Deckhouse
ФЛАНТ

Современная инфраструктура по требованиям ФСТЭК России

Контейнеризация, виртуализация и единое управление

Deckhouse
ФЛАНТ

Спикеры

Георгий Дауман

Владелец продукта Deckhouse Virtualization Platform

georgy.dauman@flant.com

Ильдар Гарипов

Руководитель отдела информационной безопасности

ildar.garipov@flant.com

План вебинара

01 О «Фланте» и вендоре Deckhouse

02 Безопасная платформа для ВМ и контейнеров

03 Кейсы использования

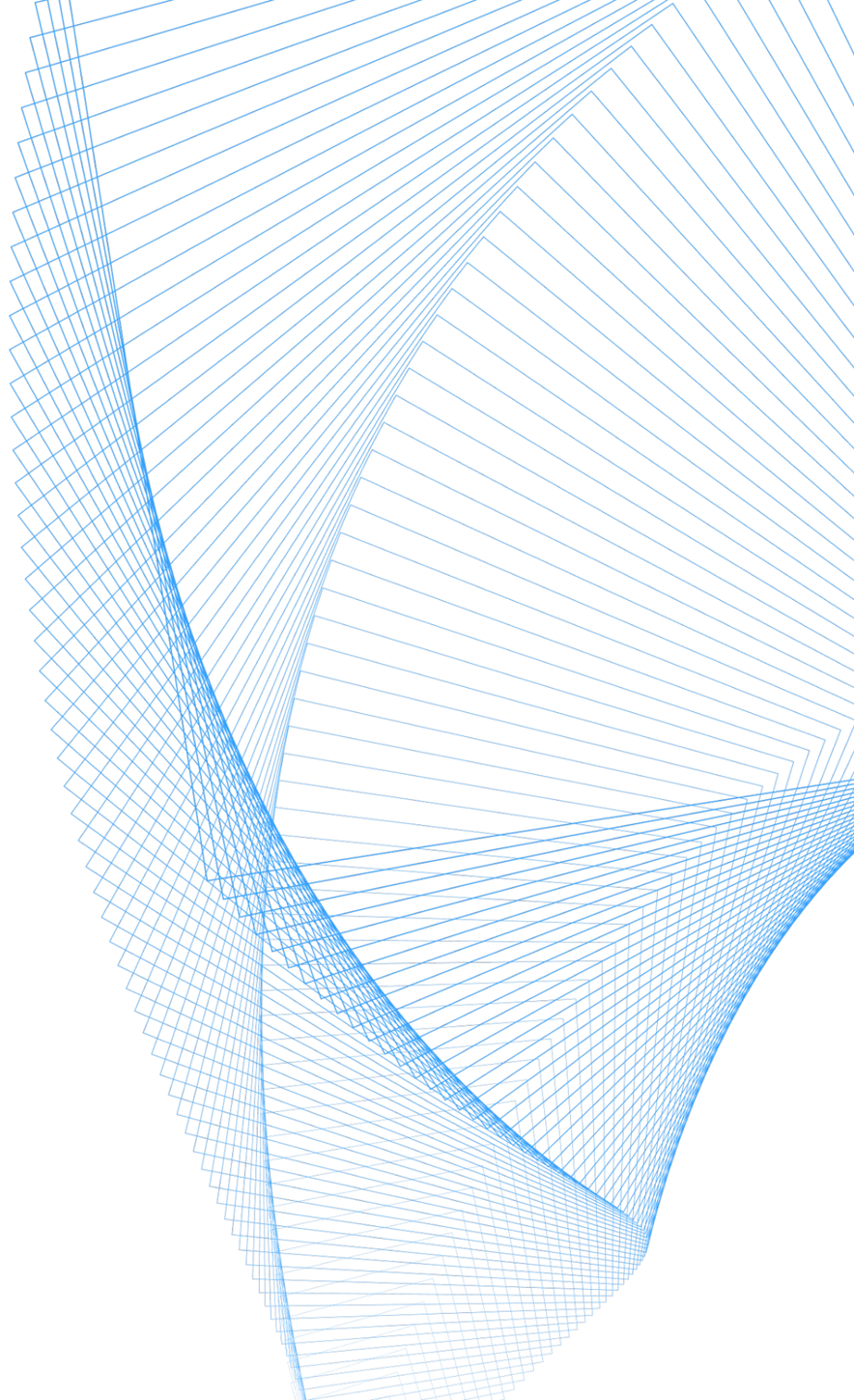
04 Сценарии применения

05 Изменения в сертифицированной редакции

06 Меры защиты и функции безопасности

07 Эволюция платформы

08 Новые возможности



ФЛАНТ

Синергия опыта вендора, интегратора, сервисной и консалтинговой компании

Deckhouse

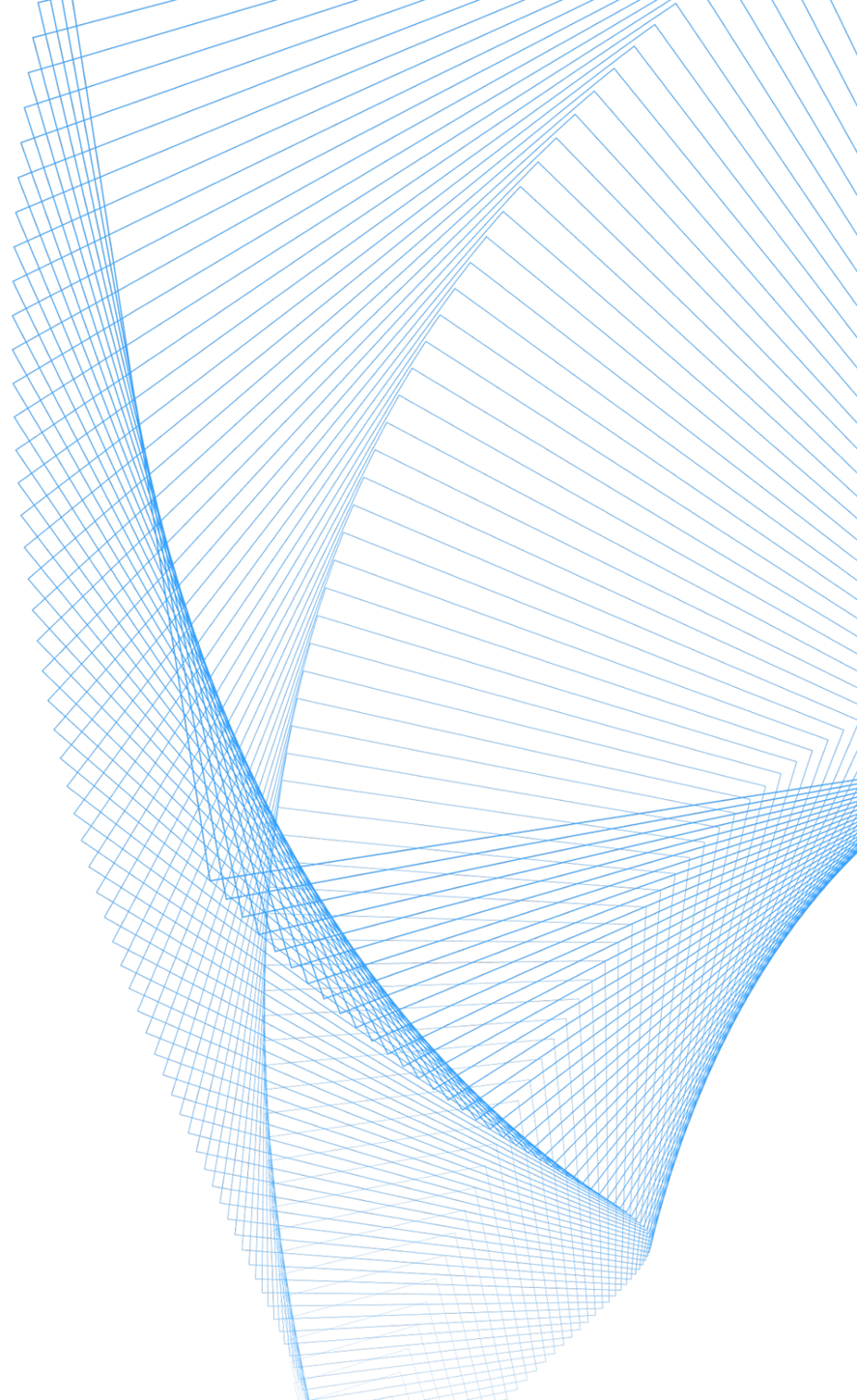
Deckhouse — продуктовое подразделение, разработчик продуктов для построения надёжной enterprise-инфраструктуры

DaaS

DaaS — комплексное DevOps-сопровождение инфраструктуры в режиме 24/7 силами выделенной DevOps-команды

Экспресс 42

«Экспресс 42» — DevOps-консалтинг.
От анализа узких мест в ИТ-процессах до создания роадмапа изменения ИТ для реализации цифровой трансформации



О вендоре Deckhouse

17+
лет опыта в Open Source

500+
сотрудников

С 2017
года используем
Kubernetes в production

№1
контрибьютор
в проекты CNCF из России

>260
компаний-
пользователей

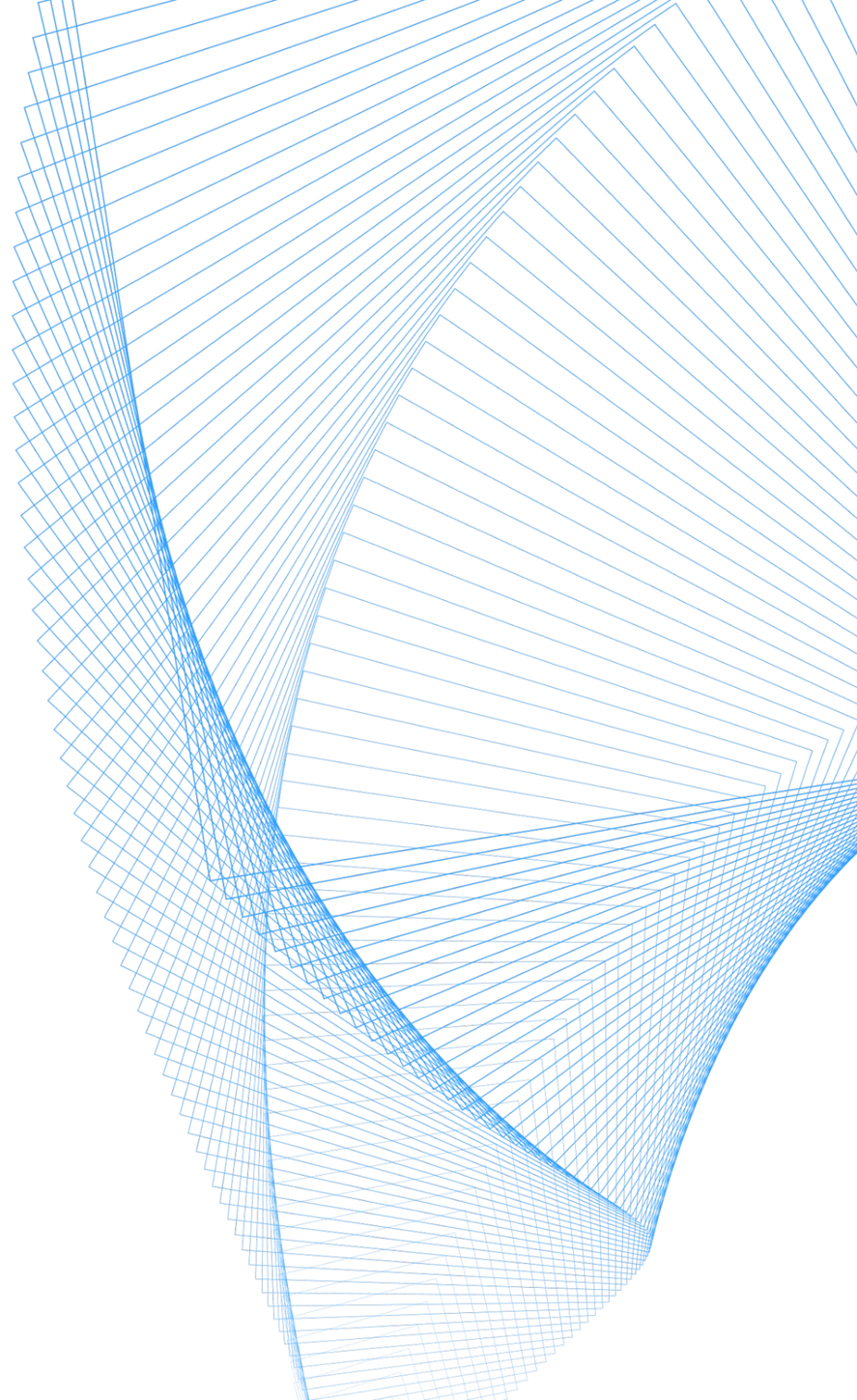
В топе
вендоров ИТ-решений
для банков и промышленности

Реестр
российского ПО

Сертификаты
ФСТЭК России

АРПП
«Отечественный софт»

Лицензии ФСБ России
и ФСТЭК России



* Рейтинг «Крупнейшие ИТ-вендоры в банках», T-Adviser, 2024 год

** Рейтинг «Крупнейшие ИТ-вендоры в промышленности», T-Adviser, 2024 год

Deckhouse
Kubernetes Platform

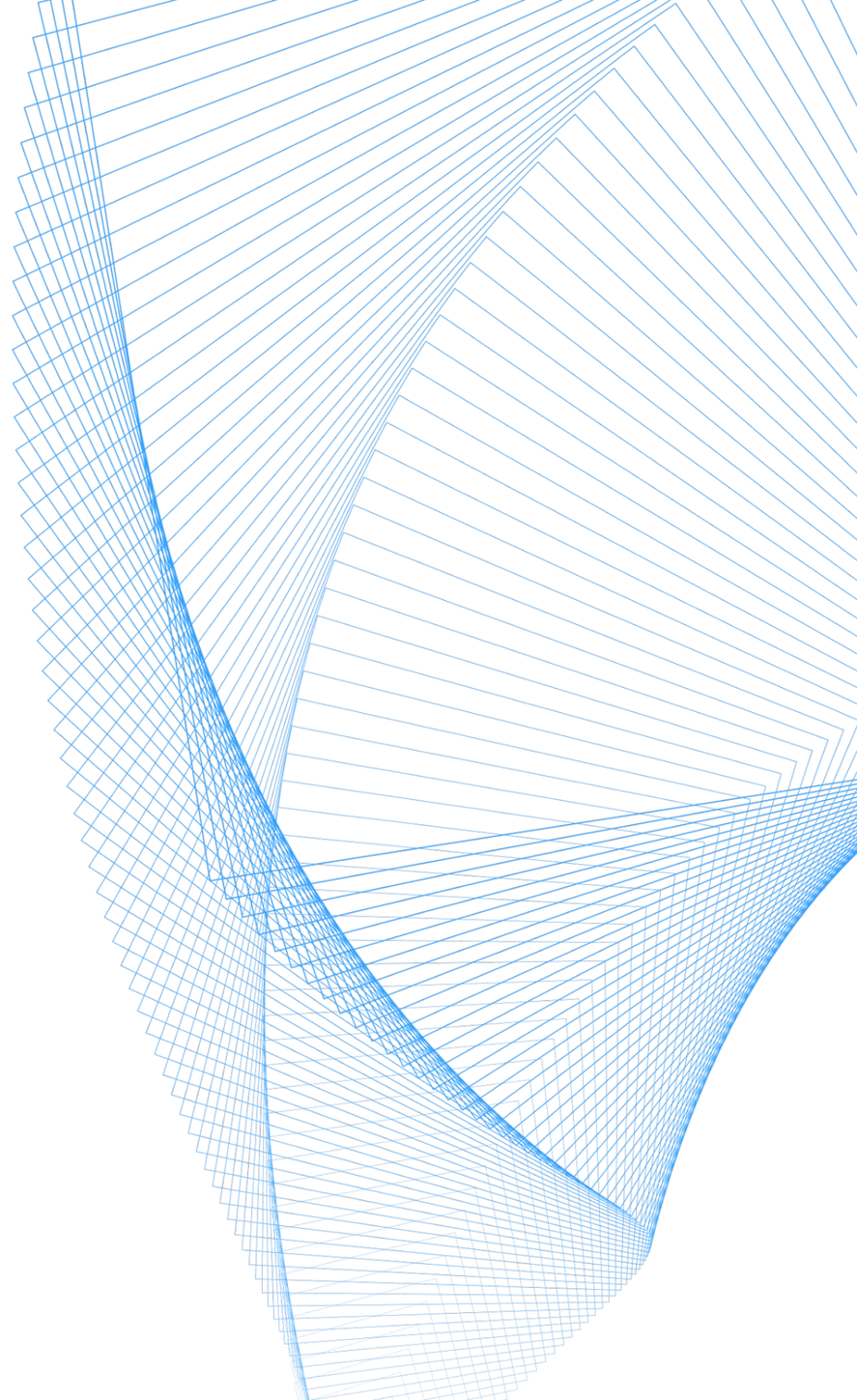
Deckhouse
Virtualization Platform

Единственное на рынке решение для создания гибридных инфраструктур, в котором виртуальные машины и контейнеры управляются как единое целое из одной панели

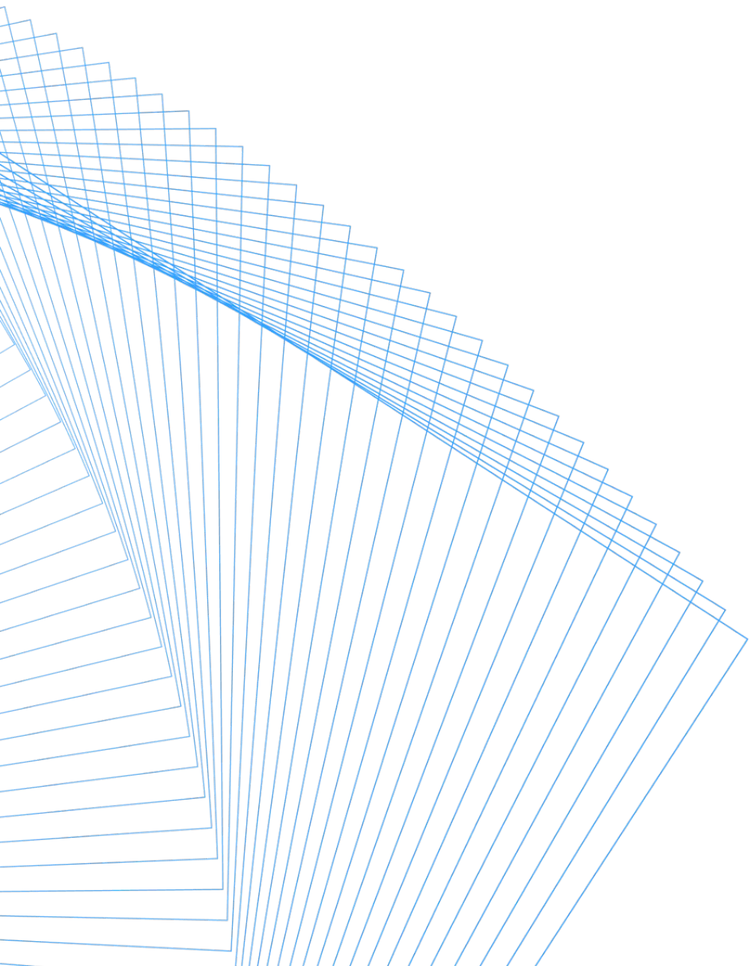
- Запуск виртуальных машин в одной среде с контейнерами
- Управление любыми пользовательскими нагрузками из одного веб-интерфейса
- Использование современных DevOps-практик для управления конфигурациями и их контроля

Первая в России платформа, объединяющая два класса продуктов, которая сертифицирована ФСТЭК России

- Упрощение масштабирования: сертификат покрывает разные сценарии использования
- Централизованное управление безопасностью для любых типов нагрузок



Кейсы использования



Кейс

Федеральное казначейство

Вызовы

Подсистема управления доходами в ГИИС «Электронный бюджет» базировалась на зарубежной ERP-системе oracle E-Business Suite с децентрализованным принципом развёртывания

Задачи

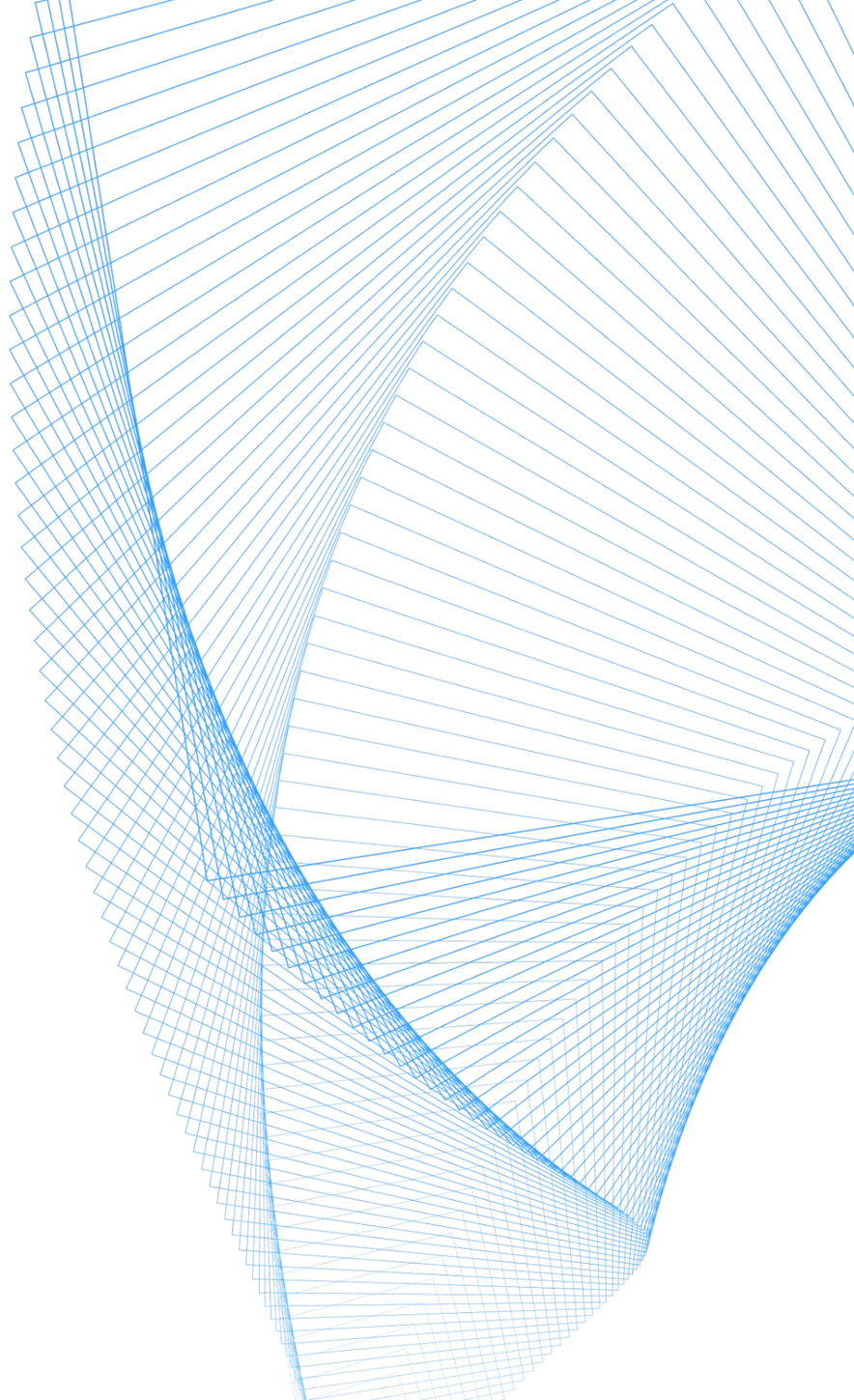
Разработать новую подсистему, интегрировать её с действующими системами и выполнить миграцию данных в масштабах страны без прерывания рабочих процессов, обеспечив бесперебойность и безопасность

Решения

«ОТР 2000» и «Флант» создали новую гибкую, отказоустойчивую систему на микросервисной архитектуре, используя актуальный стек и сертифицированное отечественное ПО

Результаты

Применение Deckhouse Kubernetes Platform CSE (DKP CSE) обеспечило необходимую производительность, динамическое масштабирование и отказоустойчивость системы при полном соблюдении требований информационной безопасности



Кейс

ФГБУ «Росгеолфонд»

Вызовы

Информационная система недропользования ФГБУ «Росгеолфонд» — объект критической информационной инфраструктуры (КИИ), требующий модернизации и повышения безопасности данных

