управлением программного продукта Basis vControl.

Задача кластера управления – обеспечить отказоустойчивую среду виртуализации для размещения на этих вычислительных мощностях служебных инфраструктурных виртуальных машин в составе:

- кластер из 3-х виртуальных машин с ПО Basis vControl для управления всей виртуальной инфраструктурой ПАК
- кластер из 3-х виртуальных машин с ПО СУБД PostgreSQL (кластер собран на базе стека кластеризации Patroni/etcd) – служебная база данных, необходимая для работы ПО Basis vControl

9.2 Кластер вычисления

Кластер вычисления в гиперконвергентном исполнении обеспечивается вычислительными ресурсами и ресурсами хранения среду виртуализации (центральный процессор, оперативная память, дисковые ресурсы). На узлах вычисления кластера работает Р-Виртуализация, которая управляет разделяемым доступом виртуальных машин к вычислительным ресурсам узлов вычисления.

При этом узлы вычисления могут образовывать единый кластер вычисления на базе одной или нескольких разделяемых систем хранения данных (аппаратных или программных). В один вычислительный кластер, определяющий максимально возможный домен обеспечения высокой доступности для виртуальных машин, рекомендуется включать 4-16 узлов вычисления.

9.3 Виртуальные машины служебных компонентов

Служебные компоненты исполняются в следующих виртуальных машинах:

- виртуальная машина с установленной программной платформой **Скала^р Геном** – ПО, предназначенное для:
- автоматизации обслуживания **Машины**
- мониторинга основных аппаратных и программных компонентов ПАК
- оповещения при сбоях
- построения отчетов по собираемым данным

Программная платформа **Скала^р Геном** детально рассматривается в разделе 10.4

- виртуальная машина с установленным ПО Avanpost FAM – используется как единая платформа аутентификации и авторизации к сервисам управления, предоставляемым ПО **Скала^р Геном**. ПО Avanpost FAM может отсутствовать, если есть его установка или аналог в инфраструктуре заказчика

Данные виртуальные машины размещены на общих узлах вычисления, без выделения служебных узлов для них.

9.4 Сетевое взаимодействие

Схема сетей **Машины** представлена на рисунках 5 и 6. Сетевое взаимодействие обеспечивается двумя наборами сетевых узлов для организации сетей под следующие задачи:

- **сети внутреннего взаимодействия** – интерконнекта – служебные немаршрутизируемые сети для трафика репликации и доступа к программно-определяемому хранилищу, трафика доступа к аппаратной СХД (роль сети хранения), трафика репликации служебных узлов
- **сети внешнего взаимодействия** (сети доступа) – множество сетей продуктивных виртуальных машин (подключения к внешней сети (uplink) осуществляются с помощью сетевых узлов, входящий в комплект **Машины**)
- **сети управления** — выделенная сеть доступа к IPMI-контроллерам узлов вычисления из состава **Машины** и сеть доступа к консоли управления гипервизора по протоколу SSH

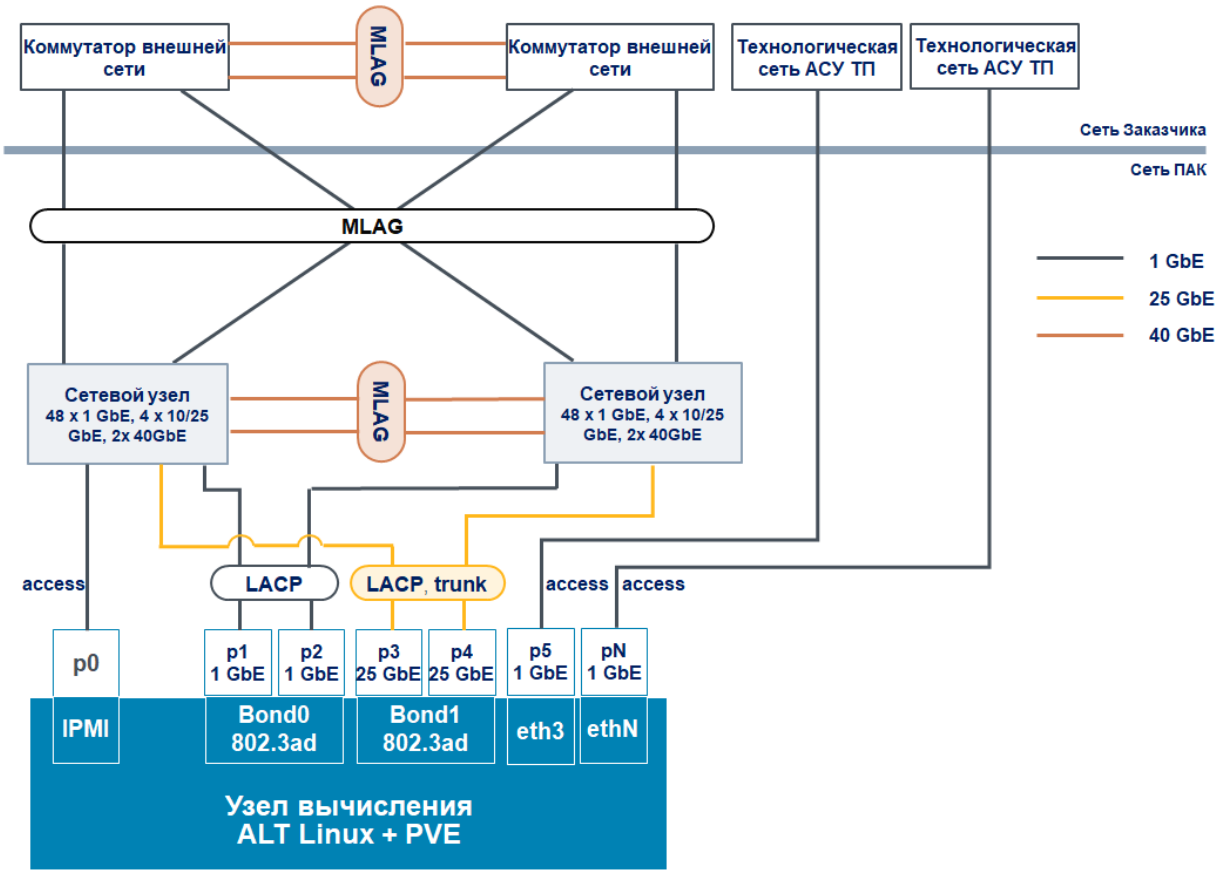

Рисунок 5. Физическая организация сетей в Машине (тип 1)

Конфигурация 2 + 0 для Машины (тип 1)

В этой конфигурации одна пара сетевых узлов обеспечивает и сети интерконнекта, и сети внешнего доступа, и сети хранения СХД, и сеть управления IPMI. Разделение сетей достигается за счет их логической изоляции через VLAN.