Задачи

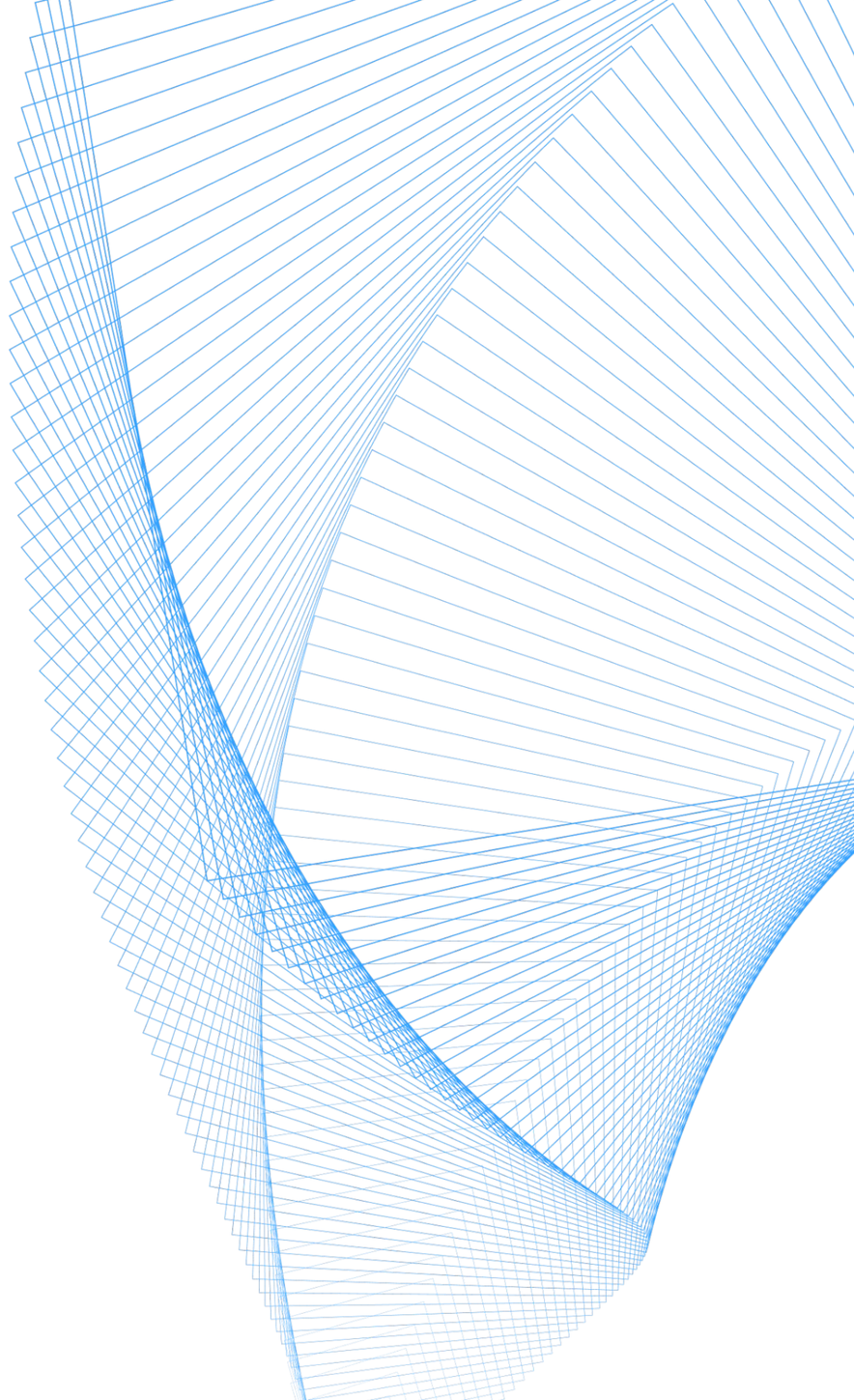
Обеспечить соответствие требованиям регулятора к объектам КИИ РФ, включая предотвращение неправомерного доступа к информации

Решения

Миграция системы на инфраструктуру под управлением сертифицированной ФСТЭК России платформы Deckhouse Kubernetes Platform CSE (DKP CSE)

Результаты

Модернизированная система на базе DKP CSE стабильно функционирует и полностью соответствует требованиям регулятора и отрасли в сфере безопасности



Кейс

АО «Флант»

Вызовы

Высокие расходы на публичные облака (1,5–3 млн руб./мес.), отсутствие стандартов разработки у 40 команд, сложность биллинга и контроля доступа

Задачи

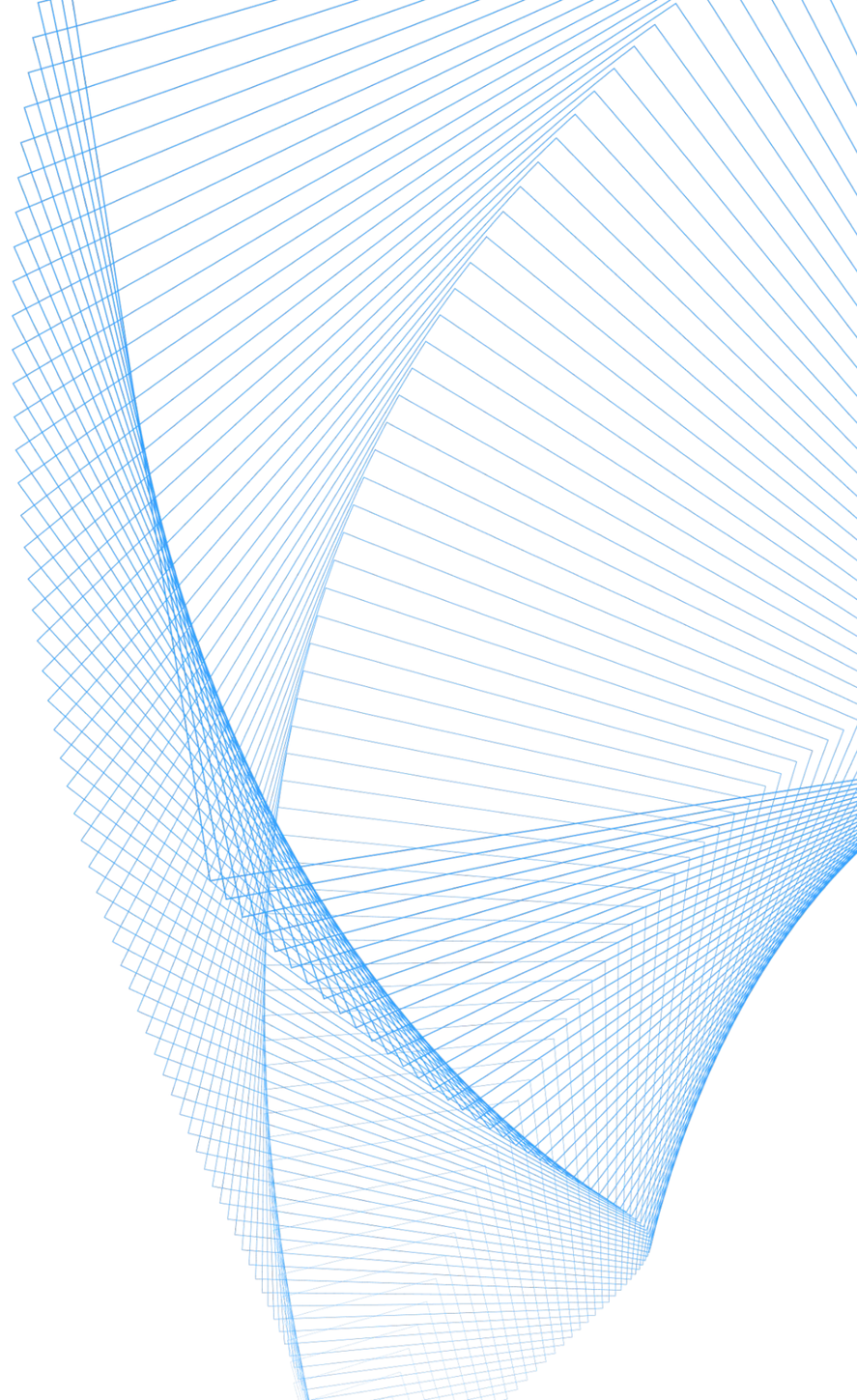
Снижение OPEX, стандартизация безопасности, ускорение создания окружений без расширения штата

Решения

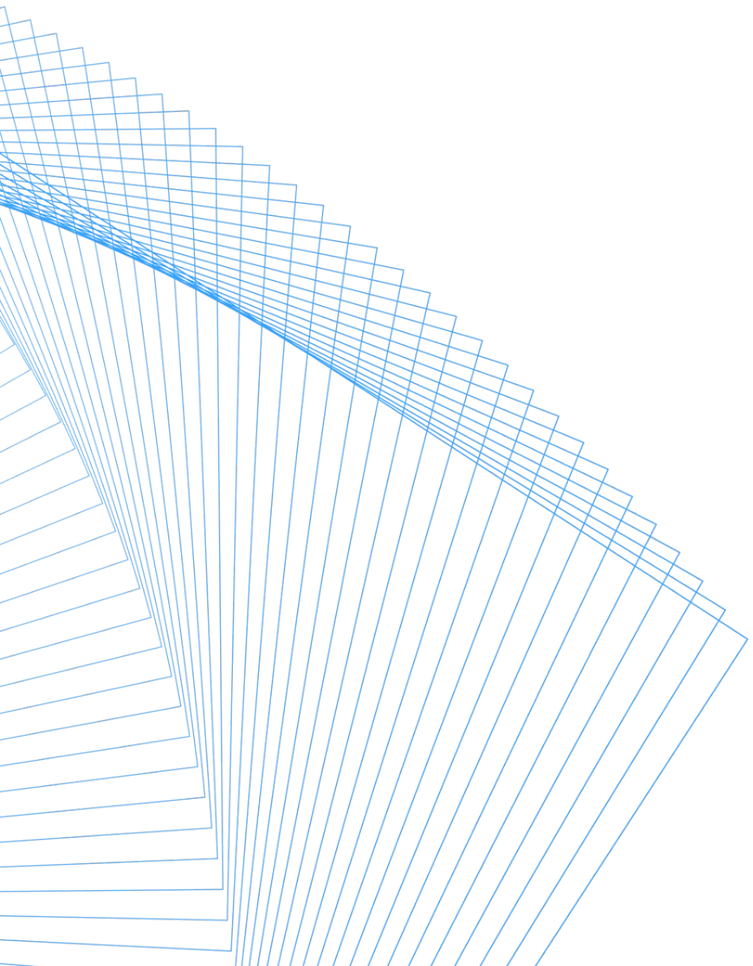
Частное облако на базе Deckhouse Virtualization Platform и Deckhouse Commander. Инфраструктура: 20 гипервизоров, >500 ВМ, >100 кластеров DKP, 50+ проектов. Автоматизация и модель самообслуживания с помощью Deckhouse Commander

Результаты

Окупаемость проекта — 1 год. Рост инфраструктуры в 2 раза за полгода при поддержке двумя инженерами (3 часа в день). Развёртывание кластера Deckhouse — 15 минут. Единый стандарт сред и безопасный доступ



Сценарии применения



Сценарий | Нефтегазовая компания

Лёгкая виртуализация

Ситуация

Обновление парка оборудования в распределённых ЦОДах
для запуска локальных приложений на базе ВМ и контейнеров

Задачи

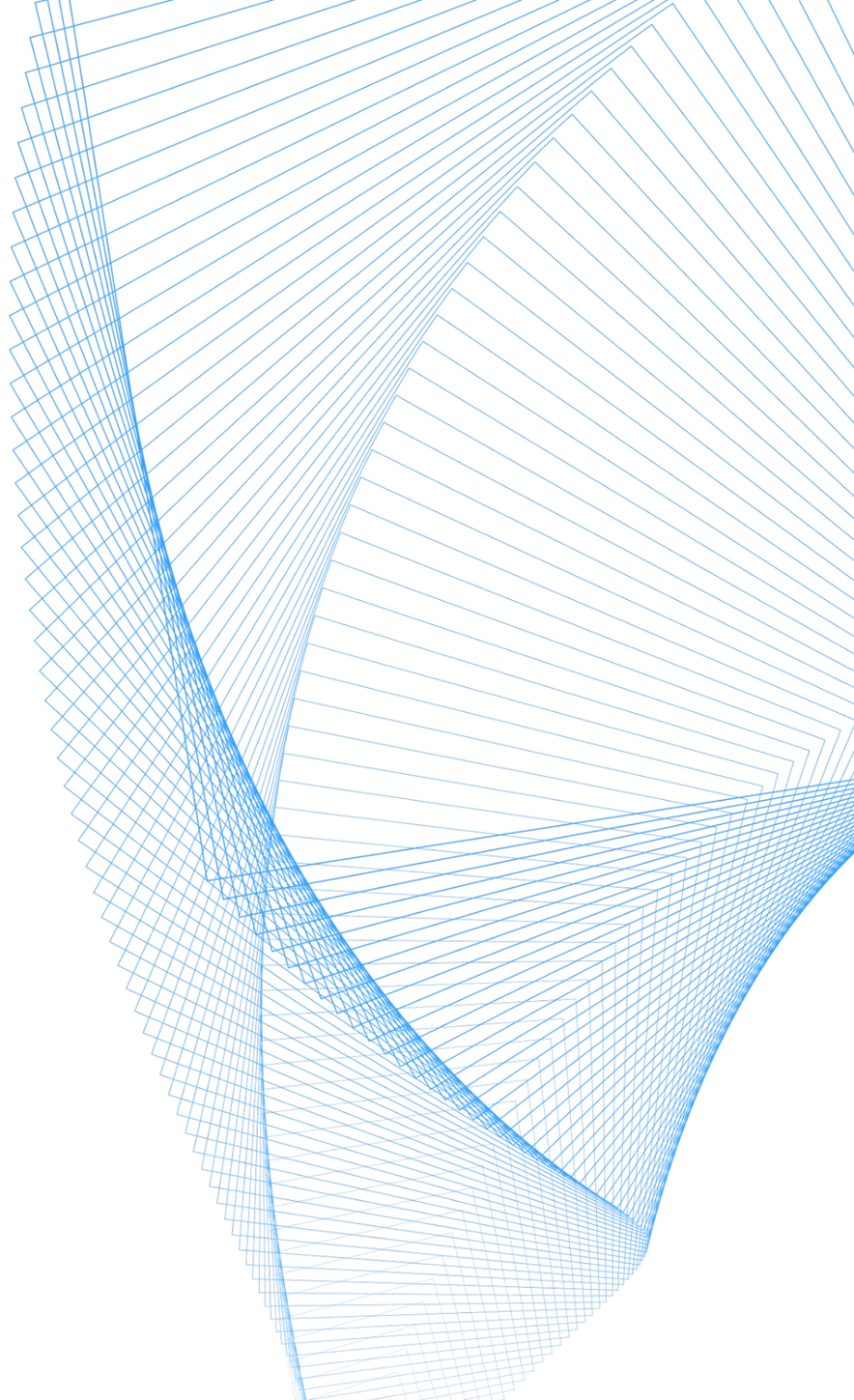
- Более эффективное использование ресурсов (снижение оверхеда)
- Централизованное управление платформой, сетью и хранилищем

Решения

DVP как платформа виртуализации + Commander
для централизованного управления

Ожидаемый результат

- Улучшение доступности за счёт централизованной поддержки от вендора
- Снижение Time to Market за счёт использования декларативного подхода к развёртыванию ВМ
- Снижение ФОТ за счёт объединения команды эксплуатации



Сценарий | Образовательное учреждение

Миграция с VMware vSphere

Ситуация

Унаследованная платформа виртуализации
VMware vSphere для работы приложений на ВМ
и микросервисных приложений в Docker

Задачи

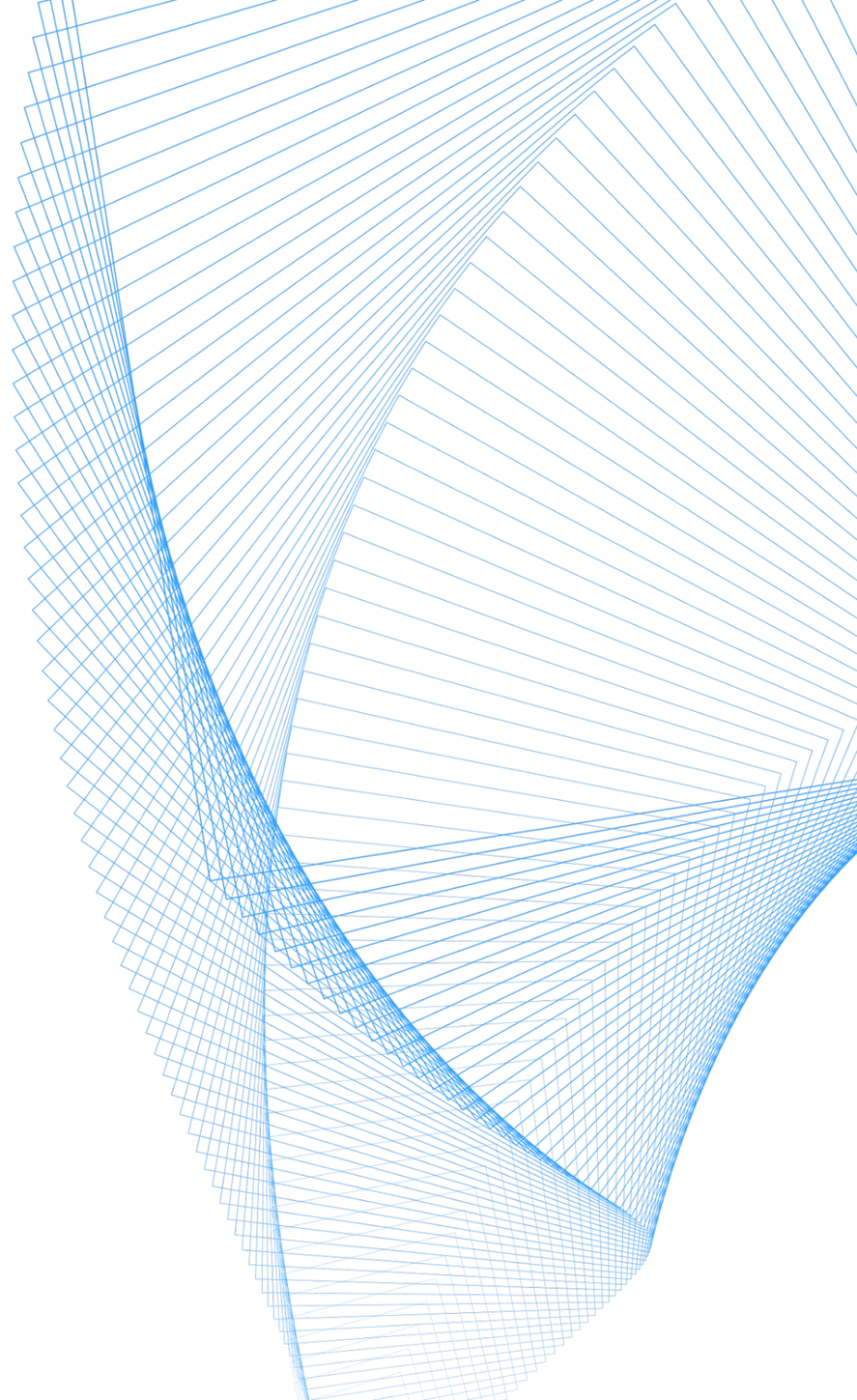
Миграция на российскую платформу виртуализации
с последующим переходом на микросервисную архитектуру

Решения

Постепенный перенос ВМ на DVP
и контейнеризация приложений в одной среде
исполнения с единым веб-интерфейсом

Ожидаемый результат

- Соответствие требованиям
  по импортозамещению инфраструктуры
- Централизованное управление безопасностью
  Всех систем, плавный переход от монолитной
  к микросервисной архитектуре



Сценарий | Крупный банк

Миграция с OpenStack на Cloud Native-виртуализацию

Ситуация

Сложная поддержка и обновление платформы на базе OpenStack

Задачи

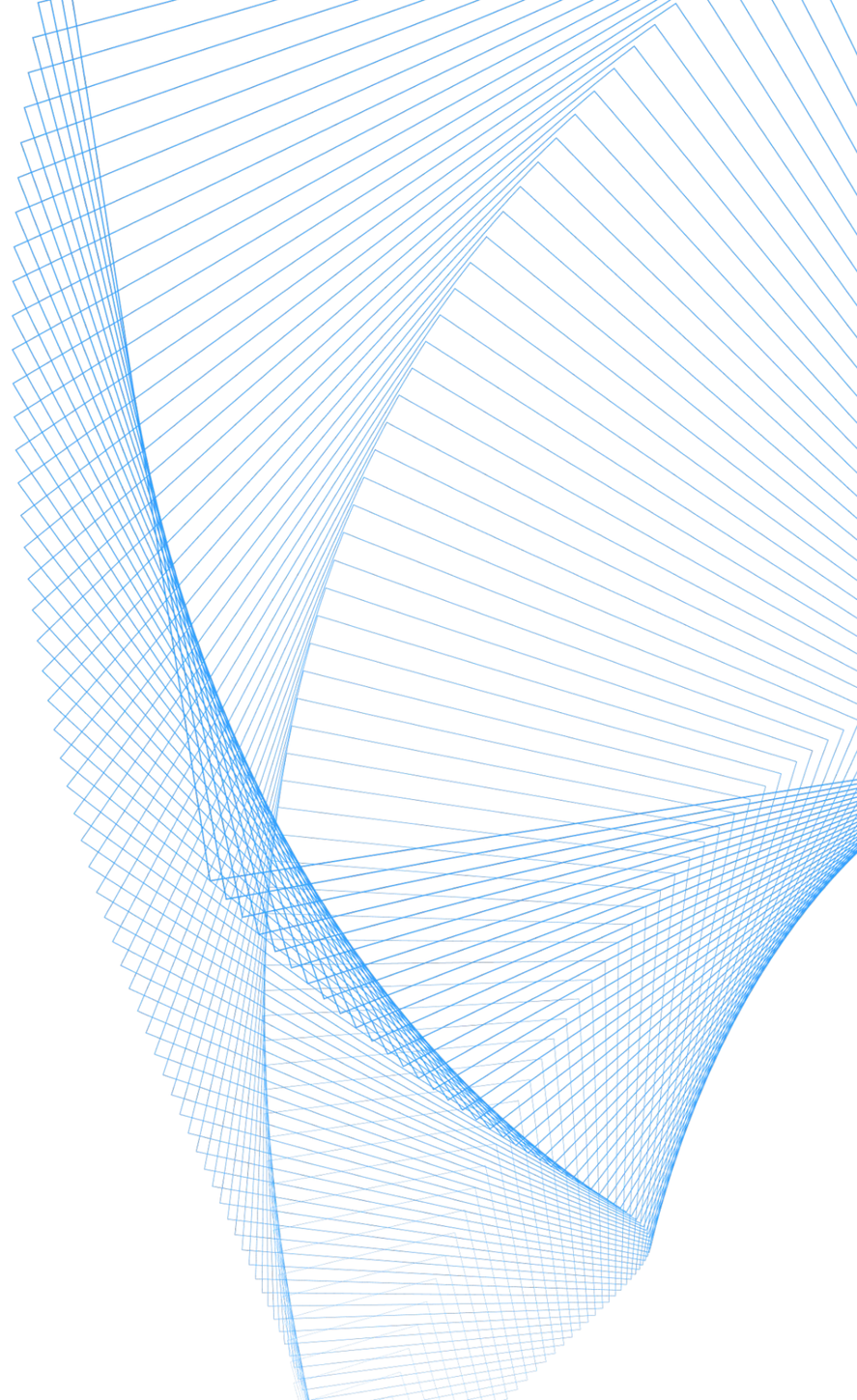
Создать фундамент для частного облака и унифицировать подход для управления BM и контейнерами

Решения

DVP для стандартизации подхода к управлению с использованием единого API, мониторинга и политик безопасности

Ожидаемый результат

- Предсказуемый процесс обновления платформы и поддержка от вендора
- Сквозная наблюдаемость для инфраструктуры и приложений
- Упрощение автоматизации благодаря использованию DevOps-подходов



Сценарий | Промышленное предприятие

Промышленные системы в производственных контурах

Ситуация

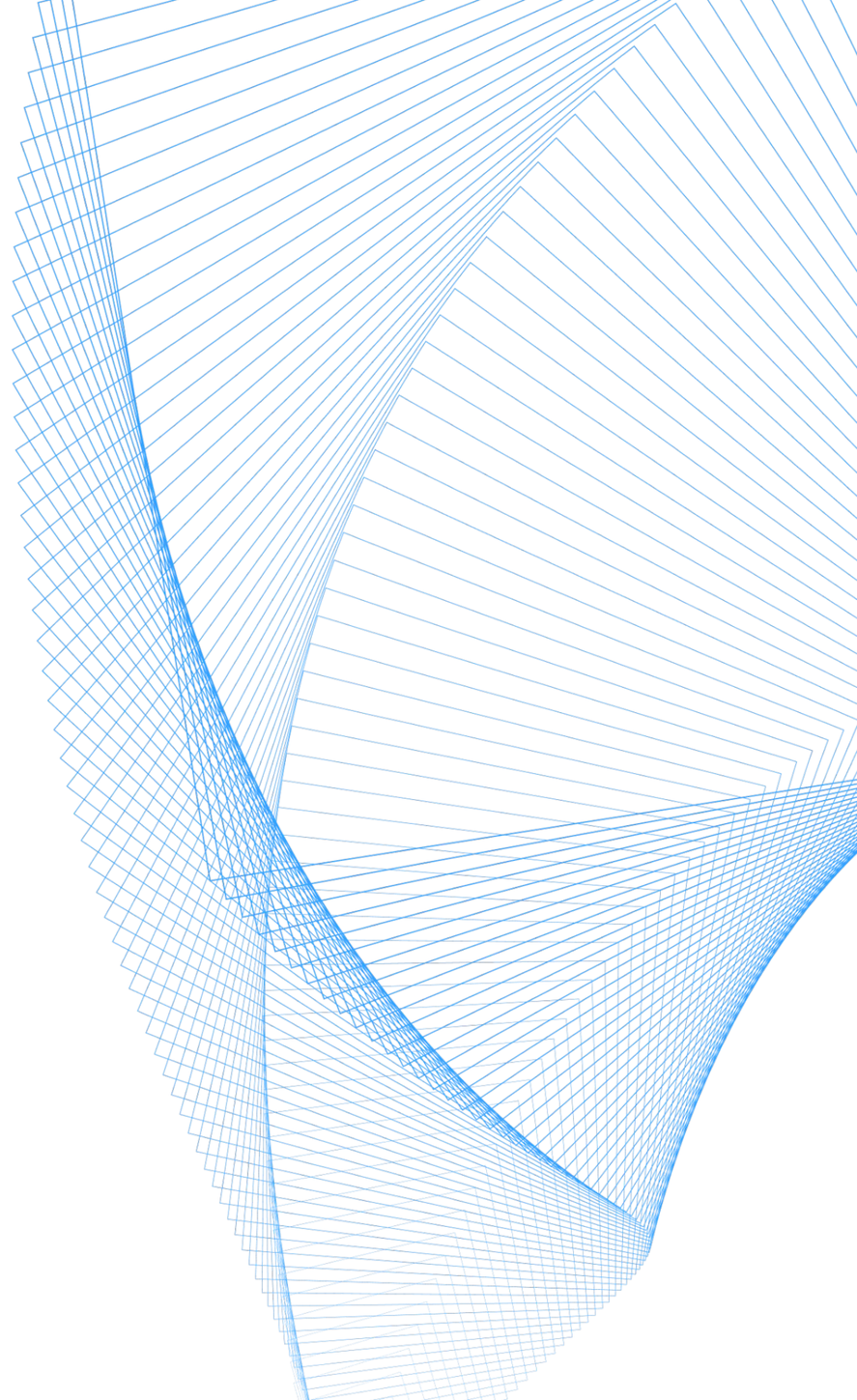
Требуется изолировать АСУ ТП и MES-системы от корпоративной сети

Решения

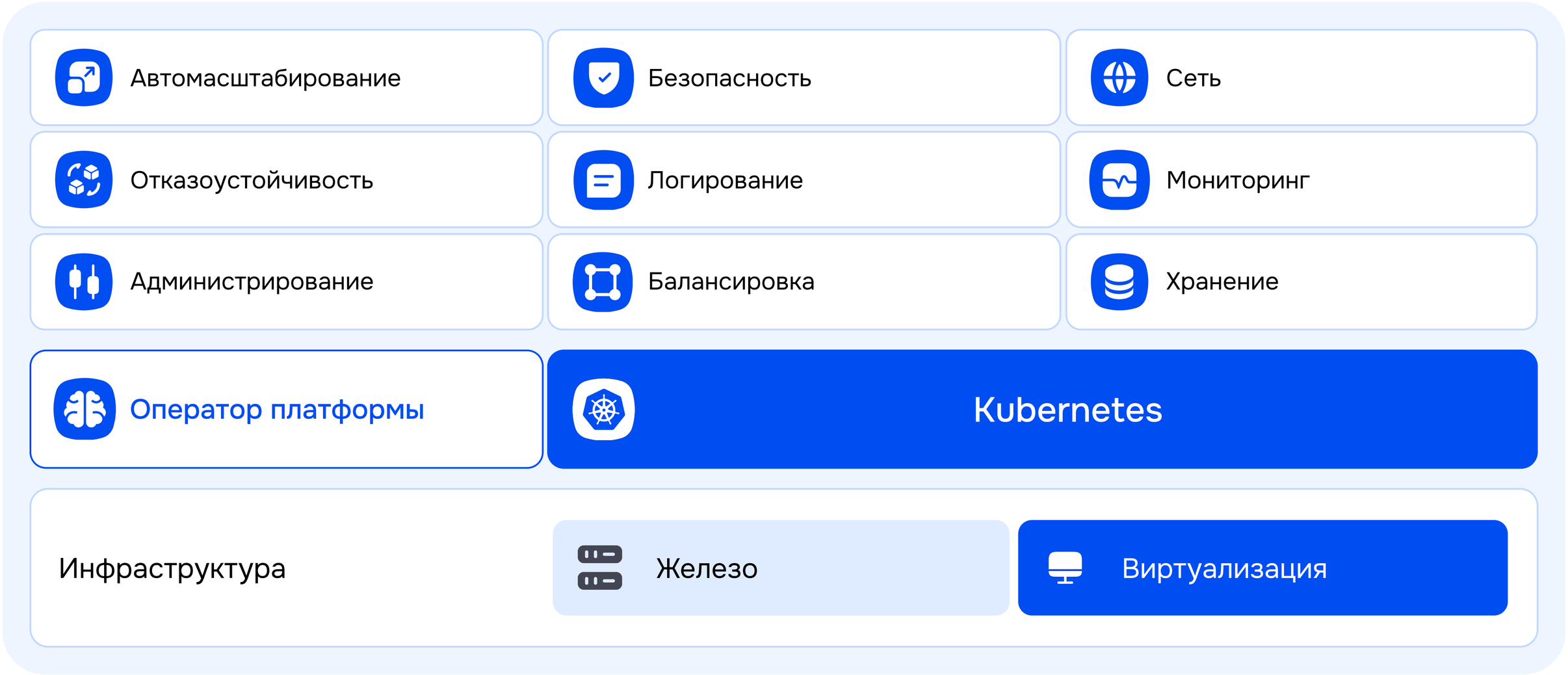
DKP и Commander для работы микросервисной MES-системы и BM для БД и репозитория в закрытом контуре

Ожидаемый результат

- Соответствие требованиям безопасности промышленных систем
- Изоляция производственного контура с доказательной базой
- Централизованное управление безопасностью распределённых приложений



Состав Deckhouse Kubernetes Platform CSE



Сертификат ФСТЭК России № 4860 от 4 октября 2024 г.

Переоформлен:
23 марта 2026 года

С октября 2024 года выпущено уже четыре версии сертифицированной редакции DKP

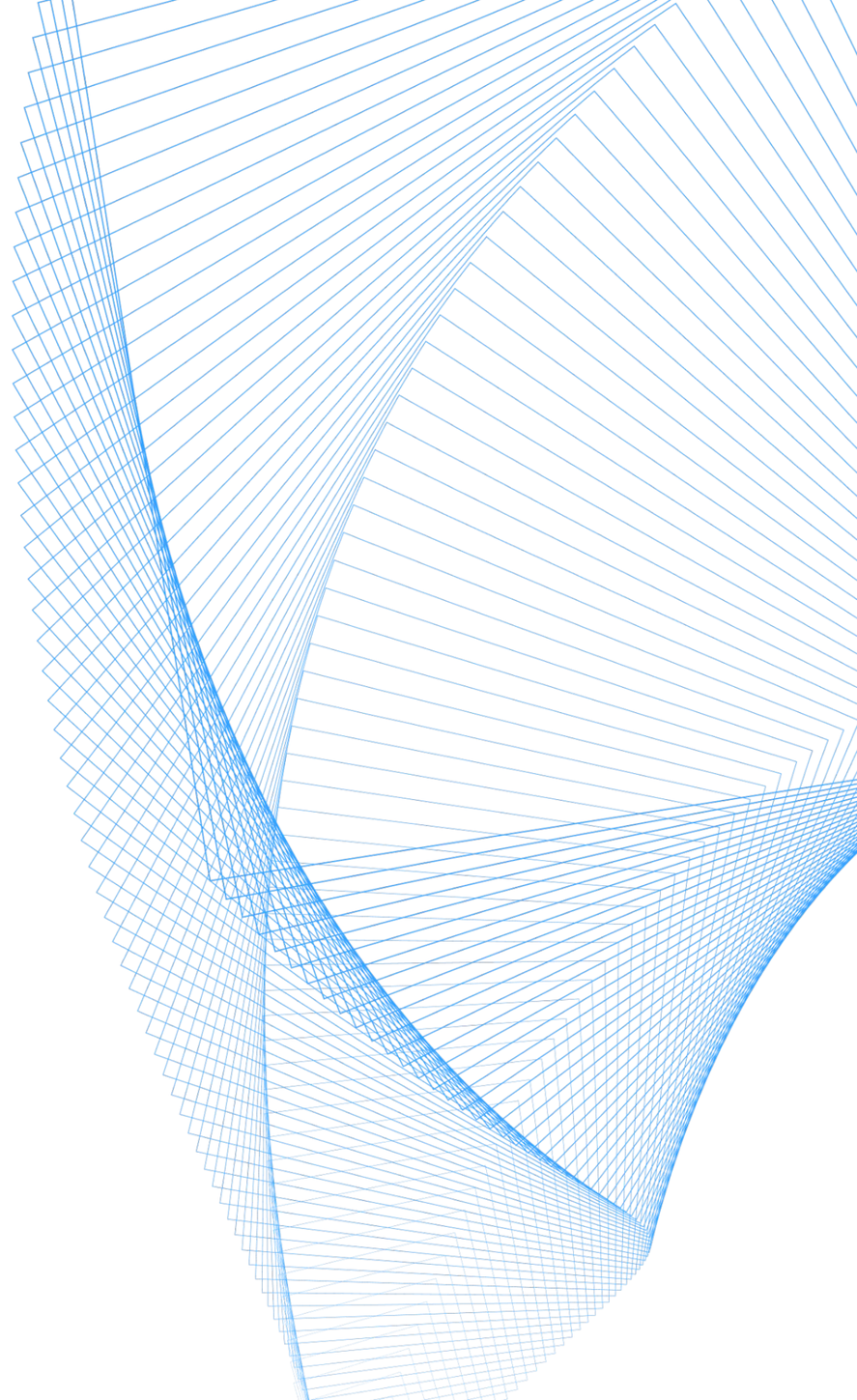
Подтверждает соответствие:

- Требованиям по безопасности информации к средствам контейнеризации (утверждены приказом ФСТЭК России № 118 от 4 июля 2022 г.) – по 4-му классу защиты
- Требованиям по безопасности информации к средствам виртуализации (утверждены приказом ФСТЭК России № 187 от 27 октября 2022 г.) – по 4-му классу защиты
- Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (утверждены приказом ФСТЭК России № 76 от 2 июня 2020 г.) – по 4-му уровню доверия

Deckhouse Kubernetes Platform Certified Security Edition

Безопасность:

- Информации на значимых объектах критической информационной инфраструктуры до 1-й категории значимости включительно
- Персональных данных в информационных системах до 1-го уровня защищённости включительно
- Информации в государственных информационных системах до 1-го класса защищённости
- Информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, до 1-го класса защищённости включительно



Варианты исполнений

DKP CSE поставляется в следующих исполнениях:

Исполнение 1

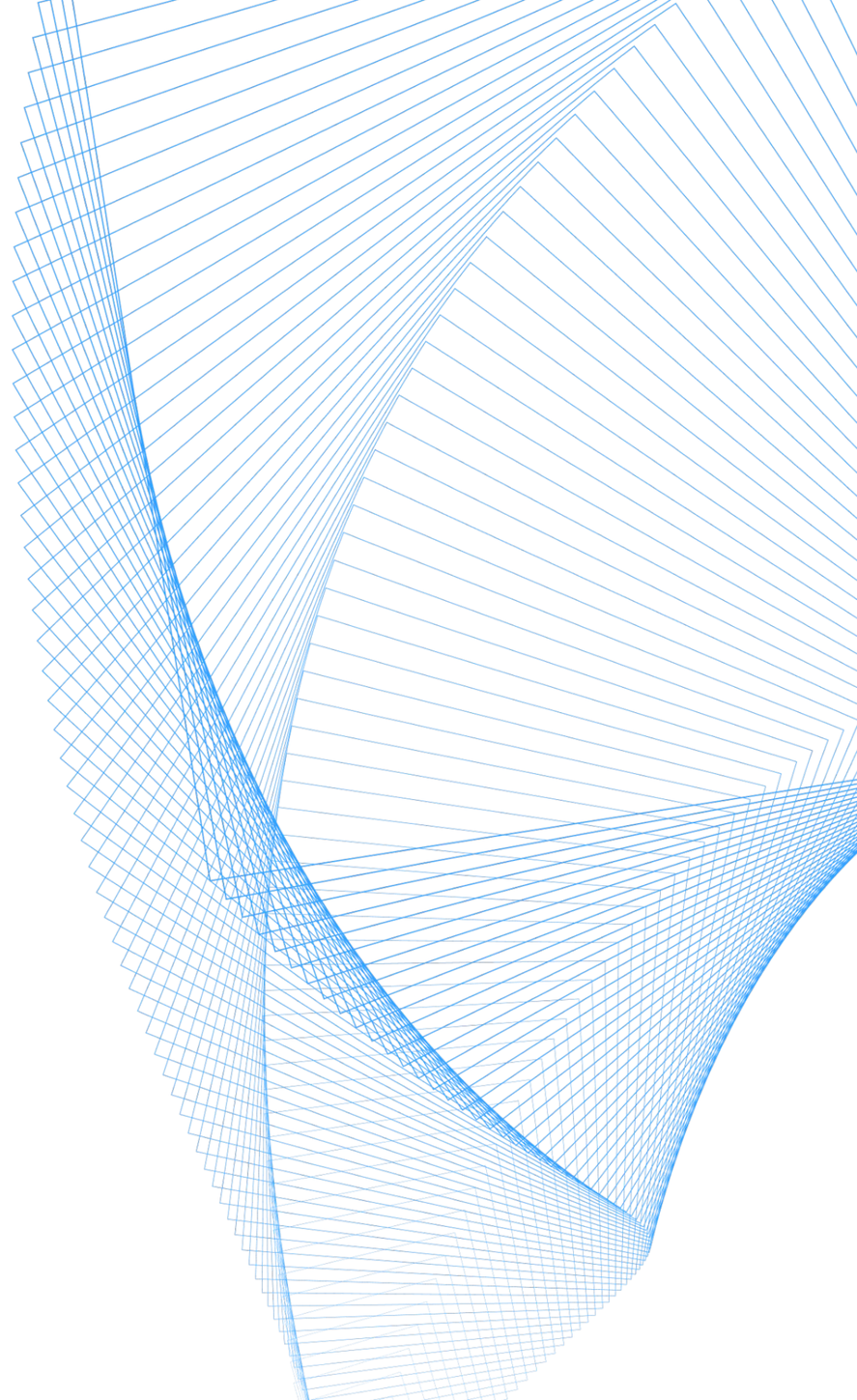
Kubernetes + Virtualization — соответствует требованиям по безопасности информации к средствам контейнеризации и требованиям по безопасности информации к средствам виртуализации

Исполнение 2

Kubernetes — соответствует требованиям по безопасности информации к средствам контейнеризации

Исполнение 3

Virtualization — соответствует требованиям по безопасности информации к средствам виртуализации



Возможности исполнений Deckhouse CSE

Возможности безопасности	DKP CSE LITE	DVP CSE	DKP CSE PRO
Исполнения	Kubernetes	Virtualization	Kubernetes + Virtualization
Приказ № 118 (контейнеры)	✓ 4 класс	✗	✓ 4 класс
Приказ № 187 (виртуализация)	✗	✓ 4 класс	✓ 4 класс
Приказ № 76 (4-й УД)	✓	✓	✓
Развёртывание в закрытом контуре	✓	✓	✓
Изоляция на уровне процессов хостовой ОС	✓	✗	✓
Изоляция на уровне гипервизора (отдельные ОС)	✗	✓	✓
Ролевая модель (RBAC)	✓	✓	✓
Централизованное управление кластерами	✓	✓	✓
Микросегментация сети	✓	✓	✓
Сбор и анализ событий безопасности	✓	✓	✓
Экспорт событий безопасности	✓	✓	✓

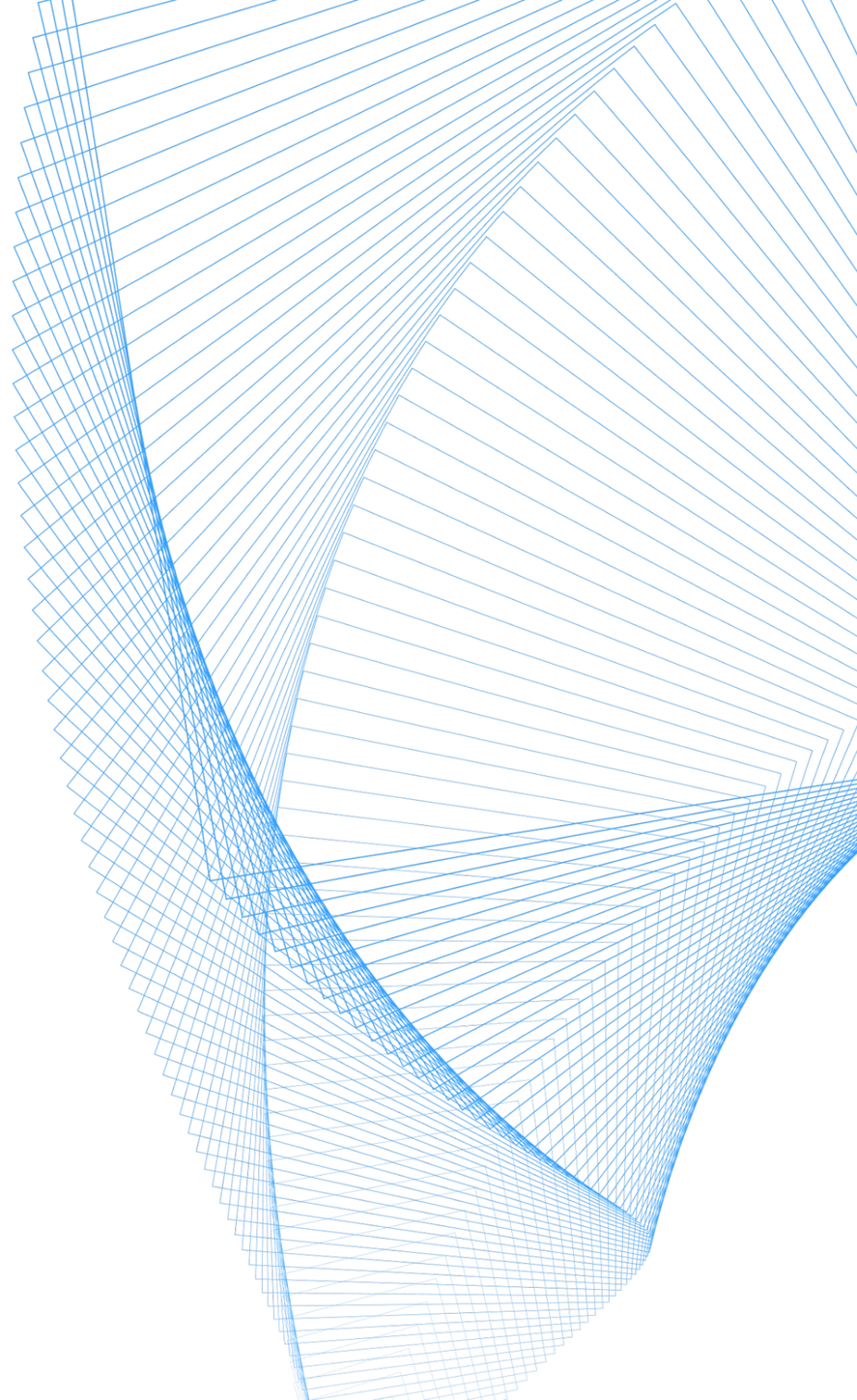
Уровни доверия и классы защиты

Уровень доверия —

это характеристика средства защиты информации, отражающая степень уверенности в отсутствии уязвимостей и недекларированных возможностей

Класс защиты

средства защиты информации определяет состав и уровень реализуемых функций безопасности



Deckhouse
Kubernetes Platform

Обновления DKP Certified Security Edition

К свойствам модулей добавлены обязательные и опциональные характеристики. Что это означает?

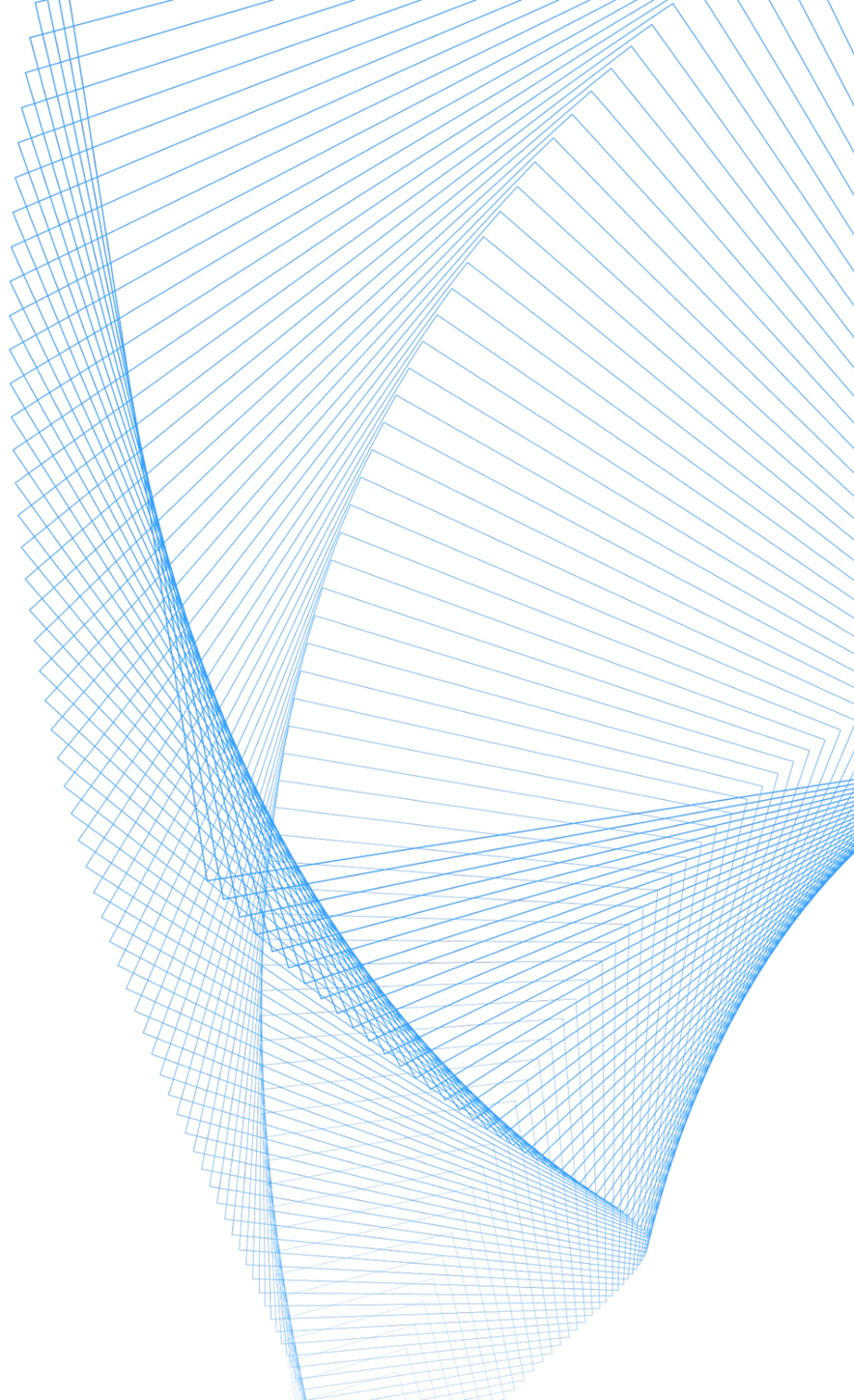
Обязательные модули обеспечивают функционирование DKP CSE и реализуют функции безопасности по требованиям приказов ФСТЭК России № 118 и № 187, опциональные модули расширяют функциональные возможности и могут быть использованы по выбору пользователя, исходя из потребностей и сценариев использования

Подробнее

Угрозы безопасности информации

Угрозы безопасности информации, которые могут быть нейтрализованы функционалом сертифицированной версии Deckhouse Platform, представлены в таблице, доступной здесь и по QR-коду