Кроме того, в зависимости от ряда факторов могут быть выбраны сетевые узлы с портами 25 Гбит/с. Сетевой узел для сети управления IPMI всегда с портами 1 Гбит/с.

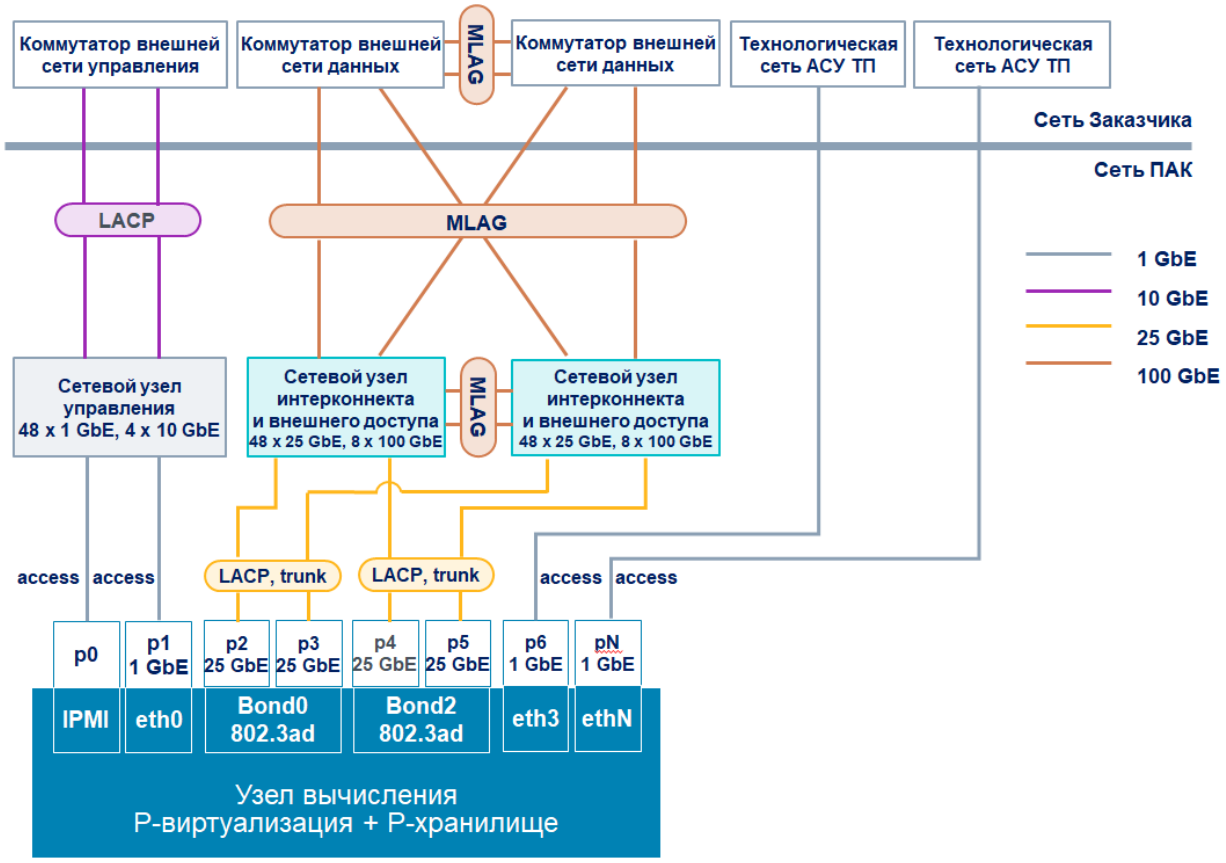

Рисунок 6. Физическая организация сетей в Машине (тип 2)

Конфигурация 2 + 1 для Машины (тип 2)

В этой конфигурации одна пара сетевых узлов обеспечивает и сети интерконнекта программно-определяемого хранилища, и сети внешнего доступа, и сети хранения СХД. Разделение сетей достигается за счет их логической изоляции через VLAN. Сеть управления IPMI реализуется на одном выделенном сетевом узле.

Выбор того, какую конфигурацию использовать, зависит от сайзинга, в частности, ожидаемой нагрузки на сети внешнего доступа и интерконнекта.

Кроме того, в зависимости от ряда факторов могут быть выбраны сетевые узлы с портами 25 или 100 Гбит/с. Сетевой узел для сети управления IPMI всегда с портами 1 Гбит/с.

10 ПРОГРАММНЫЕ КОМПОНЕНТЫ

Программная часть **Машины** реализована с помощью компонентов, перечисленных в таблице 4.

Таблица 4. Программные компоненты Машины

Наименование ПО	Назначение
ПО Basis vControl	Сервер управления средой виртуализации. Обеспечивает единый графический интерфейс управления виртуальной инфраструктурой **Машины**. Управляет гипервизорами, кластерами высокой доступности, виртуальными машинами, выполняет балансировку нагрузки, и т.д.
ПО Basis Workplace (опционально)	ПО для организации инфраструктуры виртуальных рабочих мест, которое интегрируется и работает только совместно с ПО Basis vControl.
ПО **Скала^р Геном** (которое, включает в себя компоненты ПО **Скала^р Визион**)	ПО, используемое для мониторинга основных аппаратных и программных компонентов ПАК, оповещений при сбоях в их работе, построения отчетов по собираемым данным для производства и дальнейшего обслуживания **Машины**
Р-Виртуализация	Система серверной виртуализации, разработанная компанией «Росплатформа». Это платформа для виртуализации серверов с централизированным управлением и интегрированным кластерным хранилищем, сочетающая гипервизор и системные контейнеры.
Р-Хранилище	Программно-определяемое хранилище данных от российской компании «Росплатформа» (ООО «Р-Платформа»). Это решение объединяет внутренние диски серверов в единую распределённую систему хранения данных, обеспечивая высокую производительность и отказоустойчивость.
ПО Avanpost FAM (Federated Access Manager) – опция	ПО используется как единая платформа аутентификации и авторизации к сервисам управления, предоставляемым ПО **Скала^р Геном**
ОС Альт СП (Альт 8 СП)	Операционная система со встроенными программными средствами защиты информации, которая сертифицирована ФСТЭК России, используется как базовая ОС на всех сервисных и служебных виртуальных машинах в ПАК.