DKP CSE нейтрализует до 100 % уникальных угроз безопасности информации для платформ виртуализации и контейнеризации



№	Реализованная в DKP CSE функция безопасности информации	Угроза безопасности, от которой DKP CSE обеспечивает защиту
1.	Идентификация и аутентификация пользователей в средстве контейнеризации	УБИ.031 Угроза использования механизмов авторизации для повышения привилегий УБИ.086 Угроза несанкционированного изменения аутентификационной информации УБИ.090 Угроза несанкционированного создания учетной записи пользователя УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации
2.	Изоляция контейнеров средством контейнеризации	УБИ.007 Угроза воздействия на программы с высокими привилегиями УБИ.012 Угроза деструктивного изменения конфигурации/среды окружения программ УБИ.116 Угроза перехвата данных, передаваемых по вычислительной сети УБИ.088 Угроза несанкционированного копирования защищаемой информации - изоляция блочных устройств УБИ.090 Угроза несанкционированного создания учетной записи пользователя УБИ.093 Угроза несанкционированного управления буфером УБИ.099 Угроза обнаружения хостов УБИ.117 Угроза перехвата привилегированного потока УБИ.118 Угроза перехвата привилегированного процесса УБИ.223 Угроза несанкционированного доступа к контейнерам, предоставляющего пользователям расширенные привилегии УБИ.225 Угроза нарушения изоляции контейнеров
3.	Выявление уязвимостей в образах контейнеров	УБИ.192 Угроза использования уязвимых версий программного обеспечения УБИ.226: Угроза внедрения вредоносного программного обеспечения в контейнеры
4.	Проверка корректности конфигурации контейнеров	УБИ.109 Угроза перебора всех настроек и параметров приложения

Меры по обеспечению безопасности ЗО КИИ *

Мы подготовили таблицу , в которой приведены меры по обеспечению безопасности для значимого объекта в соответствии с приказом ФСТЭК России от 25 декабря 2017 г. № 239 и то, какими компонентами DKP CSE они представлены

Данную таблицу можно использовать при проектировании системы безопасности ЗО КИИ

* ЗО КИИ — значимый объект критической информационной инфраструктуры

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта*	Категория значимости			DKP CSE 1.73
		3	2	1	
I. Идентификация и аутентификация (ИАФ)					
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	да	да	да	n/a
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	да	да	да	user-authn + внешний провайдер
ИАФ.2	Идентификация и аутентификация устройств	да	да	да	user-authn + внешний провайдер
ИАФ.3	Управление идентификаторами	да	да	да	user-authn + внешний провайдер
ИАФ.4	Управление средствами аутентификации	да	да	да	user-authn + внешний провайдер
ИАФ.5	Идентификация и аутентификация внешних пользователей	да	да	да	user-authn + внешний провайдер
ИАФ.6	Двусторонняя аутентификация				user-authn + внешний провайдер
ИАФ.7	Защита аутентификационной информации при передаче	да	да	да	user-authn + внешний провайдер
II. Управление доступом (УПД)					
УПД.0	Регламентация правил и процедур управления доступом	да	да	да	n/a
УПД.1	Управление учетными записями пользователей	да	да	да	user-authz
УПД.2	Реализация модели управления доступом	да	да	да	user-authz
УПД.3	Доверенная загрузка	да	да	да	control-plane-manager
УПД.4	Разделение полномочий (ролей) пользователей	да	да	да	user-authz
УПД.5	Назначение минимально необходимых прав и привилегий	да	да	да	user-authz
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	да	да	да	user-authn + внешний провайдер
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам				
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе				
УПД.9	Ограничение числа параллельных сеансов доступа			да	user-authn + внешний провайдер
УПД.10	Блокирование сеанса доступа пользователя при неактивности	да	да	да	user-authn + внешний провайдер

Группы мер ЗСВ * и ЗКО *

Мы подготовили таблицу , в которой приведены группы мер по ЗСВ и ЗКО из методического документа «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах» с указанием их выполнения в DKP CSE

Данную таблицу можно использовать при проектировании системы защиты информации в соответствии с приказом ФСТЭК России № 117

* ЗСВ — защита виртуализации и облачных технологий инфраструктуры

* ЗКО — защита технологий контейнерных сред и их оркестрации

Выполнение Deckhouse Kubernetes Platform Certified Security Edition 1.73 (DKP CSE) группы мер по защите виртуализации и облачных технологий (ЗСВ) и защите технологий контейнерных сред и их оркестрации (ЗКО) из методического документа «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах» (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-12-aprelya-2026-g)

Условное обозначение и номер меры	**Меры защиты информации в информационных системах**	**Функции безопасности**	**Пункты ТУ DKP CSE**
4.4 Защита виртуализации облачных технологий (ЗСВ)		**Приказ ФСТЭК России № 187**	
ЗСВ.1 Доверенная загрузка виртуальных машин	При применении средств виртуализации должны обеспечиваться: • доверенная загрузка хостовой операционной системы (при ее наличии) и средства виртуализации; • выявление загрузки виртуальных машин, состав и настройки виртуального оборудования которых содержат несанкционированные изменения. Указанные меры защиты информации реализуются за счет применениях информационной системе встроенных в базовые системы ввода-вывода механизмов безопасности, и (или) средств доверенной загрузки, и (или) встроенных в хостовые операционные системы механизмов безопасности, и (или) встроенных в средства виртуализации механизмов безопасности. **Усиления до К1 включительно:** 1) должна обеспечиваться блокировка загрузки виртуальной машины, в которой исполняемые файлы или конфигурация компонентов, участвующих в загрузке гостевой операционной системы, содержат несанкционированные изменения; 2) должна обеспечиваться блокировка загрузки виртуальной машины, если загружаемая версия гостевой операционной системы содержит критические уязвимости и (или) запрещена для использования в	**Выполняется** 9. К доверенной загрузке виртуальных машин предъявляются следующие требования: 9.1. Средство виртуализации 6, 5 классов защиты должно блокировать запуск виртуальной машины при выявлении нарушения целостности конфигурации виртуального оборудования данной виртуальной машины. 9.2. Средство виртуализации 4 класса защиты наряду с требованиями, установленными подпунктом 9.1 пункта 9 настоящих Требований, дополнительно должно блокировать запуск виртуальной машины при выявлении нарушения целостности файлов виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины) и (или) исполняемых файлов гостевой операционной системы.	3.2.4.8

Наши успехи с момента получения первого сертификата

Октябрь 2024

Первая сертифицированная версия, реализованы все обязательные функции безопасности

Декабрь 2024

Добавлены альтернативный способ управления сетью в кластере, поддержка работы с хранилищами Ceph и NFS

Апрель 2025

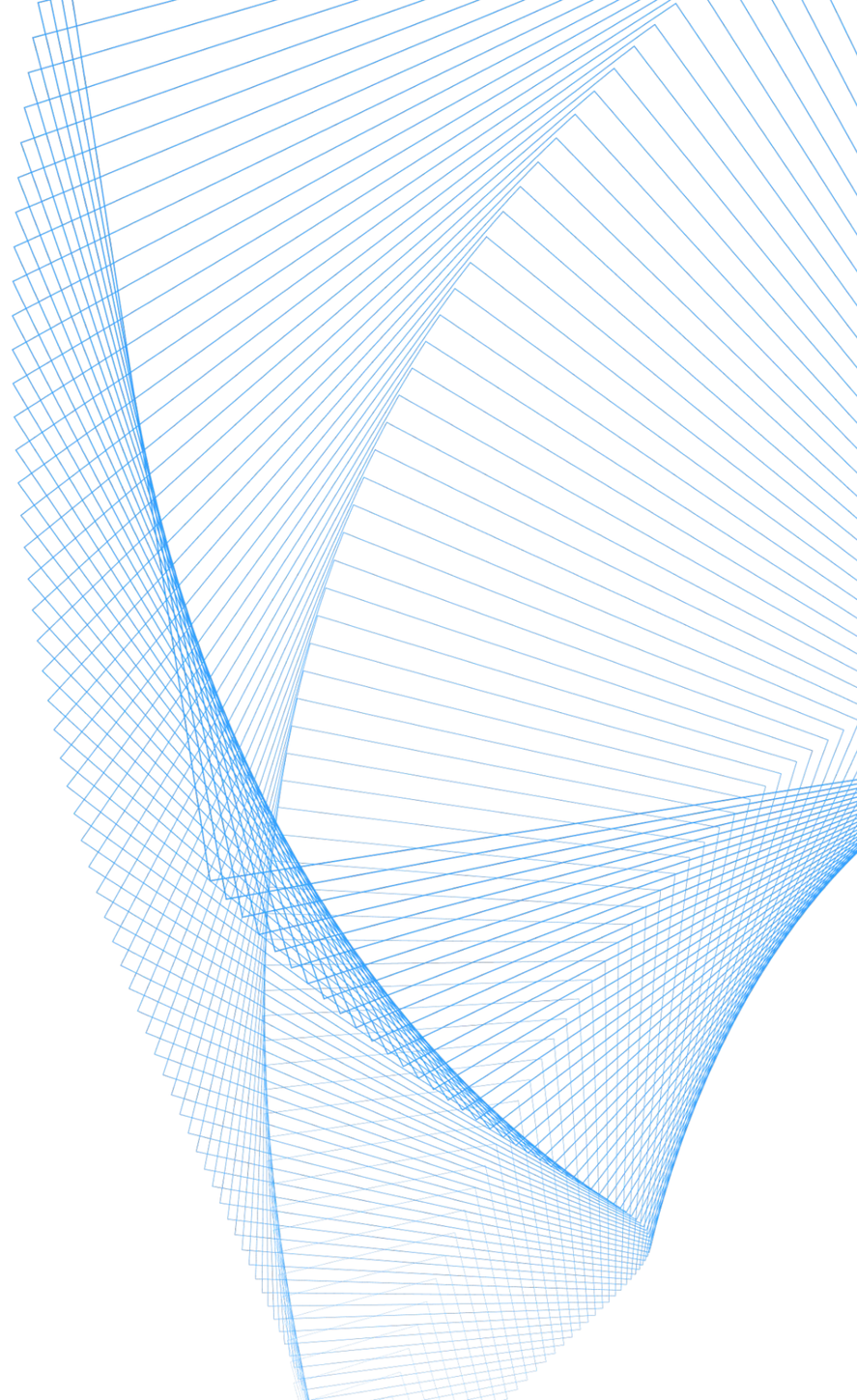
Добавлен веб-интерфейс для управления кластером и визуализации состояния системы, добавлен Istio

Март 2026

Добавлена виртуализация, выделено 3 исполнения

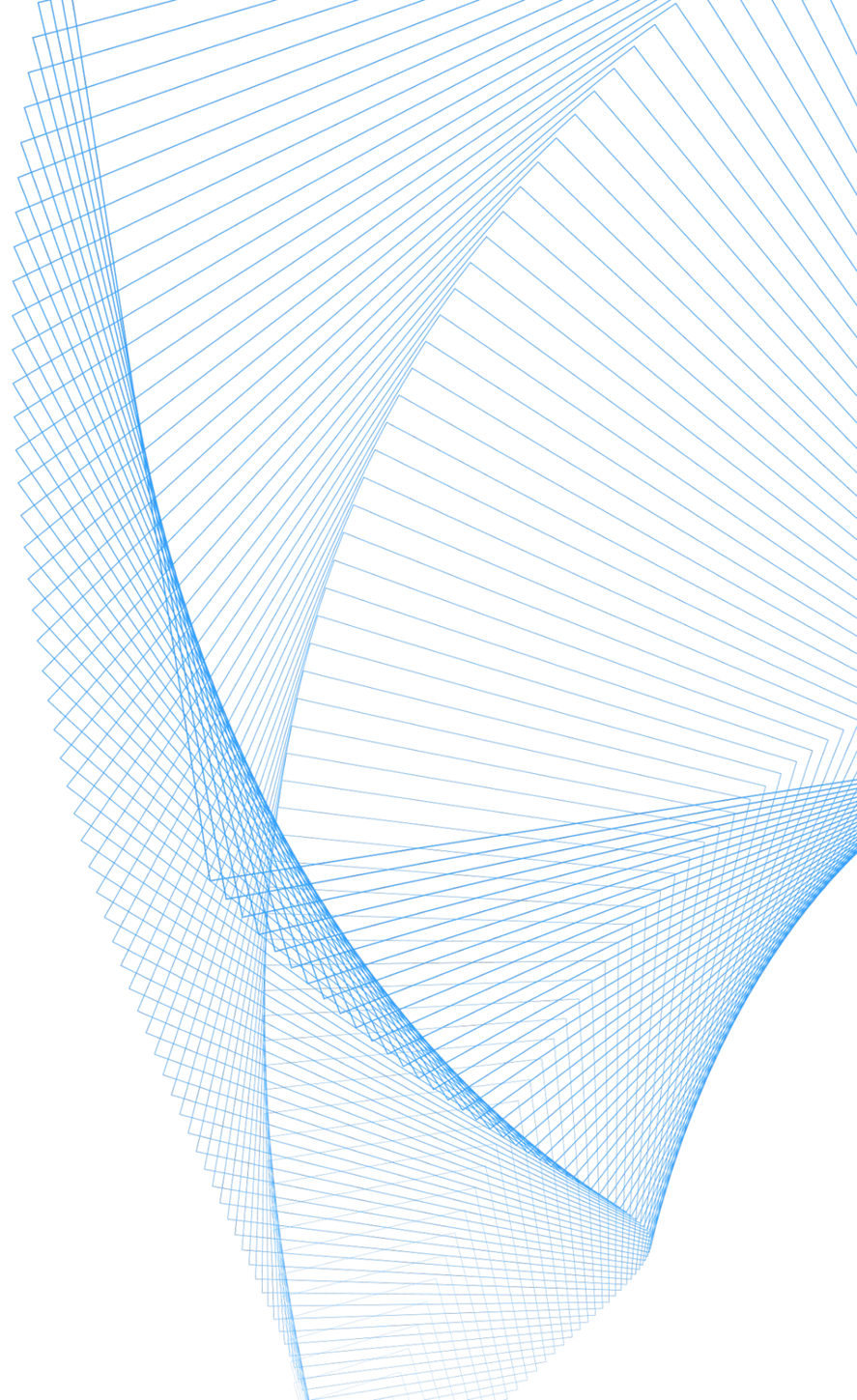
2026 год

Паритет по функциям между Enterprise и Certified Security



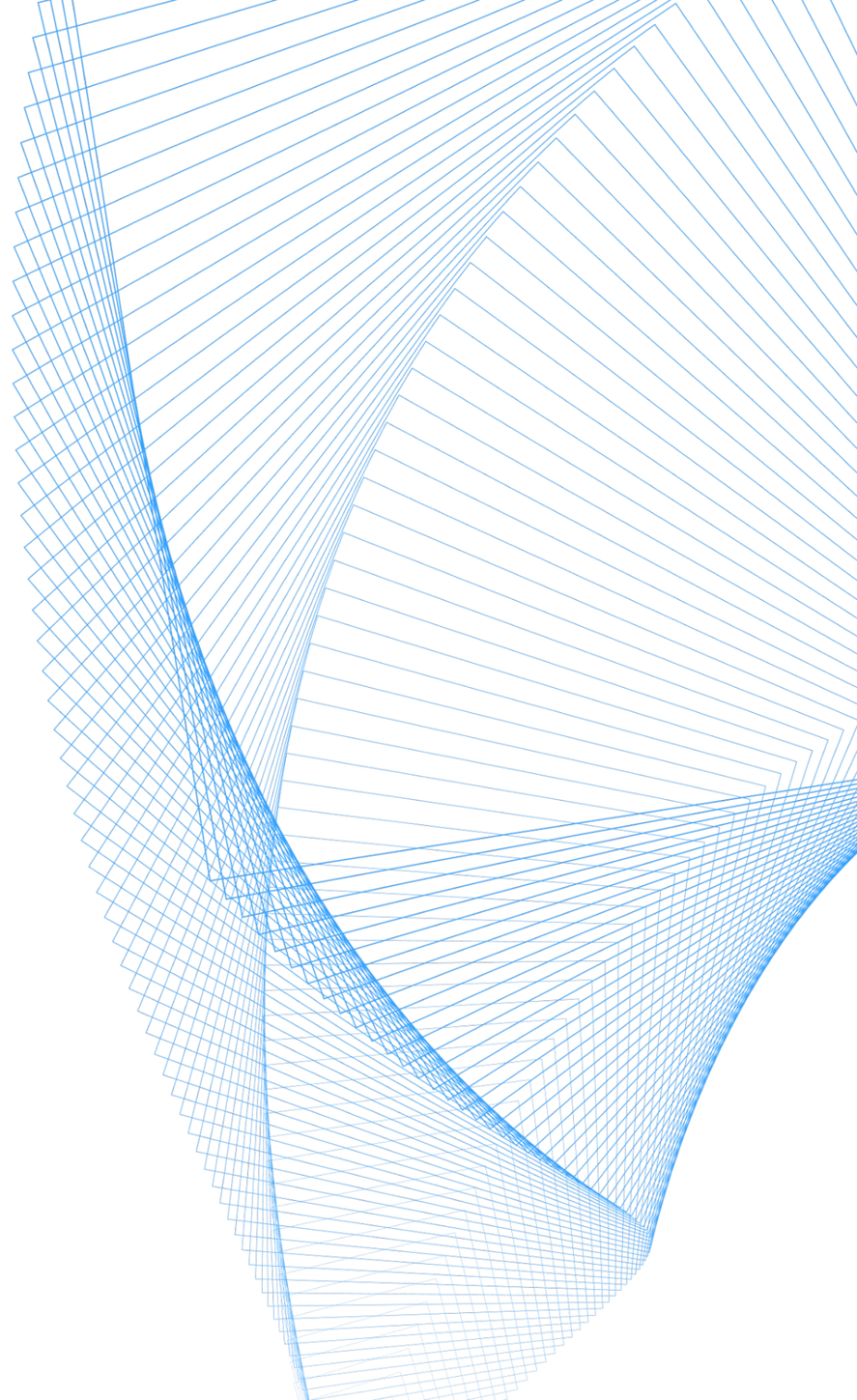
Инфраструктурные обновления платформы

Версии компонентов	Kubernetes 1.29 и 1.31, Ingress Nginx 1.12.1, Grafana 10.4.19
Архитектура	• Новые подсистемы: сеть, виртуализация, инфраструктура • Реорганизация модулей: priority-class и flow-schema интегрированы в deckhouse
Хранилища	• Локальные хранилища (LVM) • Внешние: Ceph, NFS, SCSI, Yadro Tatlin Unified Storage
Безопасность	• Устранены все известные CVE • Контроль целостности образов (Cosign)



Основные изменения в 1.73 — операционные возможности и управление

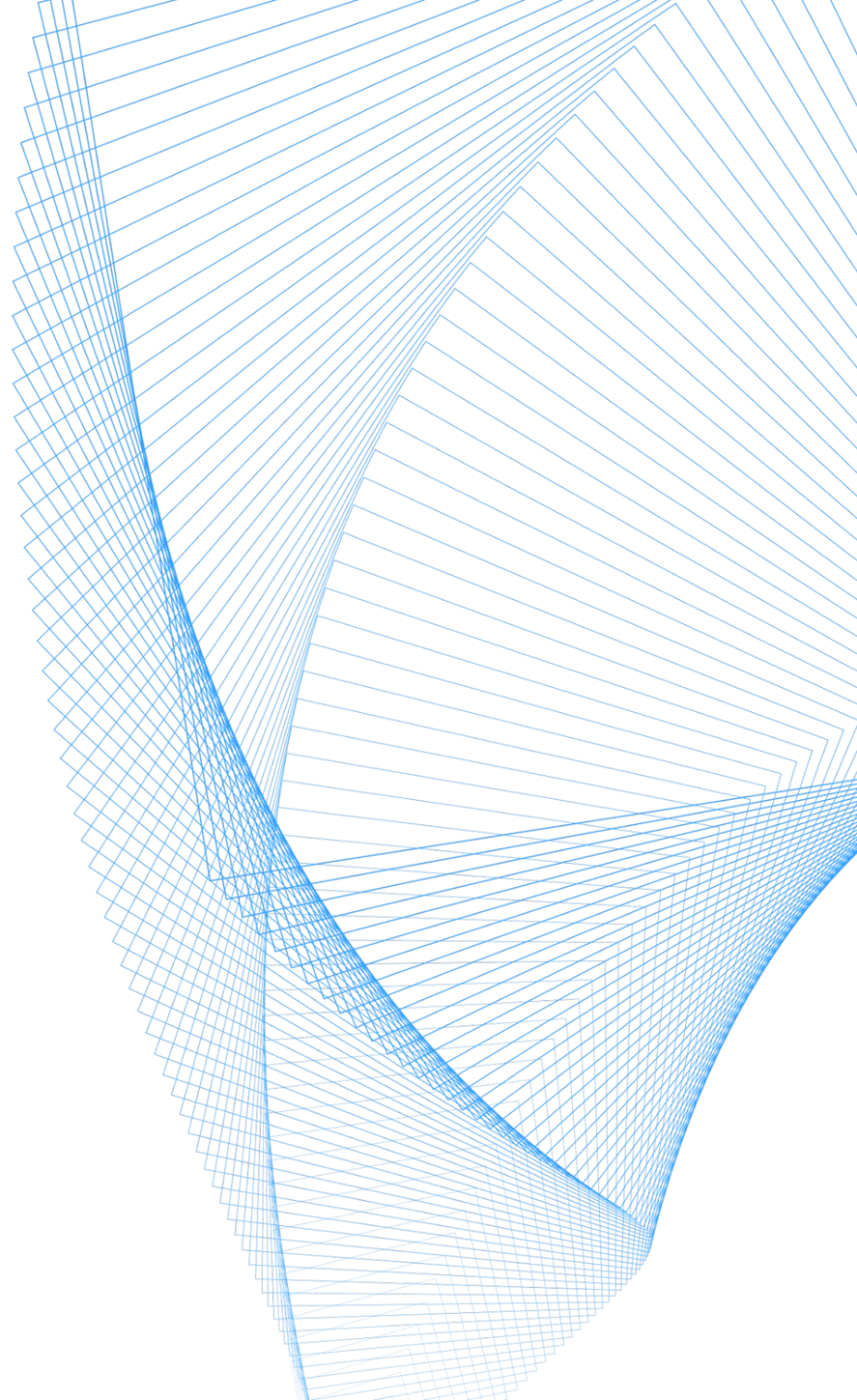
Логирование	• Сбор, преобразование, управление метками логов • Улучшенная обработка ошибок в установщике
Виртуализация	Декларативное управление ВМ и ресурсами: образы, классы, хранилища
Сеть	Управление потоками: фильтрация, маршрутизация, визуализация взаимодействий
Данные	Миграция etcd
Доступ	Локальная аутентификация, управление пользователями, парольная политика, 2FA



Над чем работаем?

Готовим платформу к запуску в качестве гипервизора первого типа

Дорабатываем подсистему «Сеть» для сертификации по требованиям межсетевых экранов по 4-му классу защиты (по типам Б и В)



Deckhouse Kubernetes Platform CSE PRO

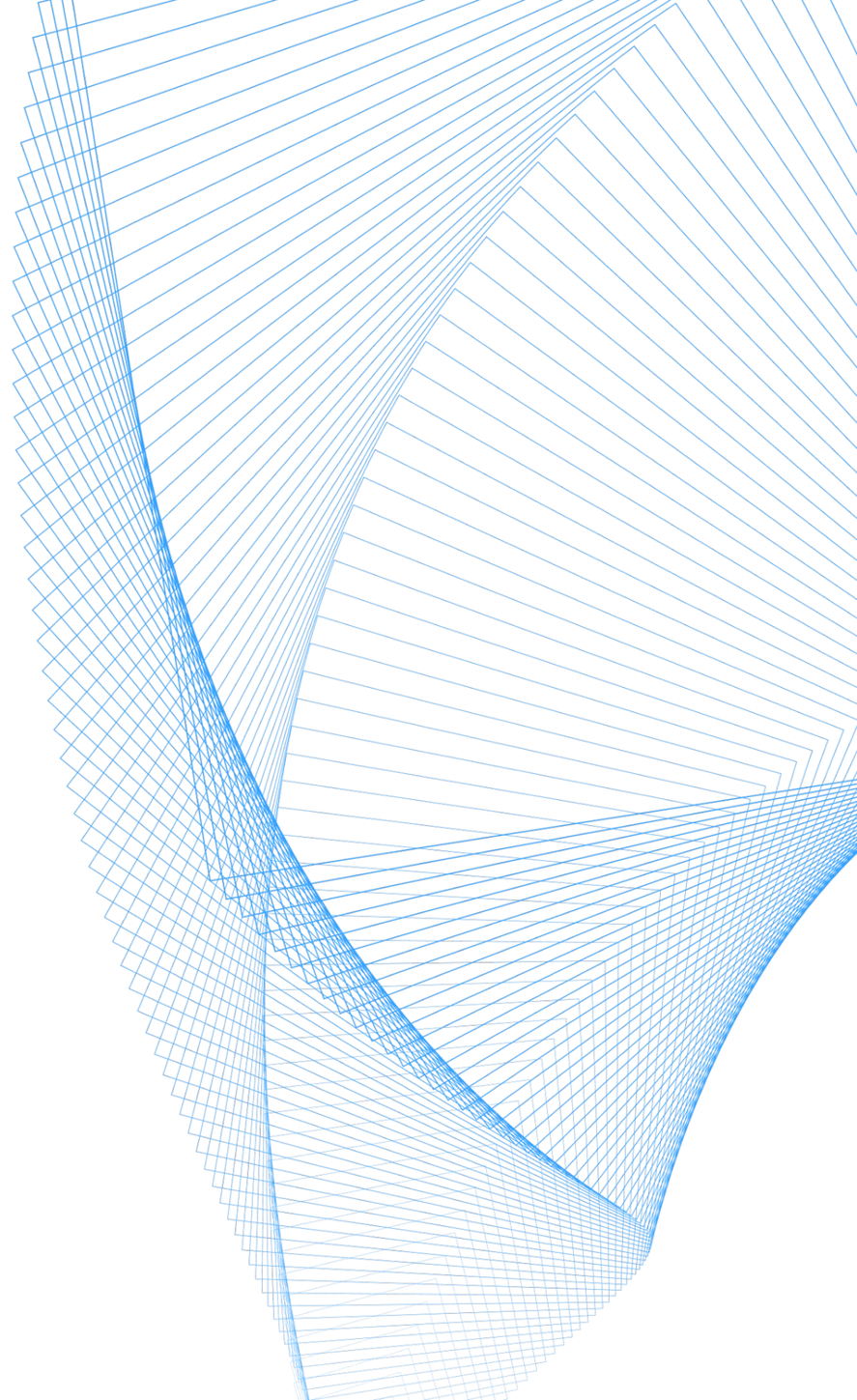
Включает в себя контейнеры + ВМ в одном кластере

- Упрощение масштабирования: сертификат покрывает разные сценарии использования
- Гибридная платформа для безопасного запуска традиционных и микросервисных приложений
- Единый веб-интерфейс и мониторинг для компонентов платформы, виртуальных машин и контейнеров
- Централизованное управление безопасностью для любых типов нагрузок
- Контролируемое развёртывание кластеров и аудит изменений

Исполнение виртуализация:

Deckhouse Virtualization Platform CSE

- Реализует все функции классической виртуализации
- При этом является не просто заменой VMware, а даёт больше функционала
- Обеспечивает цифровой суверенитет
- Фундамент для стратегического развития современной архитектуры и плавного перехода к полноценной гибридной платформе



Deckhouse — российское решение с современным подходом

Deckhouse
ФЛАНТ

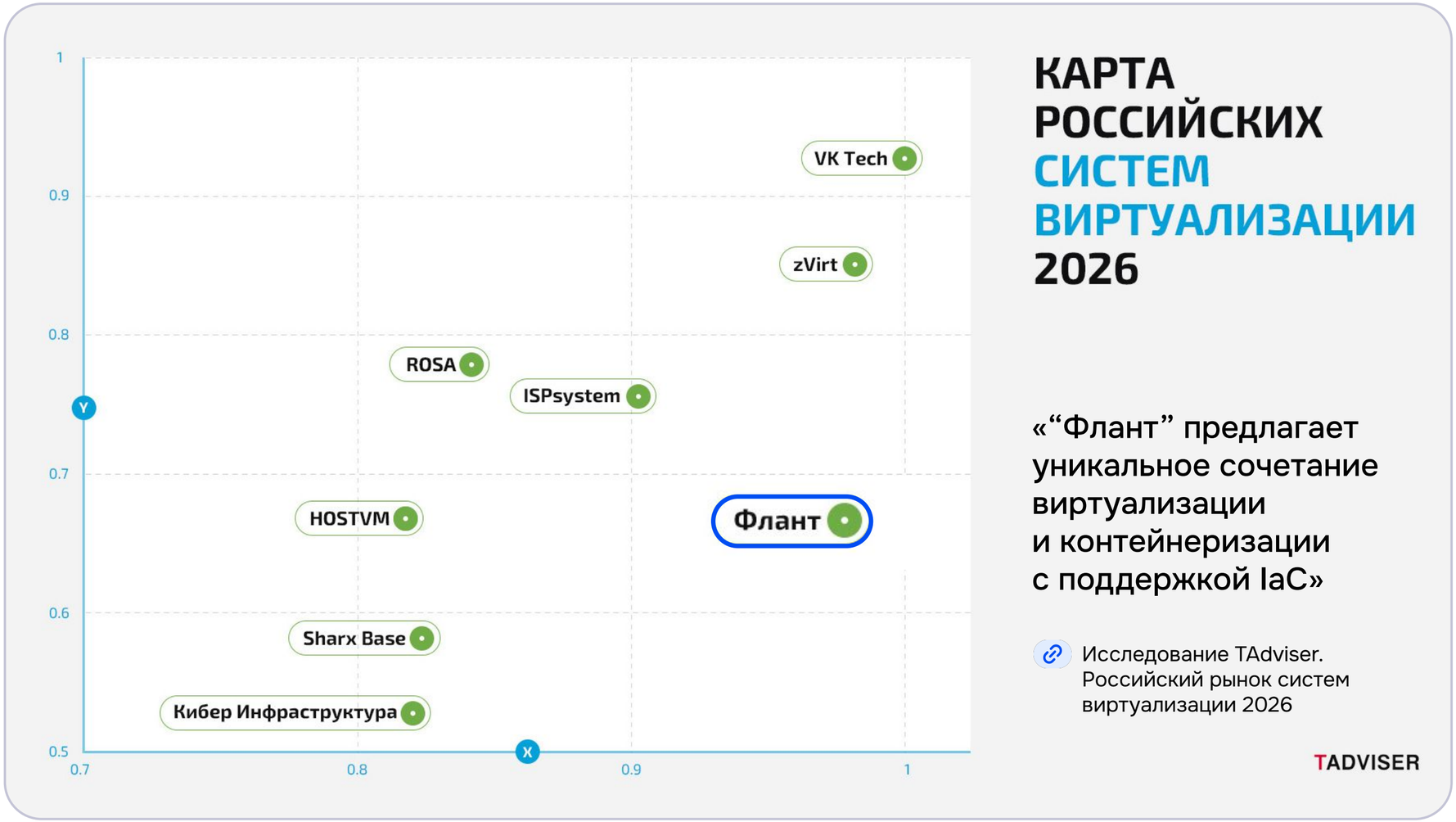
Red Hat

Google

vmware
by Broadcom

SUSE

Qalauda.io



КАРТА РОССИЙСКИХ СИСТЕМ ВИРТУАЛИЗАЦИИ 2026

«“Флант” предлагает уникальное сочетание виртуализации и контейнеризации с поддержкой IaC»

Исследование TAdviser. Российский рынок систем виртуализации 2026

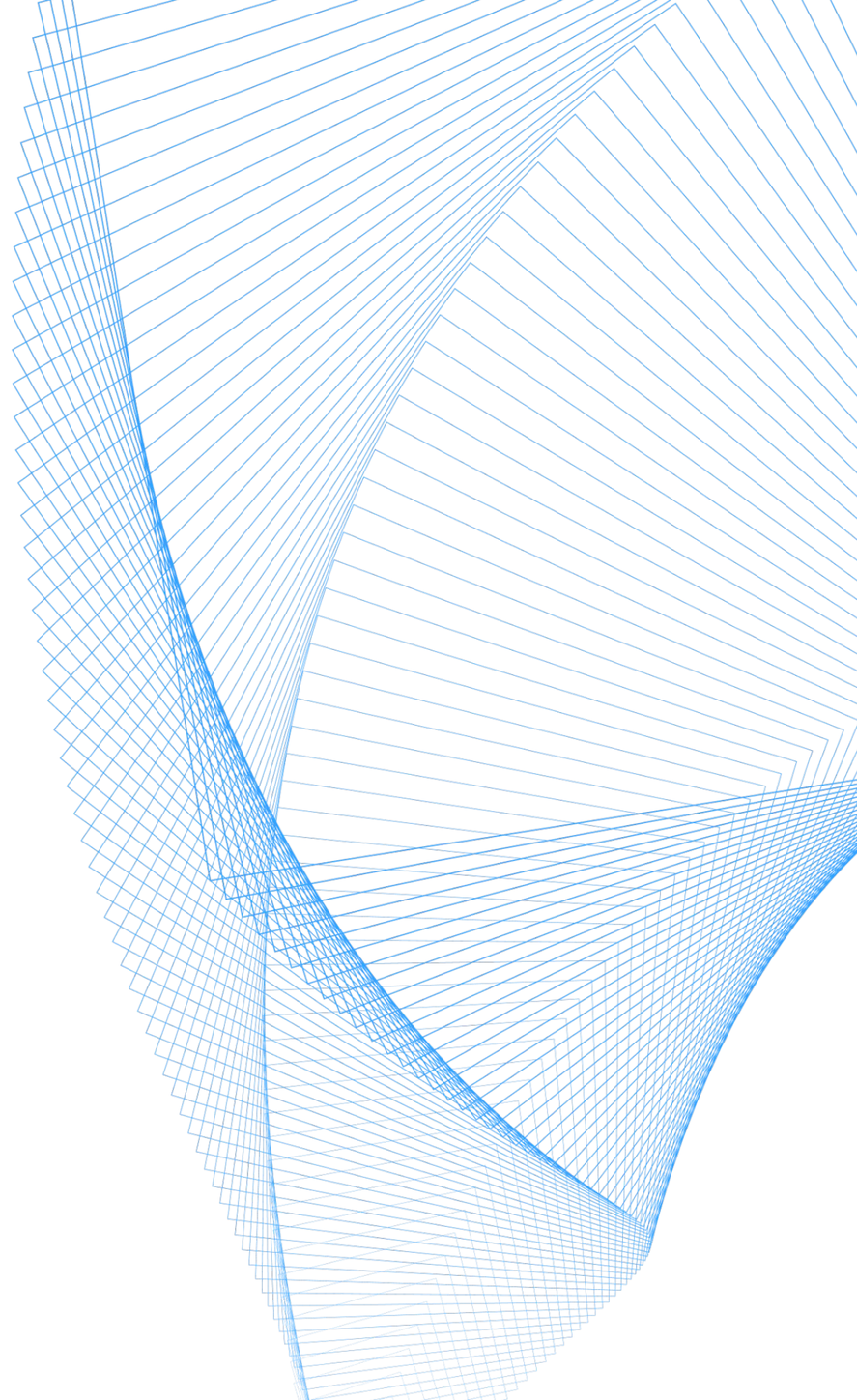
TADVISER

Deckhouse
Kubernetes Platform

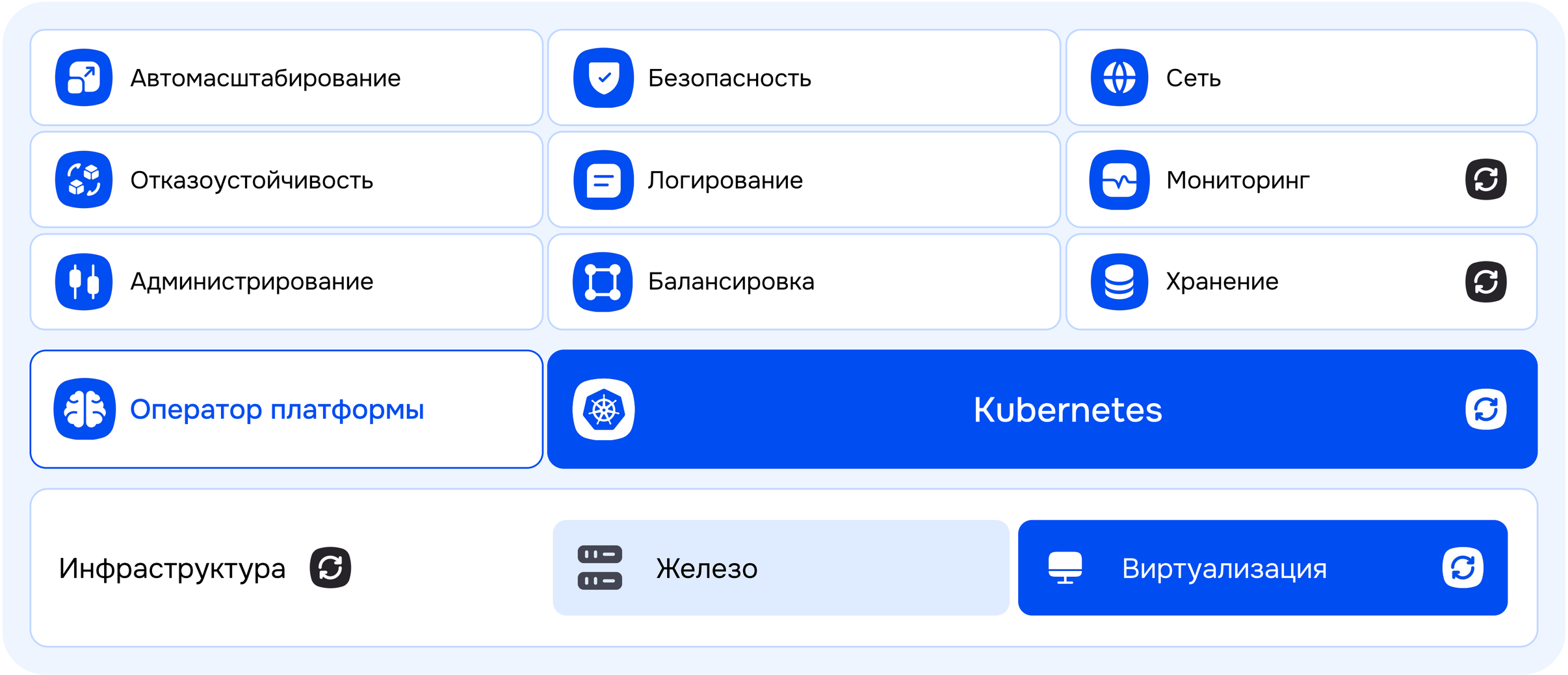
Deckhouse
Virtualization Platform

Бескомпромиссная платформа для решения любых инфраструктурных задач

Новые функции
и возможности релиза 1.73



Состав Deckhouse Kubernetes Platform CSE

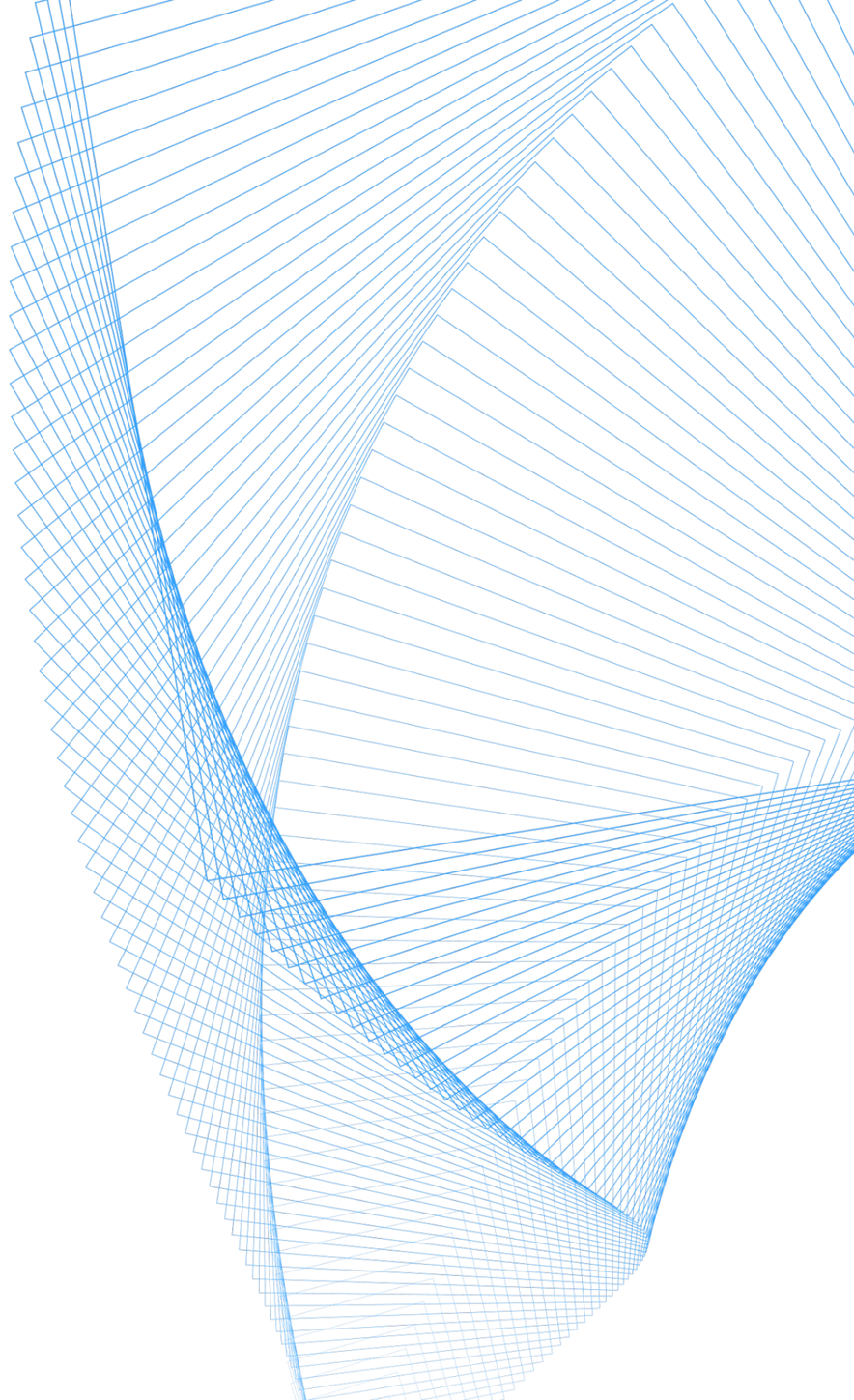


Подсистема «Виртуализация»

Запуск виртуальных машин в одной среде с контейнерами

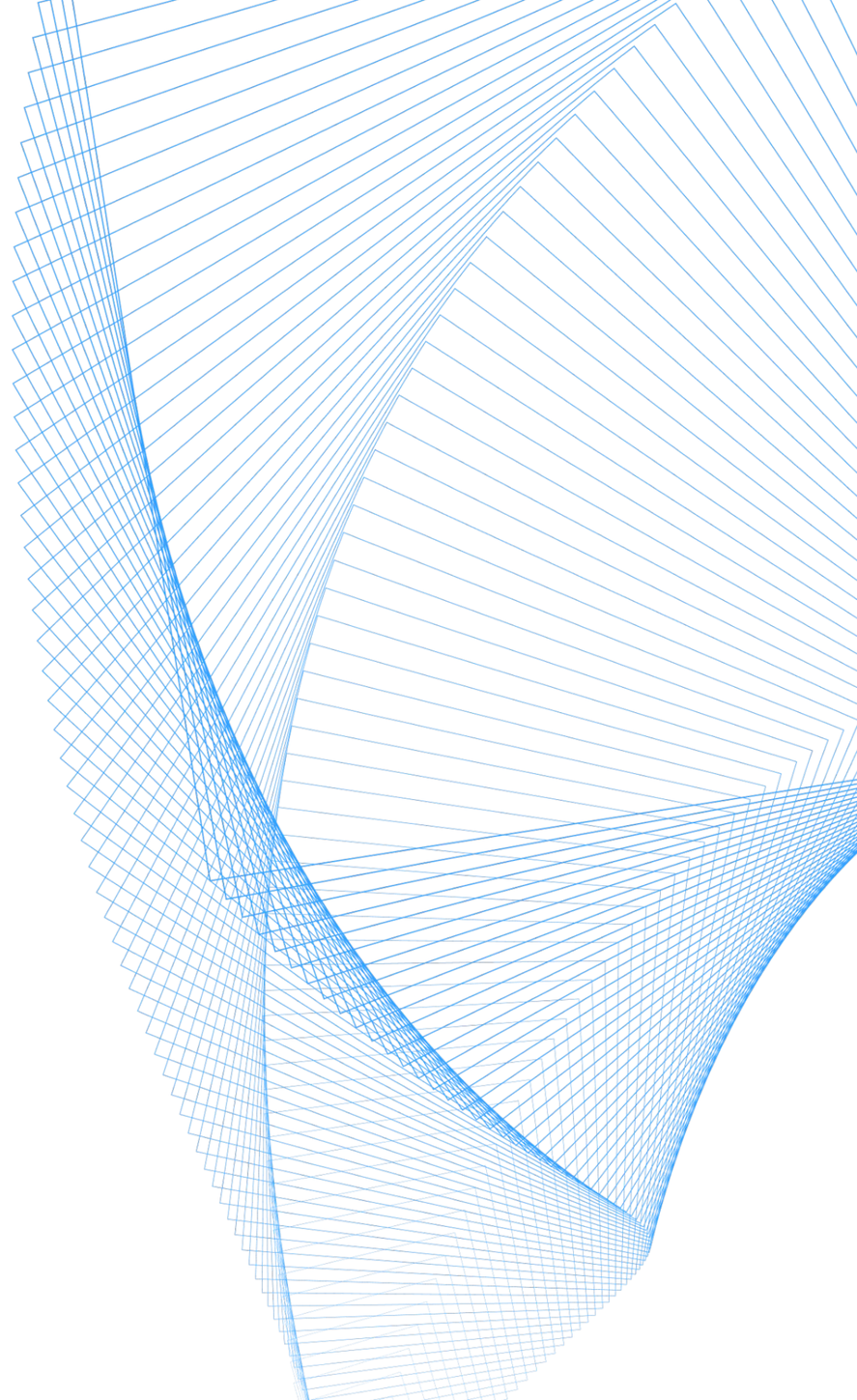
Модуль virtualization

- Управление любыми пользовательскими нагрузками из одного веб-интерфейса
- Использование современных DevOps-практик для управления виртуальными машинами



В 2026 году пора искать альтернативы виртуализации

- VMware не соответствует требованиям регуляторов
- Октябрь 2025 года — окончание поддержки vSphere 7. Нельзя получить обновления
- Без обновлений, виртуализация — не граница безопасности, а кратчайший путь для контроля над всей инфраструктурой
- Современные эксплойты для VMware делают гипервизор критической точкой атаки



Статья Huntress: «The Great VM Escape: ESXi Exploitation in the Wild»

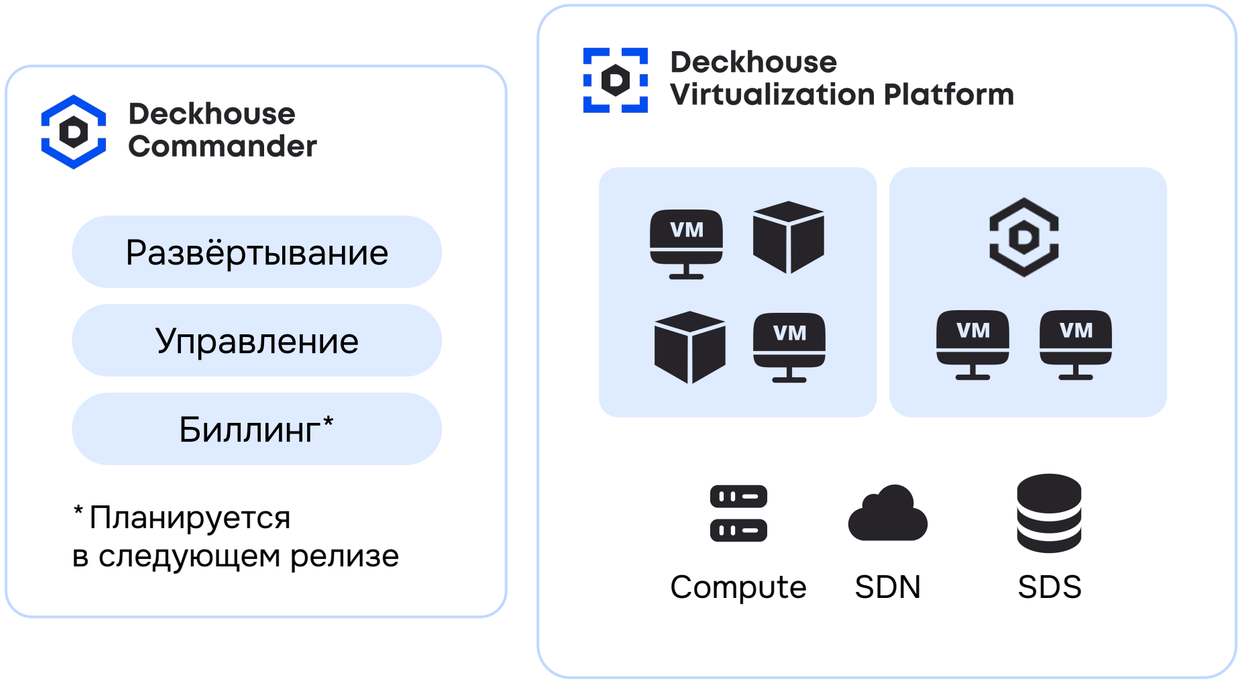
Решение от Deckhouse

Deckhouse Virtualization Platform

- Единый управляющий слой для ВМ и микросервисов
- Сквозная безопасность и наблюдаемость
- Мультитенантность и квоты (IAAS)
- Один UI для виртуализации и контейнеризации