10.1 Размещение программных компонентов

На рисунке 7 и 8 показана архитектура **Машины** с размещением программных компонентов на узлах в составе **Машины**. Виртуальные машины с ПО **Скала^р Геном**, виртуальная машина с ПО Avanpost FAM и виртуальные машины с программными компонентами ПО

Basis vControl размещены на общих узлах вычисления в едином отказоустойчивом кластере, где будут размещаться продуктивные виртуальные машины. Таким образом, имеется только один тип узлов: узлы вычисления с гипервизором под продуктивную нагрузку с развернутым на них же распределенным программно-определяемым хранилищем.

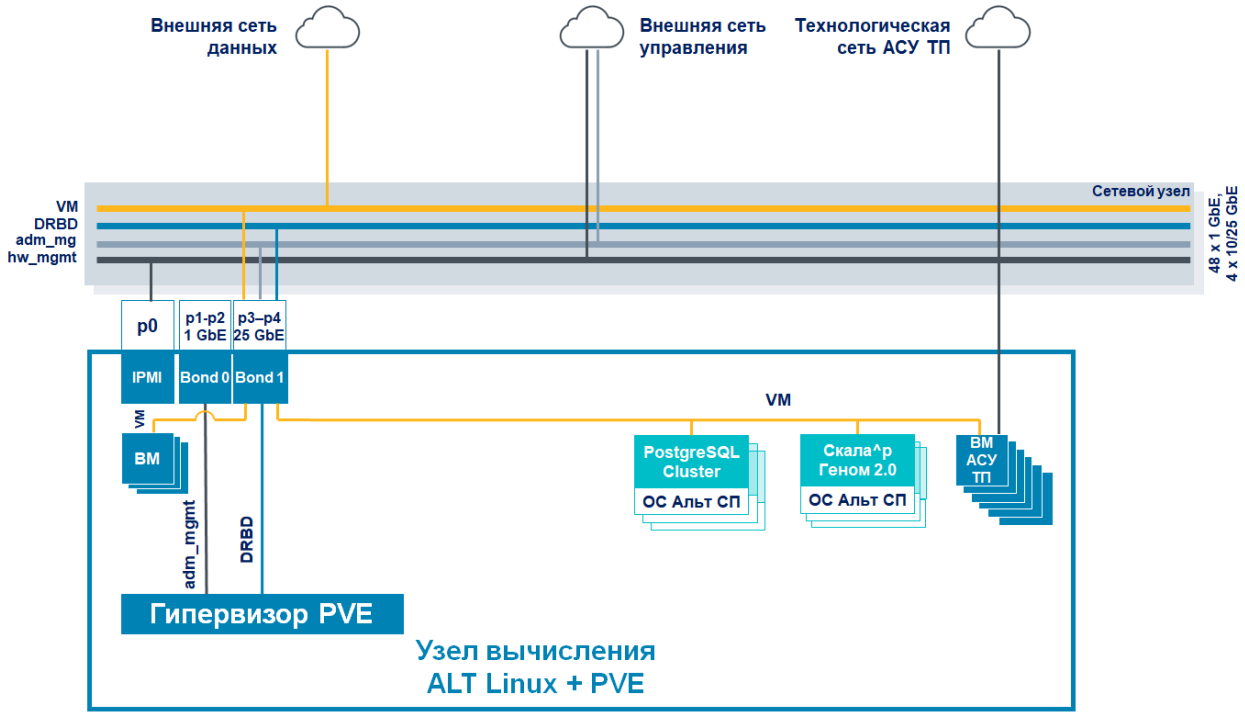

Рисунок 7. Узел и программные компоненты в архитектуре Машины (тип 1)

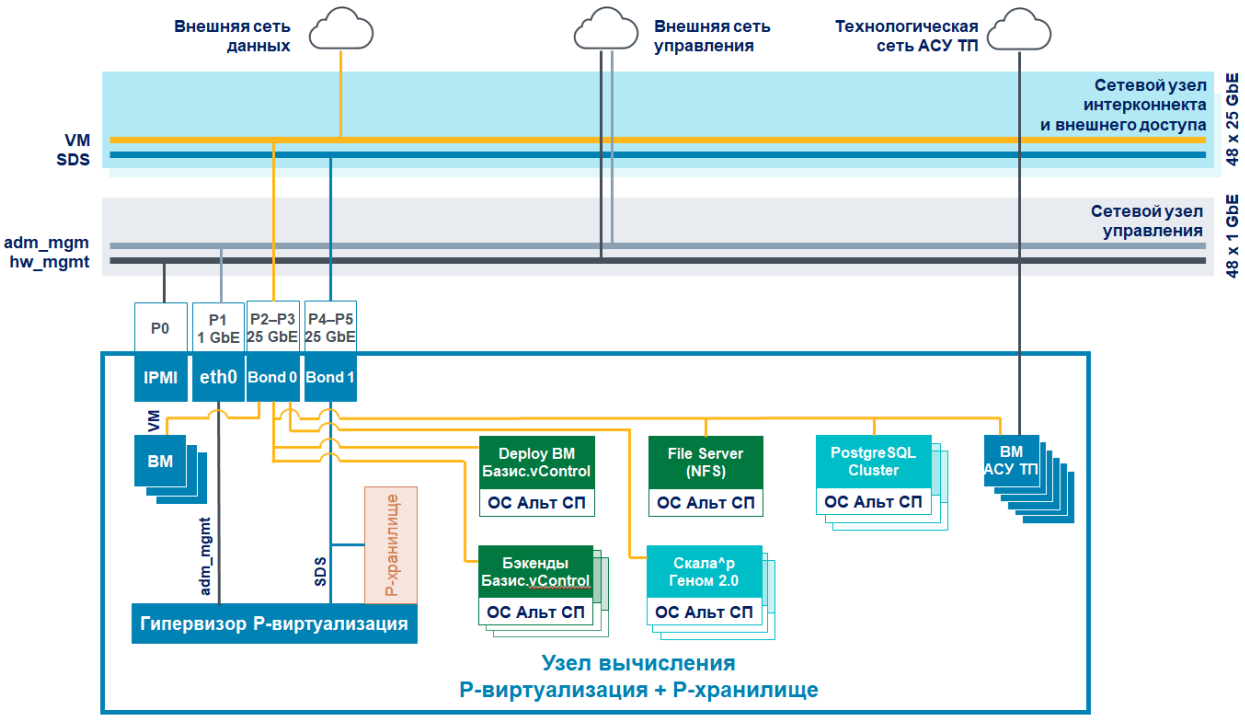

Рисунок 8. Узел и программные компоненты в архитектуре Машины (тип 2)

10.2 Basis vControl

ПО Basis vControl — это гибкая система управления и мониторинга средой виртуализации.

ПО Basis vControl позволяет выполнять следующие (административные) функции:

- заводить учетные записи пользователей, управлять доступом пользователей к системе и ее объектам
- ограничивать доступные пользователям ресурсы с помощью пулов ресурсов
- управлять жизненным циклом виртуальных сред:
  - создавать новые виртуальные среды
  - настраивать конфигурацию виртуальной среды и устанавливать дополнительное ПО в гостевую систему виртуальной среды
  - управлять состоянием работы виртуальной среды: запускать, перезагружать, приостанавливать и выключать
  - управлять правами доступа к объектам виртуальной среды для пользователей или групп пользователей
  - создавать и управлять резервными копиями и снимками виртуальных сред
- осуществлять перемещение виртуальных сред между узлами виртуализации (миграцию)
- группировать виртуальные среды в логическую структуру для упорядочивания работы и последующего делегирования управления
- создавать кластеры и управлять ими:
  - регулировать объем доступных ресурсов в кластере путем изменения его конфигурации
  - отслеживать суммарные значения потребления ресурсов и состояние виртуальных сред, созданных в рамках кластера
- подключать хосты виртуализации и управлять ими:
  - предоставлять физические ресурсы (дисковое пространство, RAM, CPU) для развертывания и работы виртуальных сред
  - просматривать информацию об использовании ресурсов
  - изменять сетевую конфигурацию
- использовать общее хранилище шаблонов виртуальных сред и ISO-образов на всех кластерах, подключенных к системе управления

ПО Basis vControl состоит из следующих программных компонентов:

- **служебная база данных** на основе СУБД PostgreSQL – для хранения информации о виртуальных ресурсах (виртуальные машины, сети), пользователях, группах, ролях, а также информации о узлах вычисления, входящих в кластер, событиях, алертах и т.д. Программные пакеты Patroni и etcd, реализующие механизм высокой доступности кластерной СУБД
- **бэкенд vControl** – основное приложение, реализующее управление платформой Basis vControl. Служит для обеспечения REST API для Фронтенда Basis vControl, взаимодействует с агентами, выполняет периодические задачи
- **агент vControl** – запускается на управляемых узлах вычисления (физических узлах вычисления). Управляет гипервизором, запускает стандартные Linux-команды, а также осуществляет мониторинг состояния узла вычисления и гипервизора

- **менеджер агентов** – осуществляет взаимодействие с агентами vControl, запущенными на физических серверах с установленным гипервизором Р-Виртуализация. Двухсторонний протокол взаимодействия между Менеджером агентов и агентами управления, установленными на хостах, построен на базе библиотеки ZeroMQ
- **хранилище метрик** на основе БД ClickHouse – выполняет хранение значений в первую очередь на хостах. ClickHouse Keeper реализует механизм высокой доступности кластерной СУБД
- **кэш-хранилище** на основе БД Redis – реализует кэш для хранения очереди команд в системе управления, а также выполняет хранение пользовательских сессий и скриншоты ВМ. Служба Redis Sentinel реализует механизм высокой доступности кластерной СУБД
- **WebSocket Server** – обеспечивает двухстороннюю связь между Бэкендом и Фронтендом Basis vControl. После авторизации пользователя Фронтенд Basis vControl устанавливает соединение с WebSocket Server, чтобы получать сообщения о всех изменениях на Бэкенде Basis vControl
- **фронтенд vControl** – реализует WebUI Графический интерфейс, который запускается в браузере пользователя

Все программные компоненты ПО Basis vControl разворачиваются в отказоустойчивой кластерной 4-х узловой конфигурации (3-х узловой для варианта с аппаратной СХД) на виртуальных машинах на узлах вычисления продуктивной нагрузки. Агенты ПО Basis vControl устанавливаются на всех узлах вычисления с гипервизорами.

Узлы вычисления кластера управления обеспечивают вычислительные ресурсы и ресурсы хранения для служебных виртуальных машин. Кластер управления продолжит работу даже после выхода из строя до двух узлов вычисления. Для обеспечения высокой доступности в решении реализована соответствующая функциональность — кластер высокой доступности на уровне гипервизора. В качестве основы он использует собственную разделяемую гиперконвергентную программную систему хранения данных или общую для **Машины** аппаратную СХД.

Для всех служебных виртуальных машин в кластере управления включается функция «высокой доступности». В этом случае соответствующие компоненты в каждом гипервизоре начинают отслеживать доступность каждого узла вычисления в кластере и вести учет того, какие виртуальные машины работают на каждом узле вычисления. В случае отказа узла вычисления, работавшие на нем виртуальные машины также «упадут», но будут перезапущены на прочих узлах вычисления **Машины**, минимизировав тем самым время простоя.