Deckhouse Commander

Централизованное развёртывание и управление кластерами Deckhouse



DVP меняет правила игры

Deckhouse
Virtualization Platform

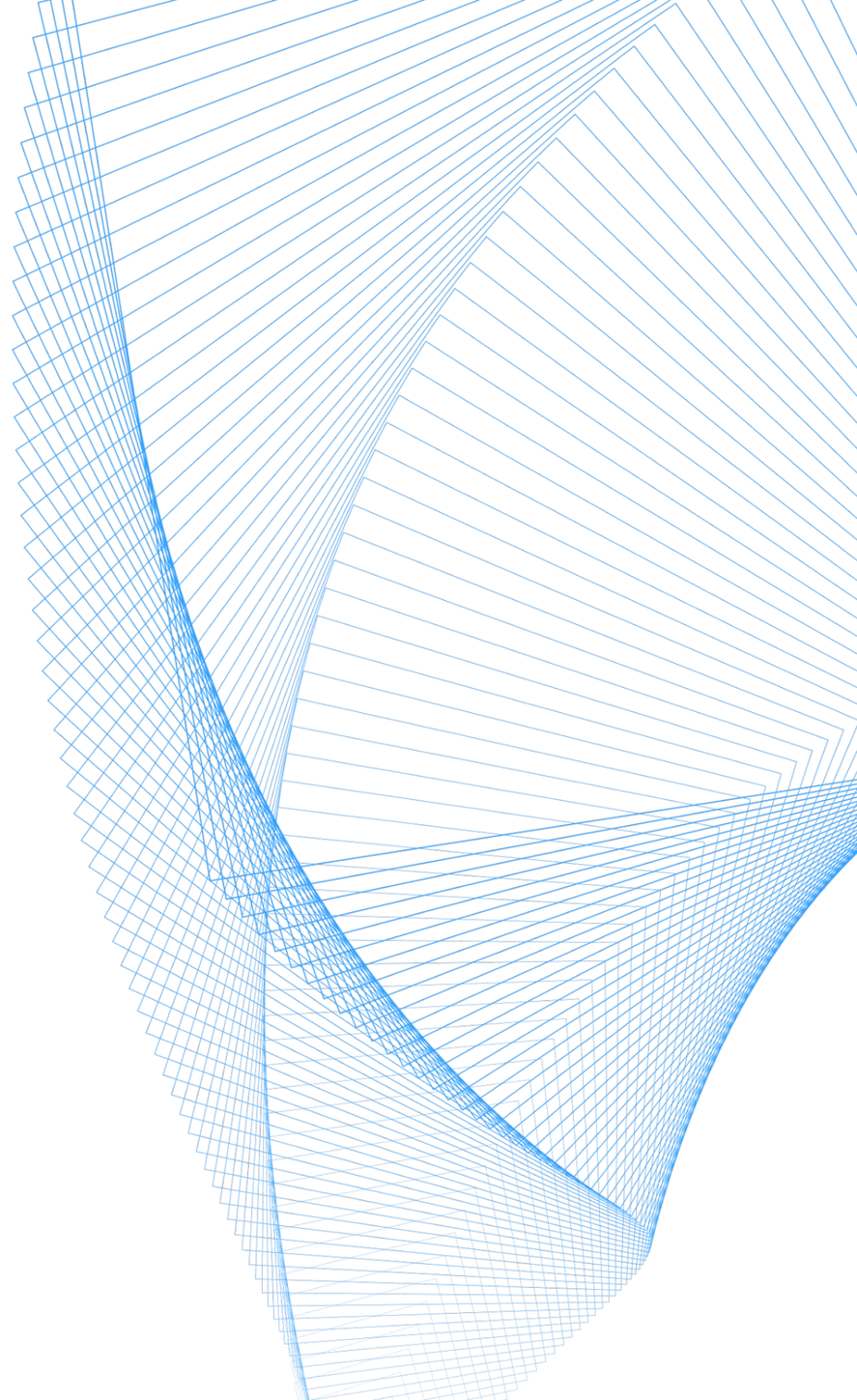
Виртуализация в стиле Kubernetes
для вашей инфраструктуры

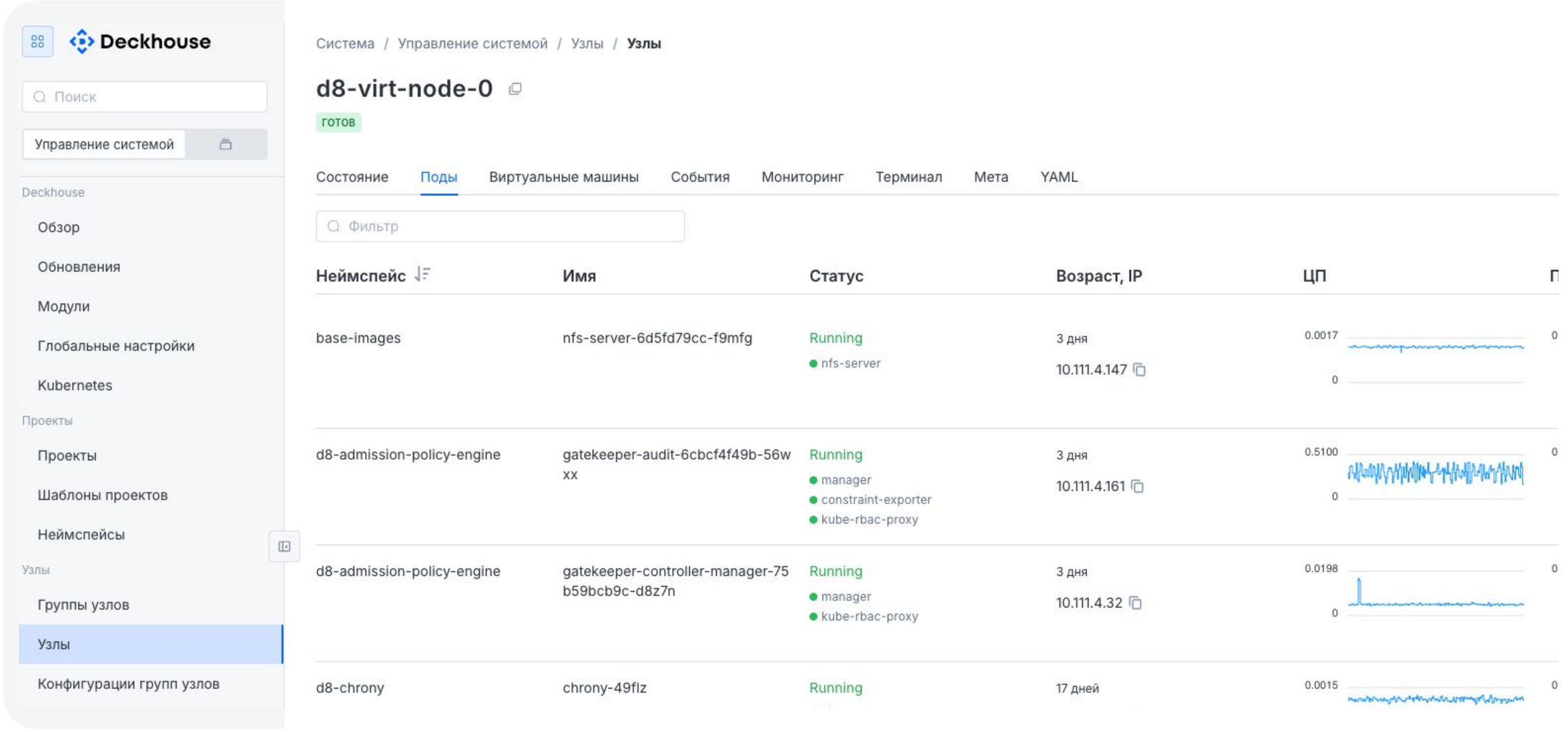
Мы не предлагаем мигрировать на ещё одну виртуализацию

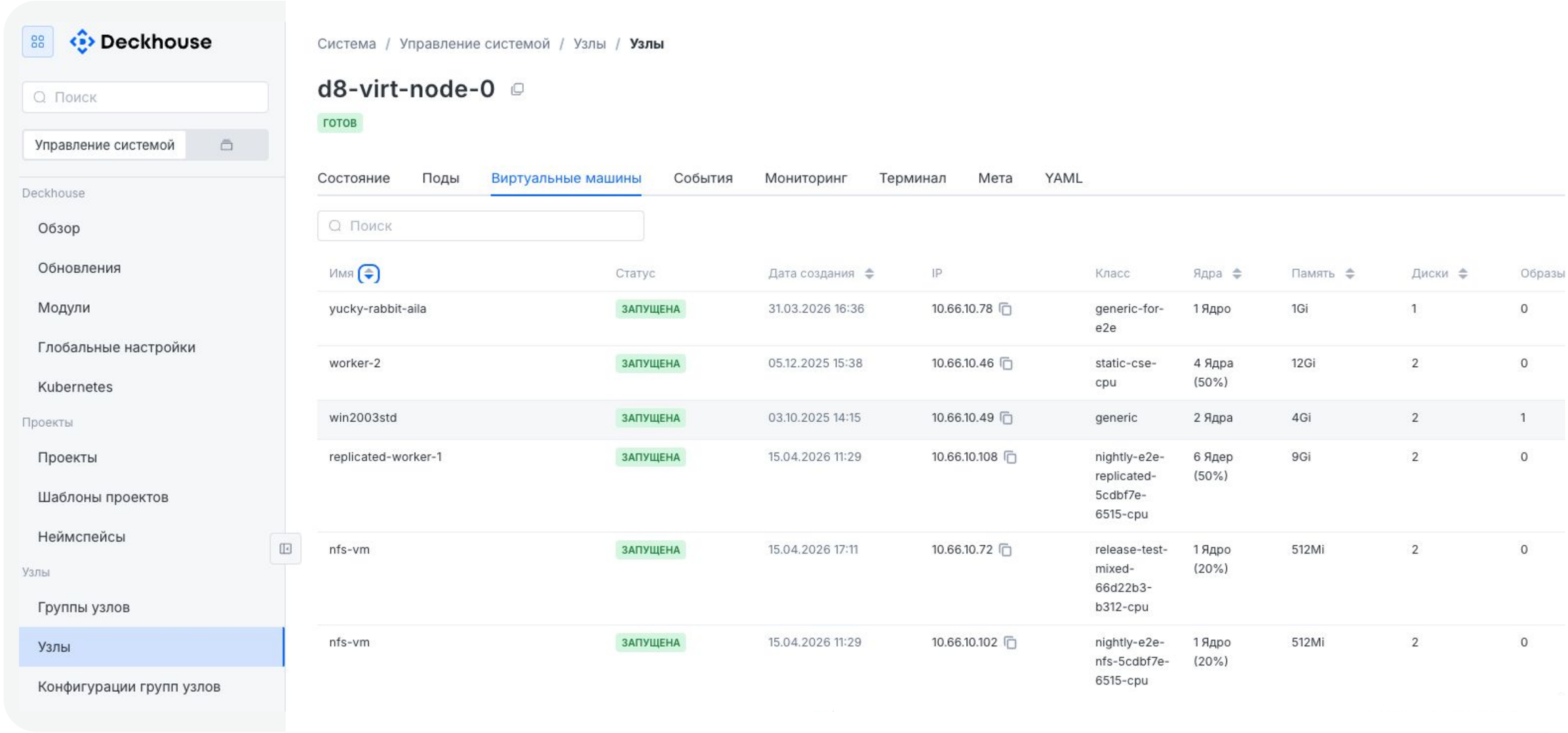
- Импортозамещение VMware на существующие аналоги — тактический шаг, не решающий задач современной инфраструктуры
- DVP — стратегический выбор, дающий единый стандарт управления любыми нагрузками

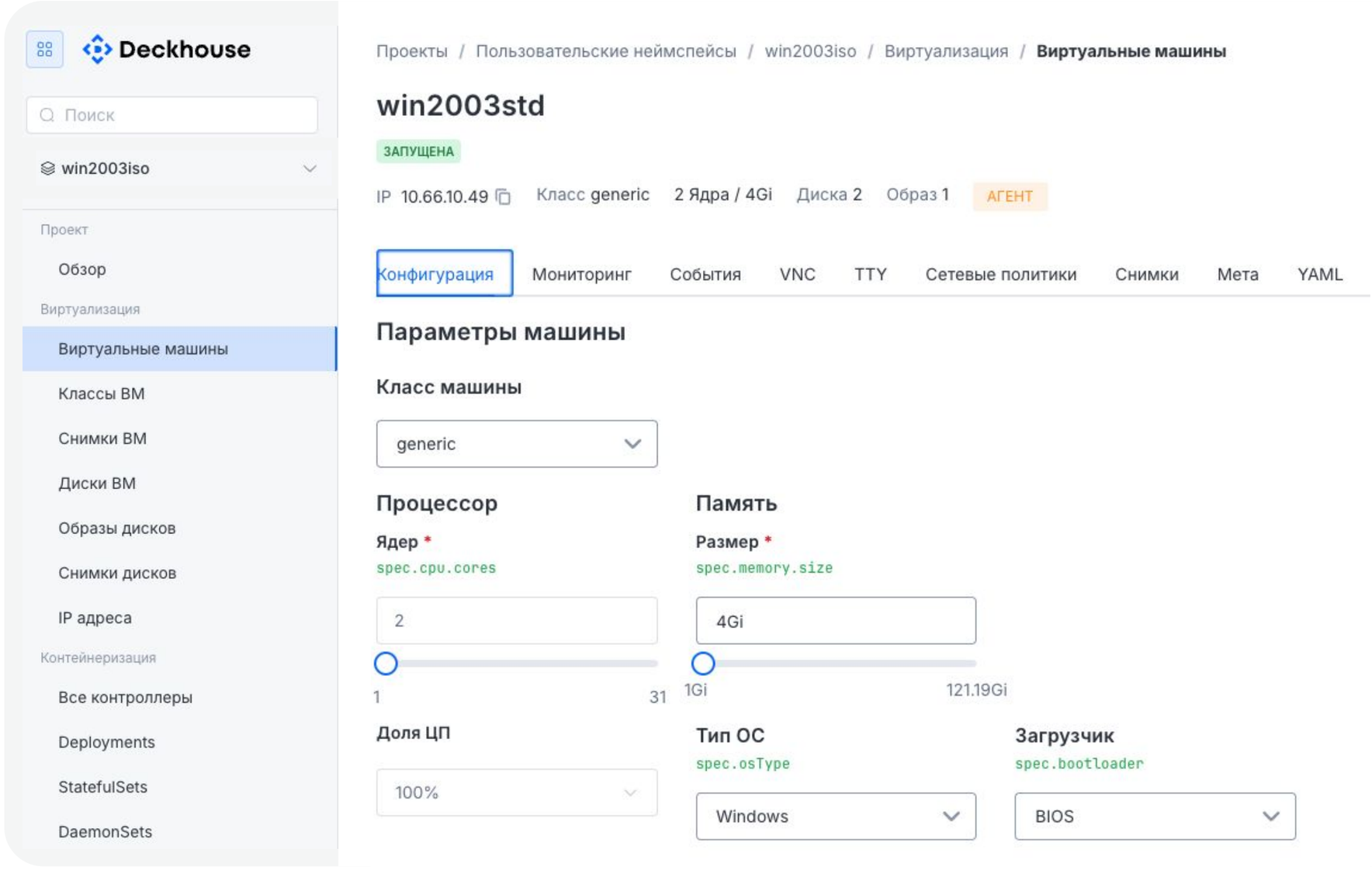
DVP использует Cloud Native-подход

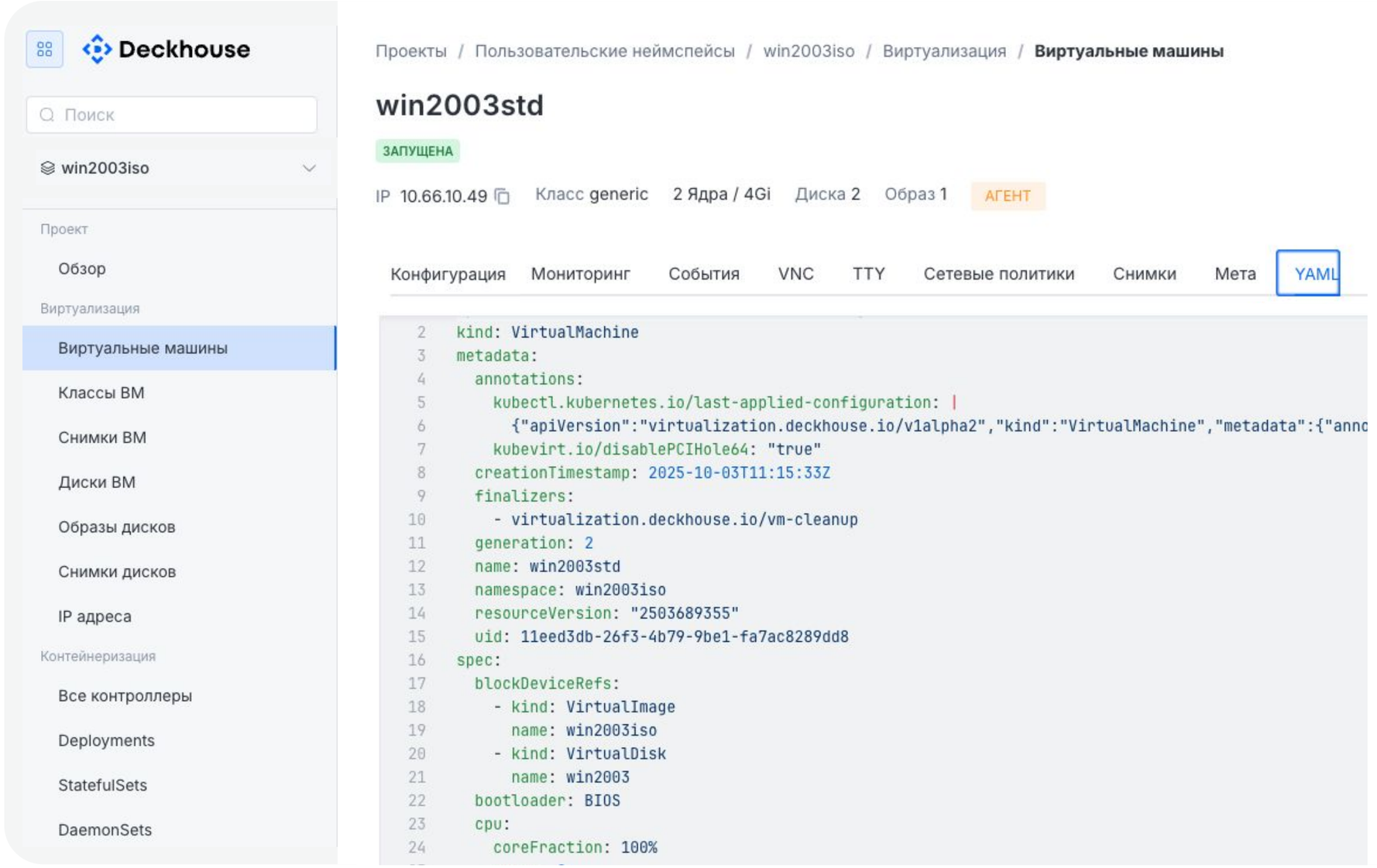
- Развёртывания за минуты, а не за дни
- Меньше ошибок в результате ручных действий
- Предсказуемый результат
- Масштабируемость и простое тиражирование
- Контроль и безопасность




Deckhouse
Поиск
Управление системой
Deckhouse
Обзор
Обновления
Модули
Глобальные настройки
Kubernetes
Проекты
Проекты
Шаблоны проектов
Неймспейсы
Узлы
Группы узлов
Узлы
Конфигурации групп узлов
Система / Управление системой / Узлы / Узлы
d8-virt-node-0
готов
Состояние
Поды
Виртуальные машины
События
Мониторинг
Терминал
Мета
YAML
Фильтр
Неймспейс
Имя
Статус
Возраст, IP
ЦП
П
base-images
nfs-server-6d5fd79cc-f9mfg
Running
nfs-server
3 дня
10.111.4.147
0.0017
0
0
d8-admission-policy-engine
gatekeeper-audit-6cbcf4f49b-56wxx
Running
manager
constraint-exporter
kube-rbac-proxy
3 дня
10.111.4.161
0.5100
0
0
d8-admission-policy-engine
gatekeeper-controller-manager-75b59bcb9c-d8z7n
Running
manager
kube-rbac-proxy
3 дня
10.111.4.32
0.0198
0
0
d8-chrony
chrony-49flz
Running
17 дней
0.0015
0


Deckhouse
Поиск
Управление системой
Deckhouse
Обзор
Обновления
Модули
Глобальные настройки
Kubernetes
Проекты
Проекты
Шаблоны проектов
Неймспейсы
Узлы
Группы узлов
Узлы
Конфигурации групп узлов
Система / Управление системой / Узлы / Узлы
d8-virt-node-0
ГОТОВ
Состояние
Поды
Виртуальные машины
События
Мониторинг
Терминал
Мета
YAML
Поиск
Имя
Статус
Дата создания
IP
Класс
Ядра
Память
Диски
Образы
yucky-rabbit-aila
ЗАПУЩЕНА
31.03.2026 16:36
10.66.10.78
generic-for-e2e
1 Ядро
1Gi
1
0
worker-2
ЗАПУЩЕНА
05.12.2025 15:38
10.66.10.46
static-cse-cpu
4 Ядра (50%)
12Gi
2
0
win2003std
ЗАПУЩЕНА
03.10.2025 14:15
10.66.10.49
generic
2 Ядра
4Gi
2
1
replicated-worker-1
ЗАПУЩЕНА
15.04.2026 11:29
10.66.10.108
nightly-e2e-replicated-5cdbf7e-6515-cpu
6 Ядер (50%)
9Gi
2
0
nfs-vm
ЗАПУЩЕНА
15.04.2026 17:11
10.66.10.72
release-test-mixed-66d22b3-b312-cpu
1 Ядро (20%)
512Mi
2
0
nfs-vm
ЗАПУЩЕНА
15.04.2026 11:29
10.66.10.102
nightly-e2e-nfs-5cdbf7e-6515-cpu
1 Ядро (20%)
512Mi
2
0


Deckhouse
Поиск
win2003iso
Проект
Обзор
Виртуализация
Виртуальные машины
Классы ВМ
Снимки ВМ
Диски ВМ
Образы дисков
Снимки дисков
IP адреса
Контейнеризация
Все контроллеры
Deployments
StatefulSets
DaemonSets
Проекты / Пользовательские неймспейсы / win2003iso / Виртуализация / Виртуальные машины
win2003std
ЗАПУЩЕНА
IP 10.66.10.49
Класс generic
2 Ядра / 4Gi
Диска 2
Образ 1
АГЕНТ
Конфигурация
Мониторинг
События
VNC
TTY
Сетевые политики
Снимки
Мета
YAML
Параметры машины
Класс машины
generic
Процессор
Ядер *
spec.cpu.cores
2
1
31
Доля ЦП
100%
Память
Размер *
spec.memory.size
4Gi
1Gi
121.19Gi
Тип ОС
spec.osType
Windows
Загрузчик
spec.bootloader
BIOS


Deckhouse
Поиск
win2003iso
Проект
Обзор
Виртуализация
Виртуальные машины
Классы ВМ
Снимки ВМ
Диски ВМ
Образы дисков
Снимки дисков
IP адреса
Контейнеризация
Все контроллеры
Deployments
StatefulSets
DaemonSets
Проекты / Пользовательские неймспейсы / win2003iso / Виртуализация / Виртуальные машины
win2003std
ЗАПУЩЕНА
IP 10.66.10.49
Класс generic
2 Ядра / 4Gi
Диска 2
Образ 1
АГЕНТ
Конфигурация
Мониторинг
События
VNC
TTY
Сетевые политики
Снимки
Мета
YAML
kind: VirtualMachine
metadata:
annotations:
kubectl.kubernetes.io/last-applied-configuration: |
{"apiVersion":"virtualization.deckhouse.io/v1alpha2","kind":"VirtualMachine","metadata":{"anno
kubevirt.io/disablePCIHole64: "true"
creationTimestamp: 2025-10-03T11:15:33Z
finalizers:
- virtualization.deckhouse.io/vm-cleanup
generation: 2
name: win2003std
namespace: win2003iso
resourceVersion: "2503689355"
uid: 11eed3db-26f3-4b79-9be1-fa7ac8289dd8
spec:
blockDeviceRefs:
- kind: VirtualImage
name: win2003iso
- kind: VirtualDisk
name: win2003
bootloader: BIOS
cpu:
coreFraction: 100%