В гипервизоре Р-Виртуализация работает отдельный сервис, обеспечивающий высокую доступность для виртуальных машин. При выборе узла вычисления для перезапуска «упавшей» виртуальной машины реализована логика выбора наименее загруженного. Для проверки соединения Агент vControl с равным интервалом посылает heartbeat-сообщения в сторону Менеджера агентов. При обрыве соединения Агент пытается пересоздать соединение. При пропуске нескольких сообщений подряд Менеджер агентов определяет, что Агент недоступен, устанавливает статус недоступности сервера, а также создает соответствующее уведомление.

Агент vControl использует для управления виртуальной инфраструктурой следующие интерфейсы:

- libvirt — интерфейс библиотеки используется для работы с пробросом физических устройств в ВС и для взаимодействия с QEMU-агентом
- shell — командный интерфейс управления (команды исполняются в консоли сервера)

- NetworkManager — управление сетевой конфигурацией хоста

ПО Basis vControl для управления виртуальной инфраструктурой нескольких вычислительных кластеров **Машины** разворачивается в следующей конфигурации:

- Все служебные роли объединяются на одной виртуальной машине. Запускаются несколько экземпляров таких виртуальных машин (обычно три) в кластерном исполнении

Защита работы сервера управления (виртуальной машины с ролью Basis vControl) от аппаратного отказа обеспечивается функцией высокой доступности (high availability, HA), работа которой не зависит от работоспособности самого ПО Basis vControl. Даже если ВМ сервера управления окажется на узле вычисления, который откажет из-за какого-либо аппаратного сбоя, функция HA отработает и восстановит работоспособность виртуальной машины на одном из доступных узлов вычислительного кластера. Обычно период недоступности в таком сценарии составляет 1–5 минут (в зависимости от конфигурации **Машины** и нагрузки на него).

Защитой от программных отказов самого сервера управления также является его периодическое резервное копирование.

В обеих конфигурациях ПО управления Basis vControl может управлять несколькими вычислительными кластерами **Машины** из единой консоли.

Такая реализация позволяет настраивать единые для всех вычислительных кластеров **Машины** хранилища шаблонов виртуальных машин, а также обеспечивать клонирование/перемещение виртуальных машин между отдельными вычислительными кластерами.

10.3 Basis Workplace

В настоящий момент опциональным продуктом, доступным для использования с **Машиной**, является продукт для организации инфраструктуры виртуальных рабочих мест (Virtual Desktop Infrastructure, VDI) — Basis Workplace.

Инфраструктура виртуальных рабочих мест предполагает набор программного обеспечения, который решает такие задачи, как:

- интеграция с системой виртуализации для развертывания из шаблона и управления жизненным циклом непосредственно виртуальных машин — рабочих мест
- брокер соединений, обеспечивающий подключение пользователей к своим виртуальным рабочим местам и терминальным серверам
- обеспечение протокола доставки удаленных рабочих столов и отдельных приложений. В составе Машины доступен протокол RX, обеспечивающий доставку рабочего стола или приложения с терминальных серверов или виртуальных рабочих мест Linux

Использование BPM требует собственного сайзинга и планирования архитектуры.

10.4 Программная платформа Скала^р Геном

Программная платформа **Скала^р Геном** предназначена для диагностики, мониторинга, обслуживания и управления как отдельным ПАК, так и инфраструктурой, состоящей из множества различных ПАК **Скала^р**. ПО **Скала^р Геном**, 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**

Архитектурно, программная платформа **Скала^р Геном** состоит из следующих сервисных виртуальных машин, вместе образующих программную платформу обслуживания, управления и мониторинга **Скала^р Геном**: ВМ Платформы (сервер управления), ВМ Топологии (сервер топологии, CMDB) и ВМ Мониторинга (**ПО Скала^р Геном** (который, включает в себя компоненты **ПО Скала^р Визион**).

Объектом мониторинга **ПО 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.

Пример интерфейса **ПО Скала^р Геном** приведен на рисунке 9.

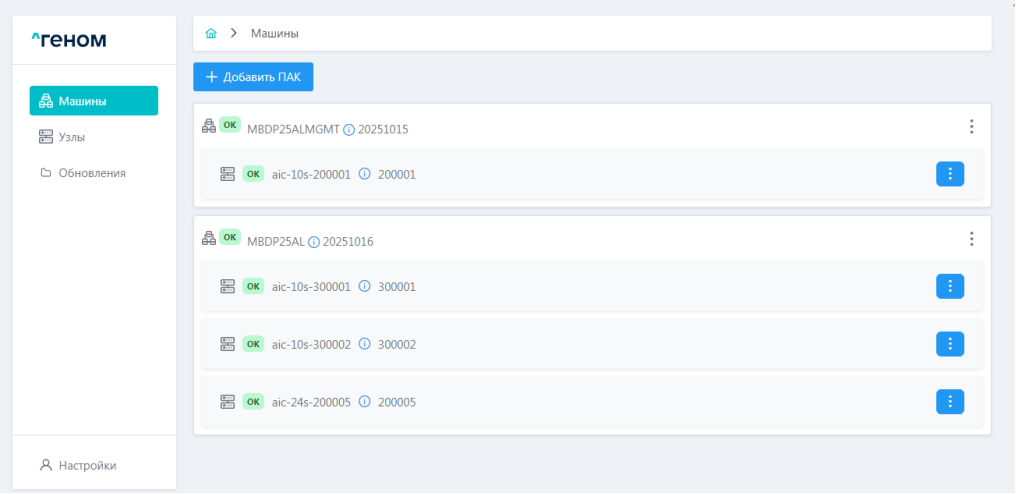

Рисунок 9. Пример интерфейса ПО Скала^р Геном

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.

ПО **Скала^р Геном** позволяет проводить настройку появления новых критических уведомлений, условия их получения гибко настраиваются в соответствии с текущими потребностями (Рисунок 10). Можно управлять формированием почтовых уведомлений: регулировать их группировку, частоту отправки и т.д.