Подсистема «Кластер Kubernetes»

Поддерживаемые версии Kubernetes — 1.29 и 1.31

Модуль registry

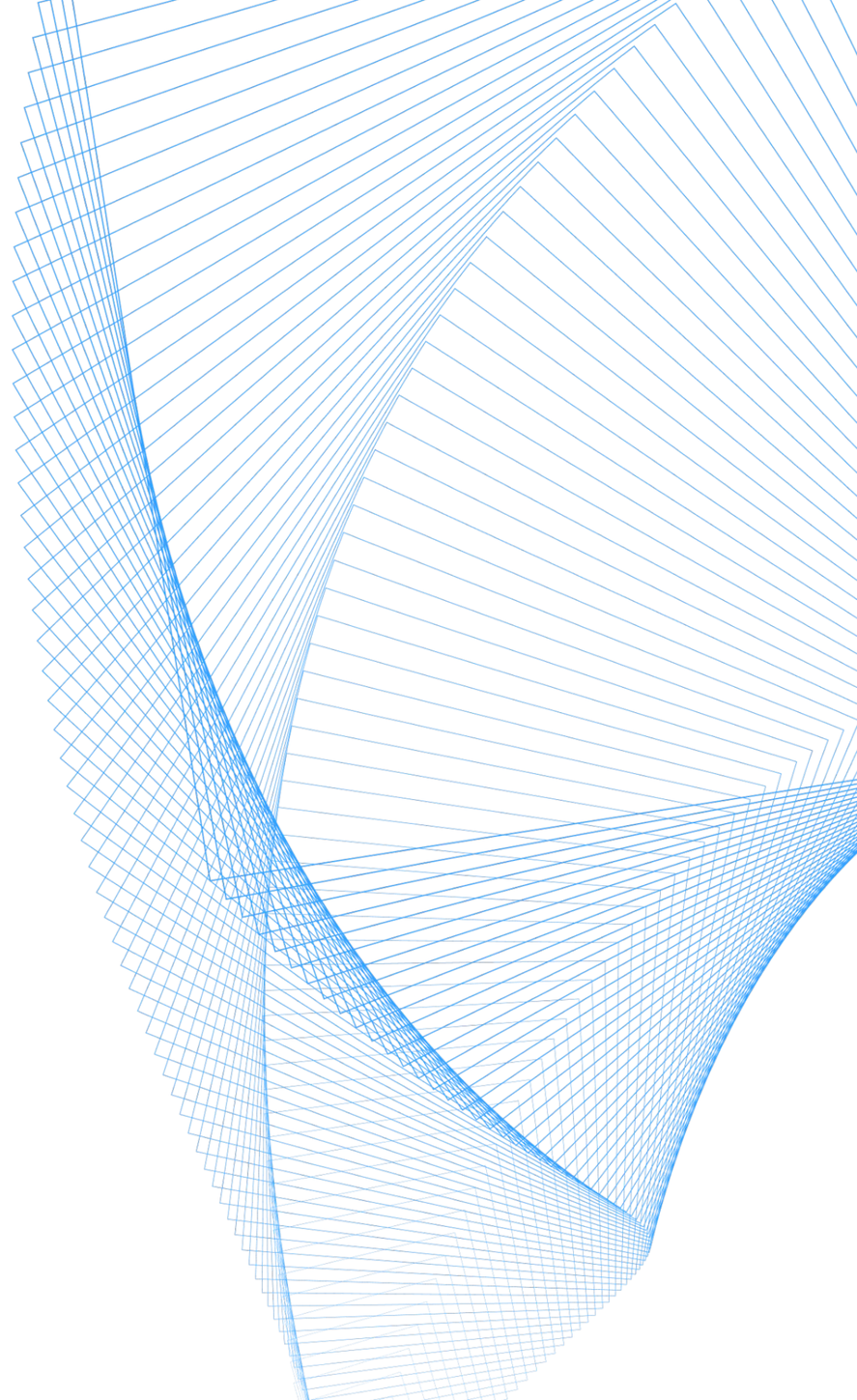
- Управляет настройками репозитория с дистрибутивом платформы
- Упрощает развёртывание в закрытом контуре

Модуль commander

Централизованное управление кластерами Deckhouse Platform через веб-интерфейс или API

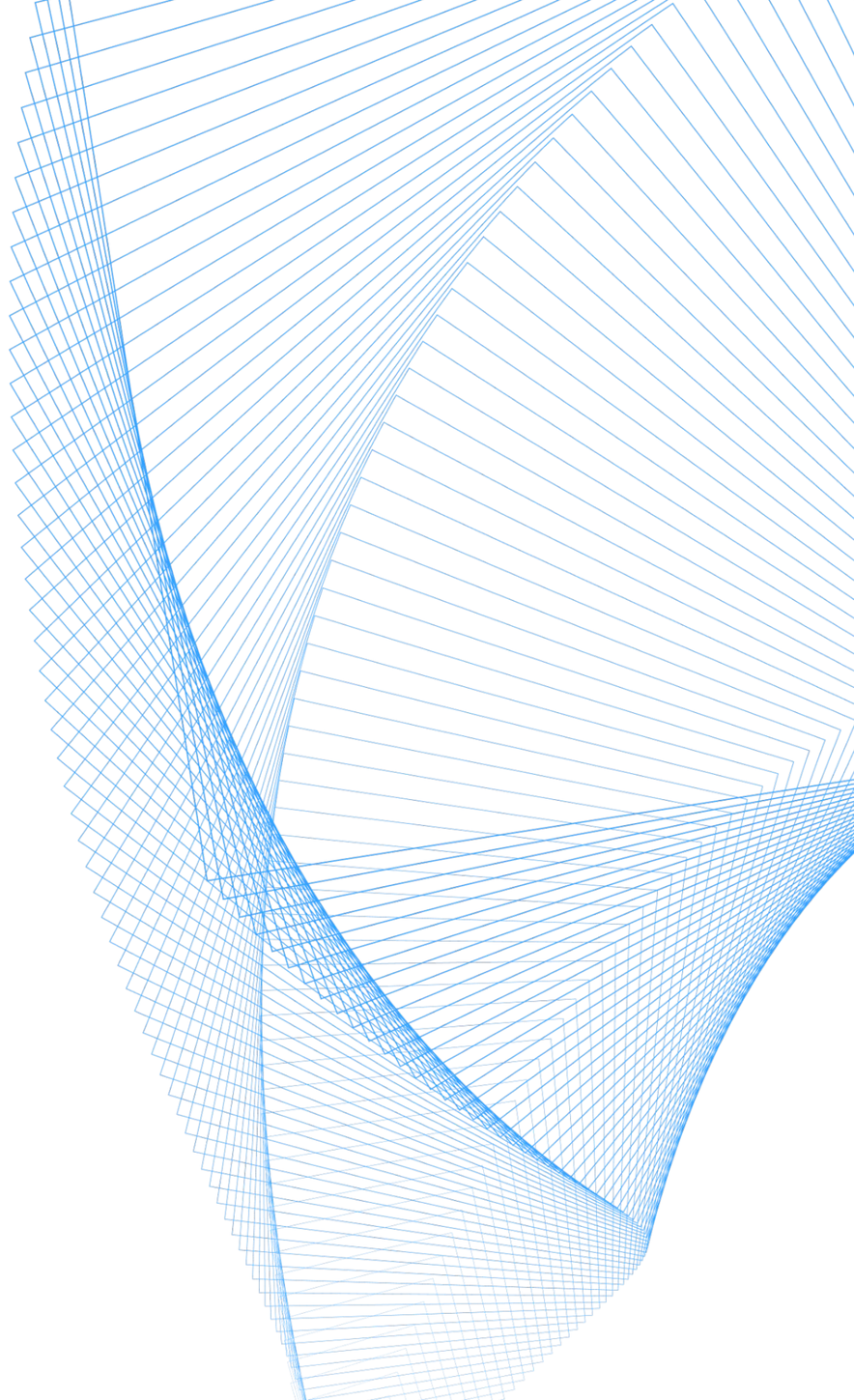
Модуль commander-agent

Агент взаимодействия с управляемыми кластерами: синхронизация ресурсов и сбор телеметрии



Управление кластерами с помощью Commander в КИИ / ЗОКИИ

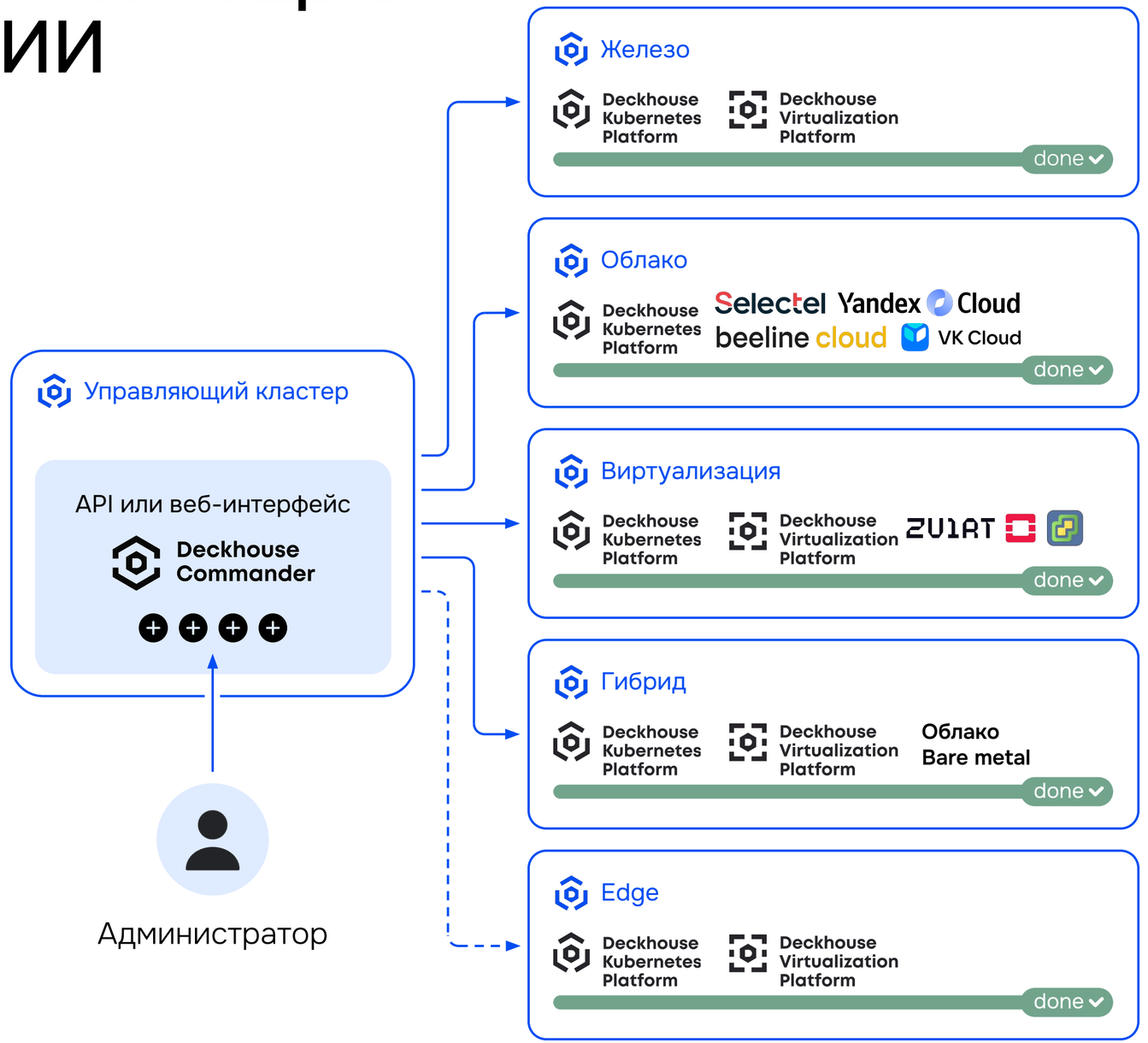
- Простое администрирование распределённой инфраструктуры (Bare metal / Private cloud)
- Установка кластеров DKP и DVP в закрытых окружениях
- Прозрачный аудит действий
- Исключение дрейфа конфигураций



Управление кластерами с помощью Commander в КИИ / ЗОКИИ

Возможности централизованного управления

- **Веб-интерфейс и API**
  Единая точка управления множеством кластеров
- **История изменений**
  Точка аудита и контроля любых производимых изменений
- **Инвентарь**
  Структурированное хранение и лёгкий доступ к справочникам
- **Шаблоны конфигураций**
  Соответствие стандартам безопасности и исключение дрейфа конфигураций для кластеров



Подсистема «Мониторинг»

Единый мониторинг для виртуальных машин и контейнеров

Модуль observability

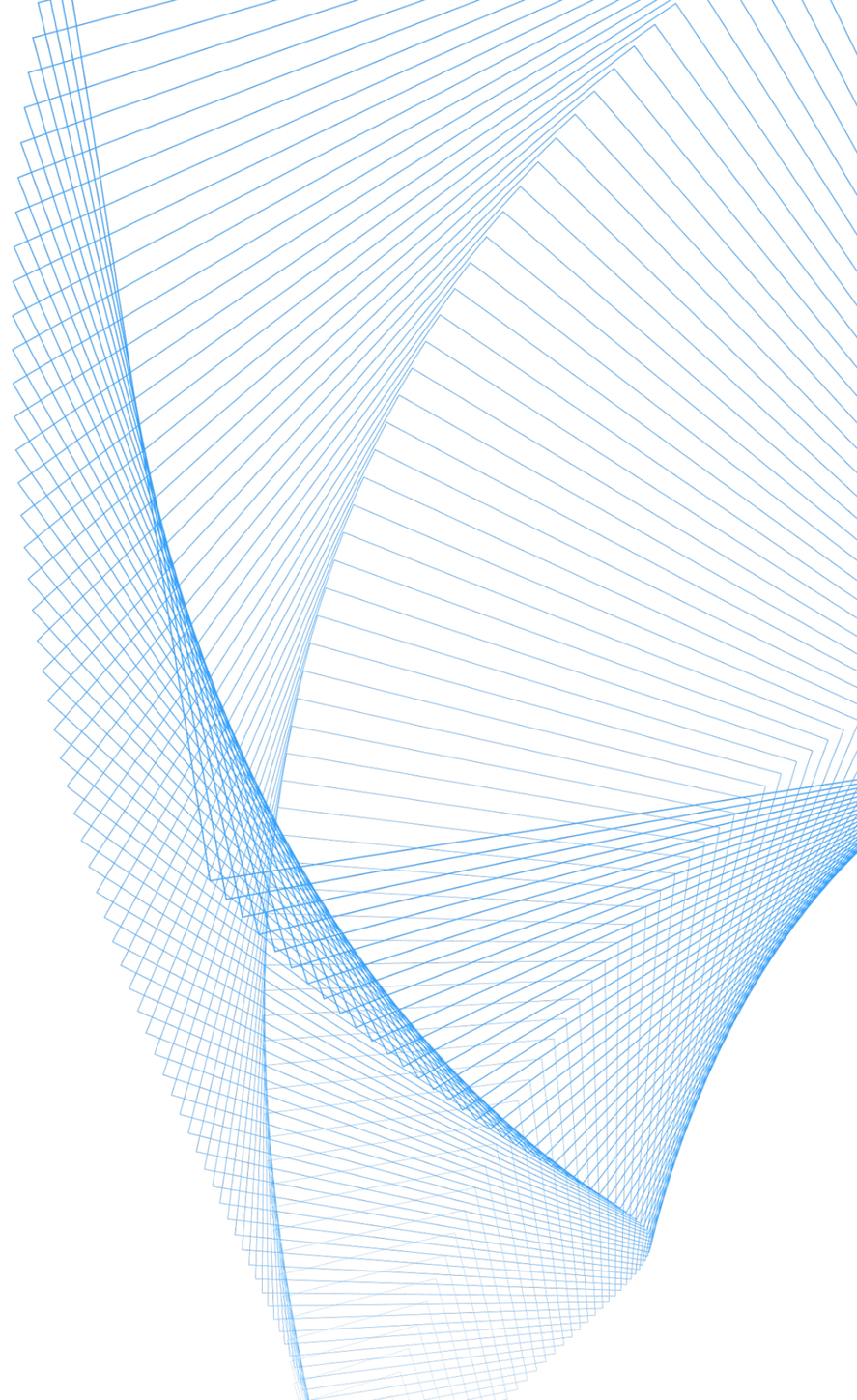
- Расширяет возможности мониторинга и отображение в веб-интерфейсе
- Дает гранулярный контроль доступа к данным мониторинга (мультитенантность)

Модуль upmeter

Проверяет доступность платформы и состояние компонентов кластера в реальном времени

Модуль prompp

Эффективный сбор и хранение метрик (до 8 раз меньше потребление памяти по сравнению с Prometheus)



General

Running VM Count	Migrating VMs	CPU Count for active VMs	Memory allocated for running VMs	Storage allocated
56	0	115	323 GiB	5.50 TiB

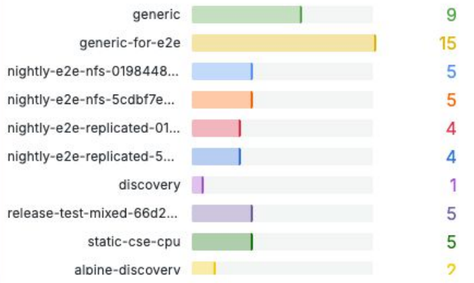
Namespaces

Namespace	Total VM	Active VM Cou	Migrating VM	CPU	Memory	VirtualDisks	Storage	VDSnapshot	VirtualImages	VMSnapshot	Service LB	Service NodeP
a-toreniyazov	6	3	-	3.00	3.97 GiB	6	10 GiB	-	1	-	-	-
aqa-test-nam...	2	2	-	21.00	2.79 GiB	2	1.95 GiB	-	-	-	-	-
commander-e...	1	1	-	2.00	2.33 GiB	1	20 GiB	-	1	-	-	1
console-review	2	2	-	1.10	2.64 GiB	13	105 MiB	4	11	15	-	-
d-antoshin	1	1	-	1.50	1.34 GiB	1	1.50 GiB	-	-	-	-	-
daniils-project	11	8	-	8.00	10.7 GiB	42	121 GiB	11	9	5	-	-
default	1	1	-	1.50	1.34 GiB	1	1.50 GiB	1	3	2	-	1
dprytkov	3	3	-	3.00	4.16 GiB	7	2.99 GiB	1	-	1	-	-
Total	100	56	0	115.30	323 GiB	189	5.50 TiB	25	50	29	1	9

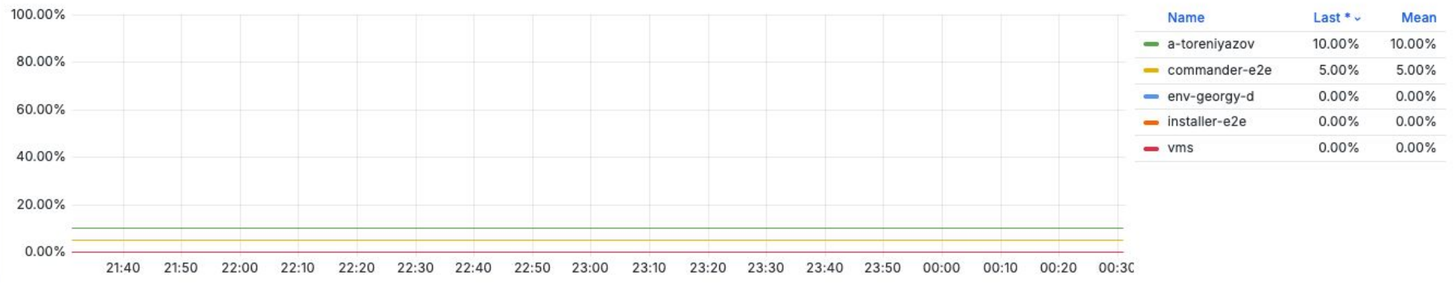
VM details *(3 panels)*

CPU details

VMs by VMClass



CPU quota usage %



Подсистема «Хранение данных»

Управление хранилищами для любых типов пользовательской нагрузки

Модуль csi-yadro-tatlin-unified

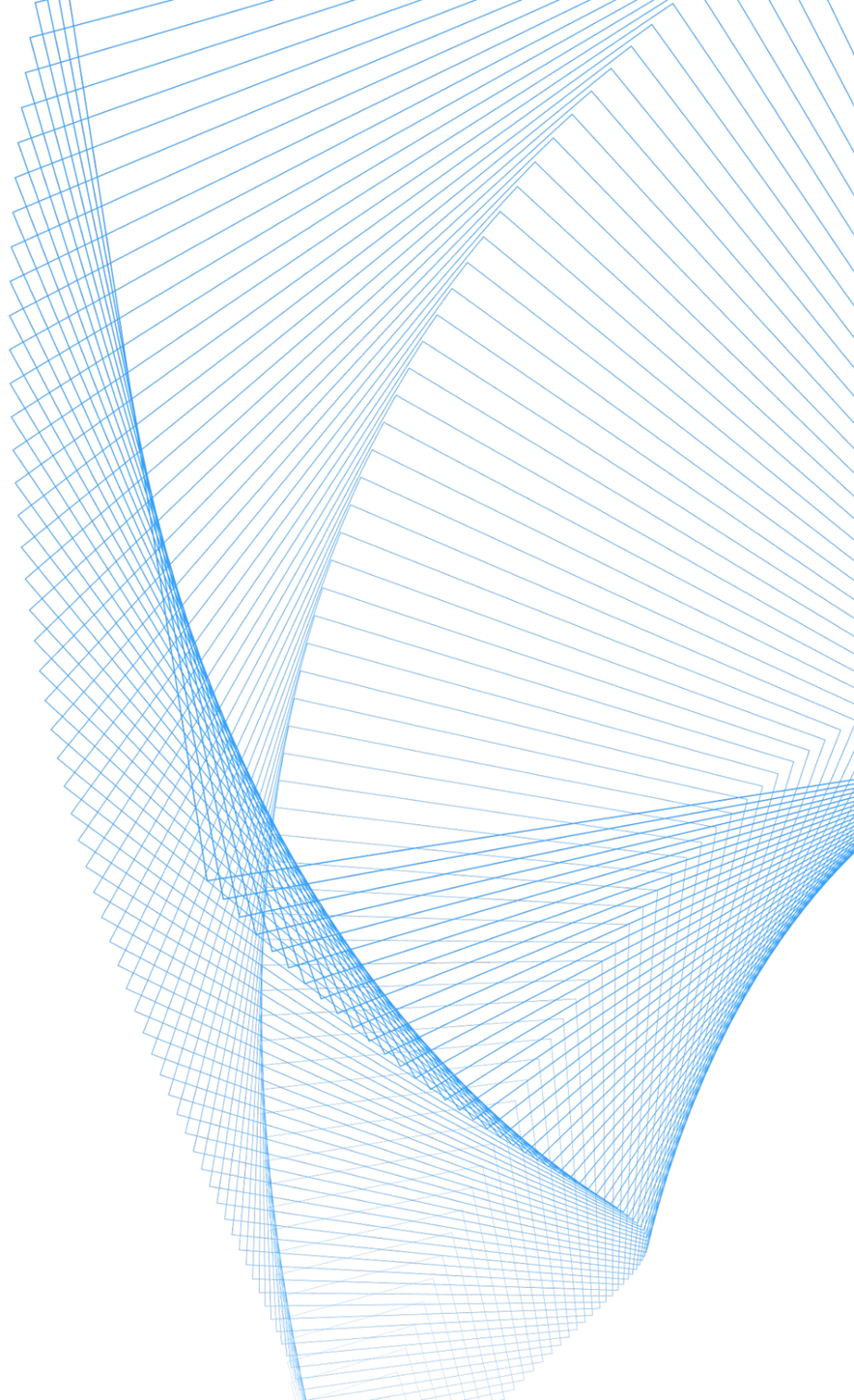
Автоматическое управление томами СХД TATLIN.UNIFIED с использованием API

Модуль csi-scsi-generic

Универсальный механизм для использования томов СХД, подключённых по протоколу SCSI

Модуль storage-volume-data-manager

Безопасный экспорт и импорт PVC и дисков ВМ для задач резервного копирования



Deckhouse
ФЛАНТ
×

Возможности Deckhouse и СХД TATLIN.UNIFIED от YADRO

Интеграция с СХД TATLIN.UNIFIED от YADRO прошла тестирование и позволяет:

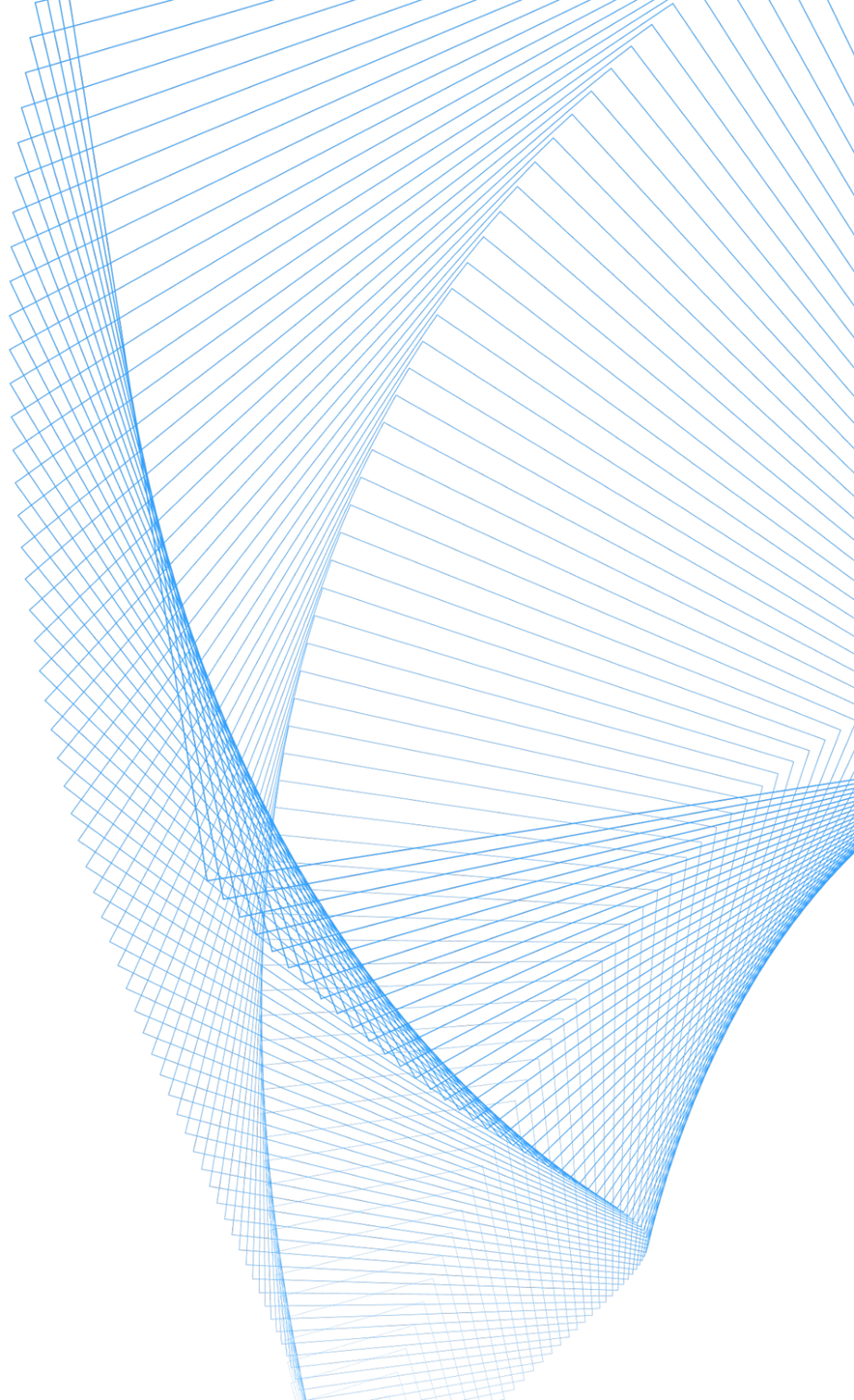
- Автоматически создавать и использовать высокопроизводительные ресурсы хранения для виртуальных машин и контейнеров
- Использовать нативный функционал СХД для создания снимков, клонирования и экспорта данных

Доступный функционал:

Автоматический заказ / высвобождение томов

Online-увеличение размера тома

Мгновенные снимки и восстановление томов из них



Подсистема «Инфраструктура»

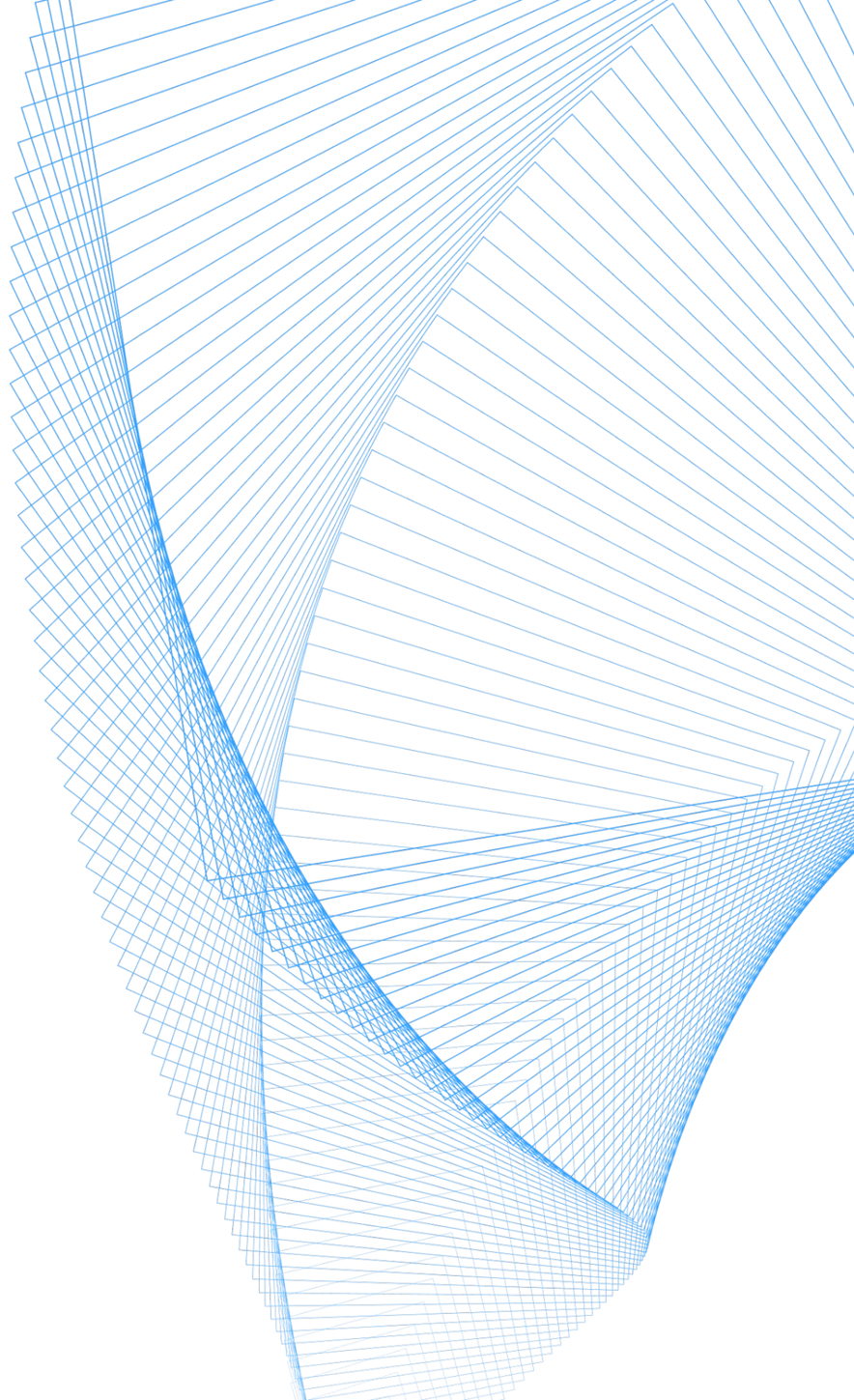
Автоматизация управления инфраструктурой

Модуль cloud-provider-dvp

Автоматизация развёртывания кластеров DKP на DVP. Используется Deckhouse Commander для создания кластеров Kubernetes «по клику»

Модуль terraform-manager

Модуль предоставляет инструменты для работы с Terraform в кластере Kubernetes

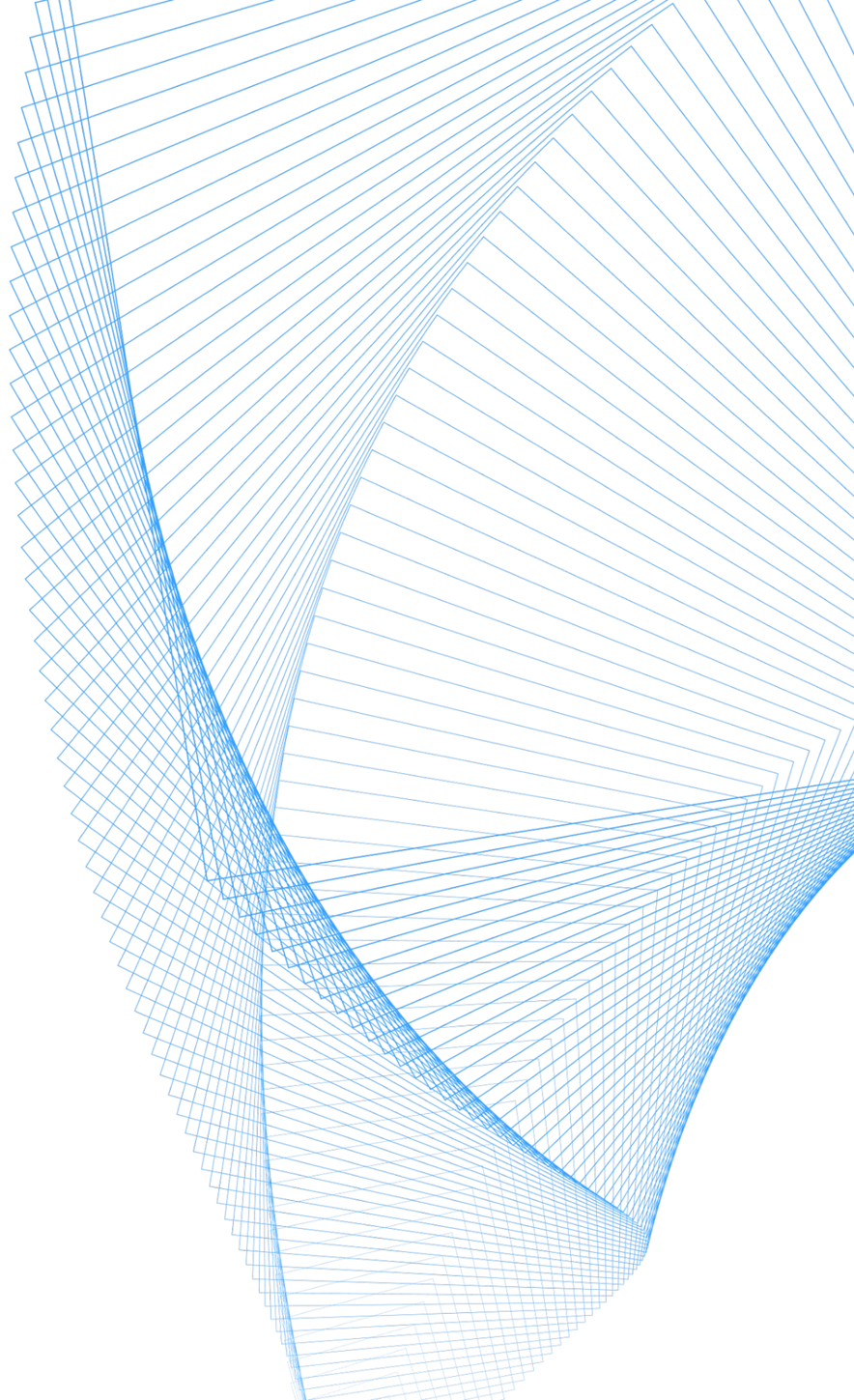


Внесение изменений и обновления DKP CSE

01 Новые версии DKP CSE выпускаем примерно каждые 6 месяцев. Информацию обо всех версиях DKP CSE и инструкции по обновлению размещаем на сайте

02 Внесение изменений в DKP CSE, связанных с добавлением новых функций безопасности информации, или внесение изменений в имеющиеся функции безопасности информации проводится с привлечением испытательной лаборатории

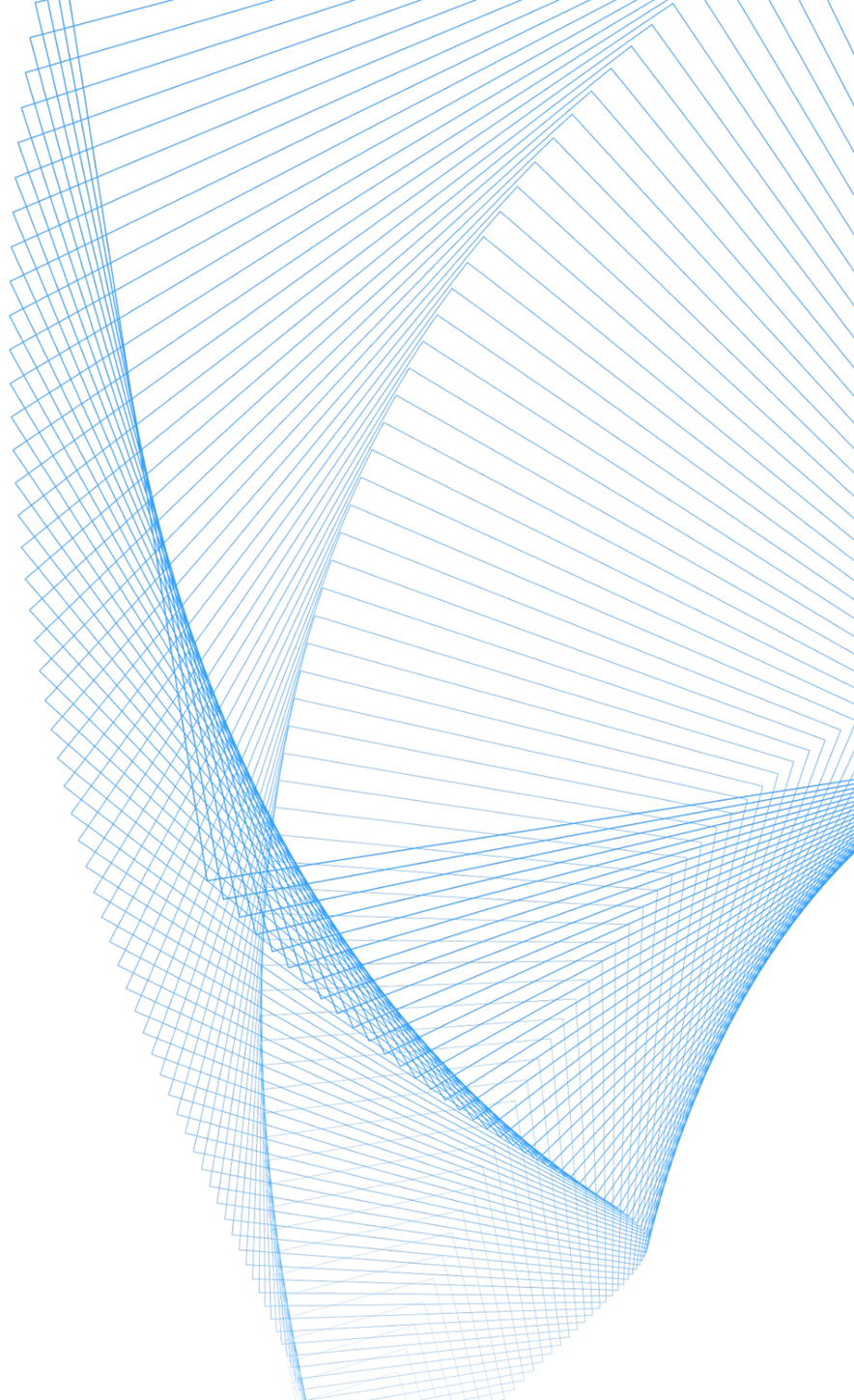
03 При внесении в DKP CSE изменений, не связанных с функциями безопасности, испытания проводятся самостоятельно силами вендора



Внесение изменений и обновления DKP CSE

04 Находимся в процессе получения сертификата соответствия процедурам разработки безопасного программного обеспечения (РБПО). Сертификат позволит проводить все испытания самостоятельно

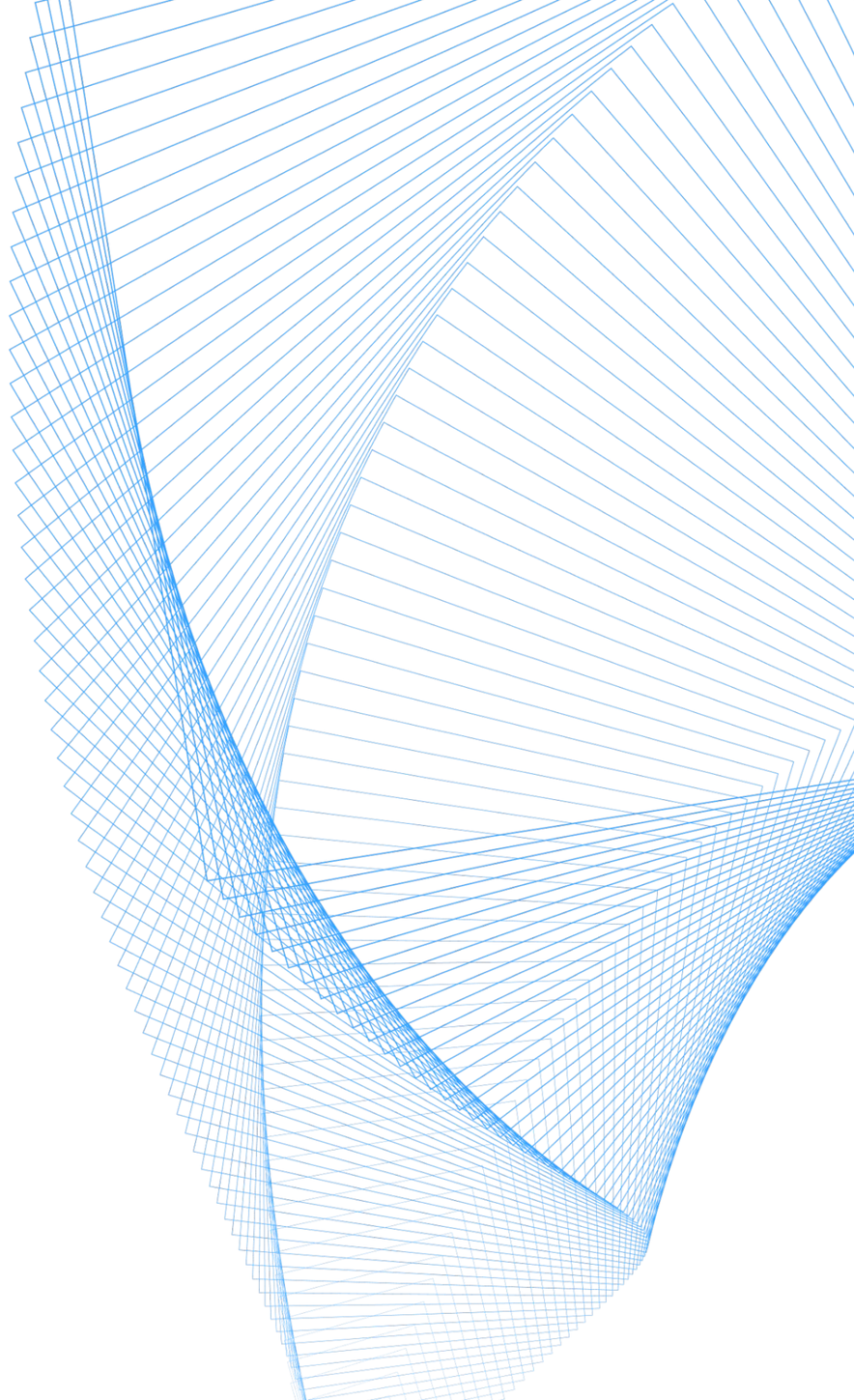
05 Первичная поставка DKP CSE — на защищённом физическом носителе. Обновления DKP CSE могут скачиваться с доверенного ресурса вендора при помощи компонента d8, который входит в состав первичной поставки DKP CSE



Процесс устранения уязвимостей DKP CSE

01 В случае обнаружения недостатков (уязвимостей) в DKP CSE в течение 48 часов разрабатываем компенсирующие меры по защите информации или ограничения по применению DKP CSE, направленные на снижение возможности эксплуатации выявленных недостатков (уязвимостей)

02 Доработка DKP CSE, в том числе разработка обновлений или мер по защите информации, нейтрализующих недостаток, выполняется в течение 60 дней с момента выявления недостатка



Промокод
от Deckhouse Академии

CSEPRO15*

Этот промокод даёт скидку 15 %
на все курсы от Deckhouse Академии

Присылайте промокод на почту
contact@deckhouse.ru

Все курсы Deckouse Академии

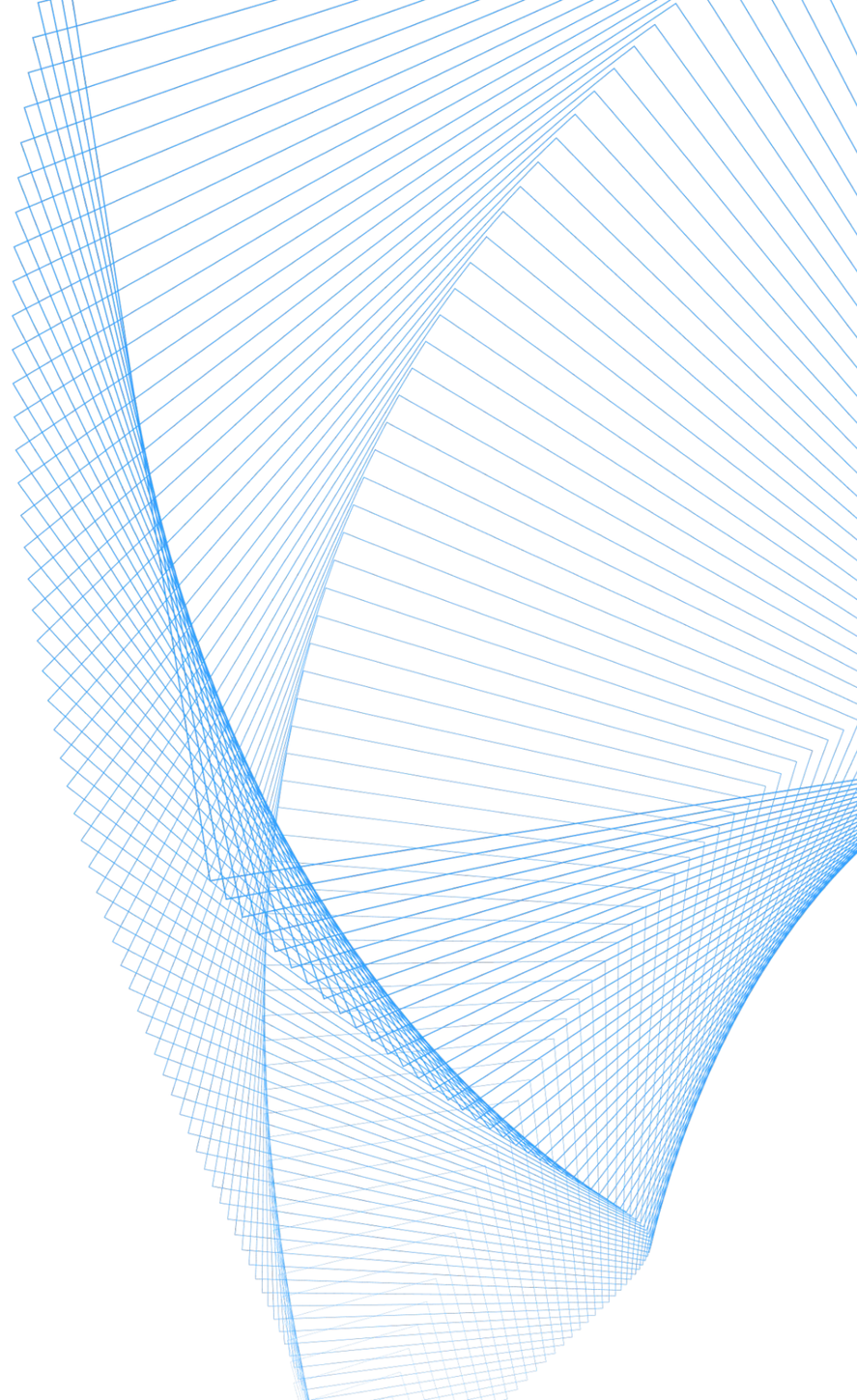
* Промокод действует по 24 мая 2026 года включительно

Deckhouse
Kubernetes Platform

Deckhouse
Virtualization Platform

Бескомпромиссная платформа для решения любых инфраструктурных задач

Выбирайте подходящее исполнение — виртуализация, контейнеры или совместная нагрузка — и управляйте инфраструктурой в едином сертифицированном контуре без дополнительных переаттестаций



Deckhouse
Kubernetes Platform

Deckhouse
Virtualization Platform

Получите чек-лист ЗОКИИ

Оцените комплексную безопасность компании и вашу готовность на соответствие требованиям регуляторов, рискам, а также общую устойчивость систем