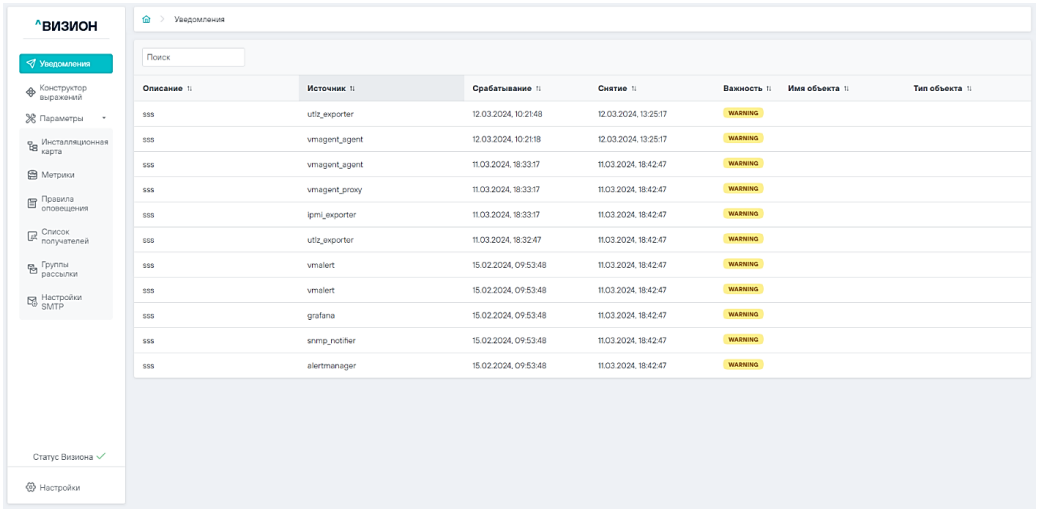

Рисунок 10. Пример интерфейса ПО Скала^р Геном (пример окна настройки уведомлений мониторинга)

10.5 Р-Виртуализация

Гипервизор, программное обеспечение виртуализации, устанавливается на каждом физическом сервере.

ПО Р-Виртуализация является классическим гипервизором на базе open-source решения KVM. Основные свойства:

- поддержка основных операционных систем, включая российские
- полноценное управление жизненным циклом виртуальных машин
- добавление устройств к виртуальной среде в процессе работы: ЦПУ, память, диски, сетевые интерфейсы
- динамическое перераспределение памяти между виртуальными средами для увеличения физически доступной памяти (за счет освобождения неиспользуемой)
- резервное копирование виртуальных сред

ПО Р-Виртуализация позволяет создавать виртуальные машины со следующими характеристиками на виртуальную машину (приведенные значения протестированы и поддерживаются производителем, технически максимальные конфигурации могут быть больше):

- количество виртуальных ядер — до 64 шт.
- объем оперативной памяти — до 1 Тбайт
- объем диска — до 16 Тбайт

10.6 Р-Хранилище

Также на каждом сервере устанавливается программное обеспечение распределенного дискового хранилища. Это ПО позволяет объединить все накопители, установленные в серверах **Машины**, в единое дисковое пространство. Оно используется любой из виртуальных **Машин** и может быть использовано внешним потребителем (по iSCSI). Для данных на этом хранилище доступно резервирование, за счет чего обеспечивается высокая доступность данных и устойчивость к сбоям хранилища при единичных отказах серверов и накопителей.

Основные функции и свойства:

- алгоритмы обеспечения избыточности данных: хранение двух и более реплик данных на накопителях разных хостов комплекса **Машин** или хранение блоков четности/избыточности (Erasure Coding). Немного упрощая, поддерживаются алгоритмы, логически похожие на RAID 1, RAID 6
- поддержка накопителей HDD и SSD с интерфейсами SATA, SAS для получения характеристик, наиболее полно отвечающих вашим требованиям
- гибкие возможности модернизации и обслуживания серверов без прерывания работы
- настройка до 4-х уровней хранения (tier). Файлы-диски виртуальных машин привязываются к одному из уровней хранения, с определенным типом накопителей

11 ВЫСОКАЯ ДОСТУПНОСТЬ И ЗАЩИТА ДАННЫХ

Для обеспечения высокой доступности в решении реализована соответствующая функциональность — кластер высокой доступности. В качестве основы кластер использует гиперконвергентное программно-определяемое хранилище, реализующее высокую доступность данных виртуальных машин.

Для организации резервного копирования реализован сервер резервного копирования, интегрированный в систему управления **Машиной**.

11.1 Кластер высокой доступности

Предполагается, что для узлов вычисления из состава **Машины** включается функция «высокой доступности». В этом случае соответствующие компоненты в каждом гипервизоре начинают отслеживать доступность каждого прочего узла вычисления **Машины** и вести учет того, какие виртуальные машины работают на каждом узле. В случае отказа узла вычисления, работавшие на нем виртуальные машины так же «упадут», но будут перезапущены на прочих узлах вычисления **Машины**, минимизировав тем самым время простоя.

Следует учитывать, что вопрос доступности ВМ находится на стыке собственно функции высокой доступности в гипервизоре и программно-определяемой системы хранения.

Для функции высокой доступности практически несущественно, сколько узлов вычисления откажут одновременно: виртуальные машины будут перезапущены на оставшихся. Но с точки зрения данных виртуальных машин, некоторые из них могут стать недоступны уже при втором-третьем одновременном отказе. Это нормальное поведение системы, и, если будет поставлена задача обеспечить высокую доступность и в случае множественного отказа узлов вычисления, она сможет быть решена путем указания соответствующих политик резервирования данных.

В гипервизоре работает отдельный сервис, обеспечивающий высокую доступность для виртуальных машин.

Эти сервисы, запущенные на каждом из узлов вычисления **Машины**, проверяют доступность друг друга по snmp, тайм-аут недоступности узла — минута.

При выборе узла вычисления для перезапуска «упавшей» виртуальной машины реализована логика выбора наименее загруженного.

11.2 Высокая доступность данных программно-определяемого хранилища

Гиперконвергентная программно-определяемая подсистема хранения **Машины** может реализовывать избыточность данных двумя алгоритмами:

- хранение заданного количества реплик - полных копий данных
- хранение блоков избыточного кодирования (Erasure Coding) на основе кода Рида-Соломона

В первом случае для каждого «блока» данных создается указанное число копий, притом никакие копии этого блока не будут расположены на одном и том же узле (Рисунок 11).

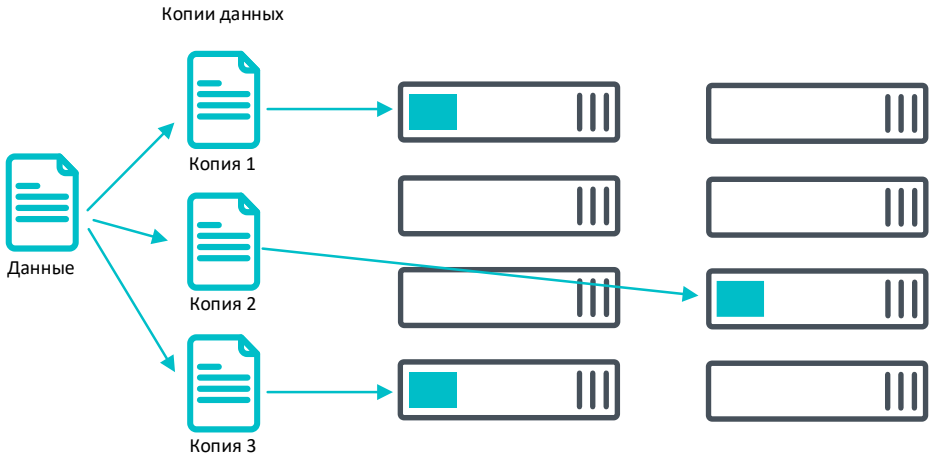

Рисунок 11. Создание реплик, полных копий данных

За счет этого в случае отказа узлов или накопителей в них данные виртуальной машины продолжат оставаться доступными.

Обычно используется политика хранения в 2 или 3 копиях данных.

Во втором случае резервирование обеспечивается добавлением блоков четности/избыточности. Могут использоваться следующие варианты (данные + четность), в зависимости от желаемого уровня доступности и количества хостов в системе: 3 + 2, 5 + 2, 7 + 2. Схема реализации технологии избыточного кодирования для случая 5 + 2 приведена ниже (Рисунок 12).

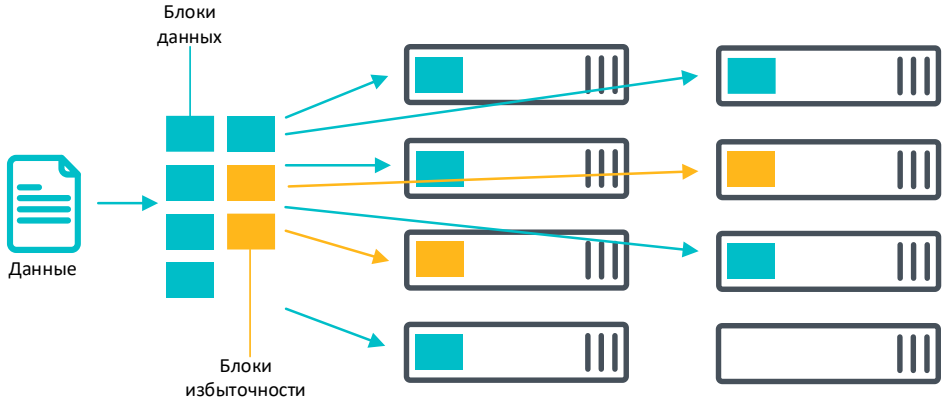

Рисунок 12. Избыточное кодирование 5 + 2

Преимущества и ограничения этих вариантов

Преимущества реализации избыточности данных репликами:

- высокая производительность дисковой подсистемы
- быстрое восстановление недостающих копий данных при отказе одного или двух узлов
- процесс восстановления недостающих реплик практически не влияет на общую производительность дискового хранилища
- чаще целесообразен для небольших комплексов

К недостаткам режима создания реплик можно отнести высокие накладные расходы на хранение данных.

Режим избыточного кодирования позволяет более эффективно использовать дисковое пространство, но у него имеются следующие ограничения:

- для достижения целевой производительности может потребоваться больше накопителей / выбор более быстрых накопителей в некоторых сценариях
- более низкая скорость восстановления недостающих копий данных (rebuild) при потере одного или двух узлов
- дополнительная загрузка процессоров
- для его использования требуется пять узлов и больше

Встроенный инструмент резервного копирования

В сервере управления виртуальной инфраструктурой с ПО Basis vControl реализован встроенный механизм осуществления резервного копирования виртуальных машин.

Доступны выбор ВМ для резервного копирования, управление расписанием автоматизированного резервного копирования, выбор места хранения резервных копий. Поддерживается инкрементальное и полное резервное копирование.

По умолчанию резервные копии хранятся на программно-определяемой системе хранения **Машины**, этого достаточно для защиты от логических ошибок (например, случайного удаления ВМ).

Если модель угроз предусматривает защиту от отказа программно-определяемой системы хранения, то поддерживается и рекомендуется использовать внешнее хранилище резервных копий, с подключением по протоколу NFS, либо применять Модуль резервного копирования для резервного копирования данных, описанный в разделе 8.2.4.

Использование третьих систем резервного копирования также возможно, совместимость конкретных продуктов и версий следует уточнять в документации.

12 ПОСТАВКА И ЛИЦЕНЗИРОВАНИЕ ПО В СОСТАВЕ МАШИНЫ

Необходимое программное обеспечение **Машины** поставляется исключительно в составе данного ПАК и лицензируется по метрикам комплекса в соответствии с его размером.

Основное функциональное ПО (Таблица 5) лицензируется в составе Лицензионного пакета Модулей, составляющих **Машину** (и может облагаться нулевым НДС).

Специализированное и системное ПО входит в структуру Модулей и **Машины**, и не выделяется в обособленный пакет. Таблица содержит информацию о номенклатуре данного ПО.

На состав лицензируемого ПО, эксплуатируемого в составе **Машины**, также влияет выбор в пользу защищенного исполнения функционального ПО виртуализации (сертифицированная ФСТЭК версия). Кроме того, выбор типа применяемой системы хранения, а именно: гиперконвергентного программно-определяемого распределенного хранилище данных либо аппаратной СХД, используемой для организации постоянного хранилища, также учитывается при формировании необходимого лицензионного пакета. Необходимая для заданного уровня расширенной гарантии на ПАК техническая поддержка входит в лицензии.

Ниже приведен перечень ключевых компонентов Лицензионного пакета **Машины** (Таблица 5).

Специализированное и системное ПО в составе **Машины** приведено в таблице 6.

Таблица 5. Компоненты Лицензионного пакета

Краткое наименование компонента	Назначение	Единица лицензирования
ПО **Скала^р Геном**. Лицензия на систему эксплуатации инфраструктур на базе **Машин Скала^р**	ПО обеспечения эксплуатации инфраструктур на базе **Машин Скала^р**, а также развертывания, управления, мониторинга и конфигурации	Узел вычисления /сетевой узел в составе ПАК
Basis vControl P-Виртуализация	Обеспечение виртуализации серверных систем (сервер управления входит в эту лицензию)	Процессор (сокет)
Basis vControl P-Хранилище	Реализация распределенного дискового массива	Тбайт полезной ёмкости
Basis Workplace	Система виртуализации рабочих мест	Именованные пользователи или конкурентные сессии

Краткое наименование компонента	Назначение	Единица лицензирования
Лицензия на ПО Basis vControl, стартовый пакет	ПО серверной виртуализации	На 1 ПАК

Таблица 6. Специализированное и системное ПО в составе ПАК

Краткое наименование компонента	Назначение	Единица лицензирования
ОС **Астра** или ОС **Альт Сервер**, с подсистемой виртуализации, сертифицированные версии	ОС узлов для запуска служебных виртуальных машин (компонентов Геном, включая мониторинг, обслуживание и др.)	Узел вычисления
ПО Системы единой аутентификации **Машин Скала^р Avanpost FAM**	*Опционально*: организация универсальной сертифицированной платформы авторизации и аутентификации (IAM) в составе ПАК при отсутствии ее аналогов в инфраструктуре заказчика	4 процессорных ядра, специальная облегченная лицензия только для ПАК **Скала^р**, не более 100 учетных записей

Собственное ПО **Скала^р** и специальные лицензии только для ПАК **Скала^р** поставляются исключительно и только в составе ПАК **Скала^р**.

13 ГАРАНТИРОВАННОЕ КАЧЕСТВО

Качественные показатели **Машины** 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
- первичное развертывание ПО осуществляется в автоматическом режиме
- дополнительные настройки ПО осуществляются в соответствии с утвержденной методикой и пошаговой инструкцией
- осуществляется функциональное тестирование сформированной **Машины**
- отклонения от типового решения **Машины** исключены

Передача в эксплуатацию

- **Машина** полностью сформирована, протестирована, готова к размещению в сети заказчика и размещению прикладного ПО
- в комплекте с **Машиной** передаются паспорт, сертификат на поддержку
- проводится обучение специалистов заказчика работе с **Машиной** (по запросу)

Поддержка

- **Машина** 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 **Скала^р** или сертифицированным партнером **Скала^р**
- у заказчика есть возможность выбора варианта поддержки (9x5 или 24x7)
- в сложных случаях в решении проблем на третьей линии поддержки участвуют архитекторы и инженеры, разработчики ПО и **Машины**

Дополнительные требования

Возможна реализация дополнительных требований по модернизации или развитию **Машины** (по запросу), в том числе:

- аппаратная модернизация решения
- горизонтальное или вертикальное масштабирование нового или имеющегося решения
- изменение функциональности компонентов дистрибутивов ПО, их доработка
- тестирование приложений, производительности приложений или иное другое запрошенное тестирование

Работы выполняются с участием архитекторов и инженеров, команды разработчиков аппаратной части и программного обеспечения **Машины** и ПО **Скала^р МСП.ТП**.

14 ТРЕБОВАНИЯ К РАЗМЕЩЕНИЮ

Изделие представляет собой серверный монтажный шкаф 19”, высота 42U, с дальнейшей возможностью модульной расширяемости.

Наполнение шкафа оборудованием и совокупный вес зависят от выбранного варианта решения.

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

Расчетная потребляемая мощность шкафа составляет от 6 до 11 кВт.

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

Требования для подключения **Машины** к локальной сети заказчика определяются на этапе формирования спецификации **Машины**.

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

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

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

15 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Поставка **Машины** осуществляется с предварительными сборкой, тестированием и настройкой оборудования согласно требованиям заказчика. Качественная поддержка **Машины** обеспечивается едиными стандартами гарантийного и постгарантийного технического обслуживания:

- пакет услуг по технической поддержке на первый год включен в поставку
- заказчик может выбирать пакет в базовом режиме 9x5 или в расширенном режиме 24x7 (опция для критической функциональности)
- срок начально приобретаемой годовой технической поддержки может быть увеличен до 3 и 5 лет, также доступна пролонгация поддержки по окончании сроков
- возможно включение в состав стандартных пакетов дополнительных опций и услуг

Состав типовых пакетов услуг по технической поддержке представлен в таблице ниже (Таблица 7).

Таблица 7. Пакеты услуг по технической поддержке Скала^р

Услуга	Пакет «9x5»	Пакет «24x7»
Режим «Обслуживание комплекса **Скала^р** в режиме 9x5» (в рабочее время по рабочим дням)	+	–
Режим «Обслуживание комплекса **Скала^р** в режиме 24x7» (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	+	+

Услуга	Пакет «9x5»	Пакет «24x7»
Доставка оборудования на замену за счет производителя	+	+
Расширенные опции обслуживания	–	+
Времена реагирования и отклика, не более:		
Время регистрации обращений	30 минут, рабочие часы (9x5)	30 минут, круглосуточно (24x7)
Подключение специалиста к решению инцидентов критичного и высокого уровней	В течение 1 рабочего часа (9x5)	В течение 1 часа (24x7)

Примечание к срокам ремонта оборудования

Машина архитектурно является устойчивой 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 **Машине** предусмотрено как минимум двойное резервирование основных компонентов, позволяющее сохранять данные и работоспособность даже при выходе из строя нескольких дисков и/или узлов вычисления (серверов).

Полное описание услуг поддержки доступно на сайте skala-r.ru.

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.