

beeline **cloud**

Флант + beeline cloud: Deckhouse в безопасном облаке. Вызовы и задачи.

Александров Вячеслав Андреевич

Директор по развитию бизнеса,
АО «Флант»

☎ + 7 (916) 703-47-32

✉ vyacheslav.aleksandrov@flant.ru

Еремин Максим Дмитриевич

Руководитель направления развития
продуктов (PaaS+Big Data), beeline cloud

☎ + 7(926)227-28-56

✉ meremin@datafort.ru



Ф Л А Н Т



Ф Л А Н Т

Эксперты в DevOps и инфраструктуре

Профиль: отказоустойчивость, Kubernetes – оркестрация контейнеров, DevOps – сопровождение разработки.

Единственный российский вендор, входящий в TOP-200 компаний в мире — контрибьюторов в Kubernetes

В декабре 2022 в версию Kubernetes 1.26 включено улучшение платформы (KEP), предложенное и реализованное Flant ([cnews](#)).

Сертификация CNCF

Первый в России сертифицированный поставщик услуг по Kubernetes.

Более 5 лет опыта в Kubernetes

Опыт построения инфраструктуры для 1000+ компаний.

**РОССИЙСКИЙ РАЗРАБОТЧИК,
СОЗДАЮЩИЙ ПО МИРОВОГО
УРОВНЯ**

15

лет опыта

На рынке с 2008 года

6000+

серверов

Под нашим управлением

150+

компаний

Доверяют Флант
свой продуктив

CNCF

№1 в России

30k

приложений

Работают на решениях
Флант



АРПП

Отечественный софт

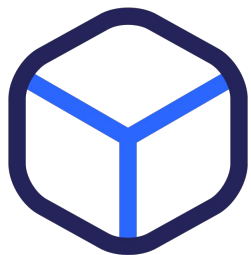
Флант входит в ассоциацию разработчиков программных продуктов «Отечественный софт»

ИТ-инфраструктура: вызовы и задачи

- Обеспечение надёжности production-сред
- Не хватает компетенций и технологической зрелости по определенным задачам
- Высокие расходы в процессах выстраивания и поддержки инфраструктуры
- Зависимость от иностранного программного и аппаратного обеспечения
- Перегружены команды и отдельные специалисты
- Низкая утилизация, автоматизация, производительность и т.д.
- Не удастся объединить большое количество платформенных наработок в целостное решение, переносимость ПО
- Низкие показатели "Time to market" для новых приложений. Медленный процесс разработки и поставки продуктов (из-за недостатка технологических практик, стандартов и подходов)

Что включает современная инфраструктура:

1



Контейнеры

Docker, containerd

2



Системы оркестрации

Kubernetes, Deckhouse, OpenShift

3



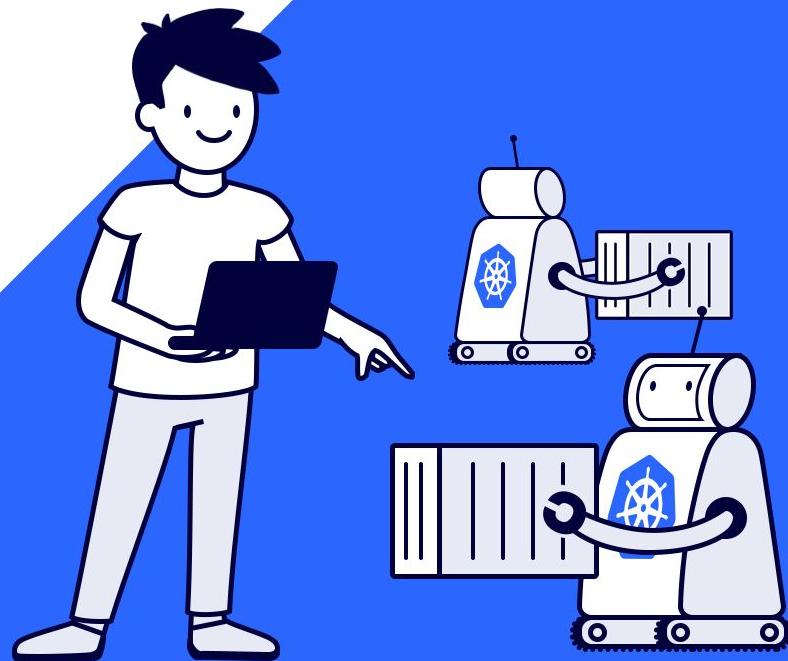
DevOps-методология

Практики, инструменты, процессы

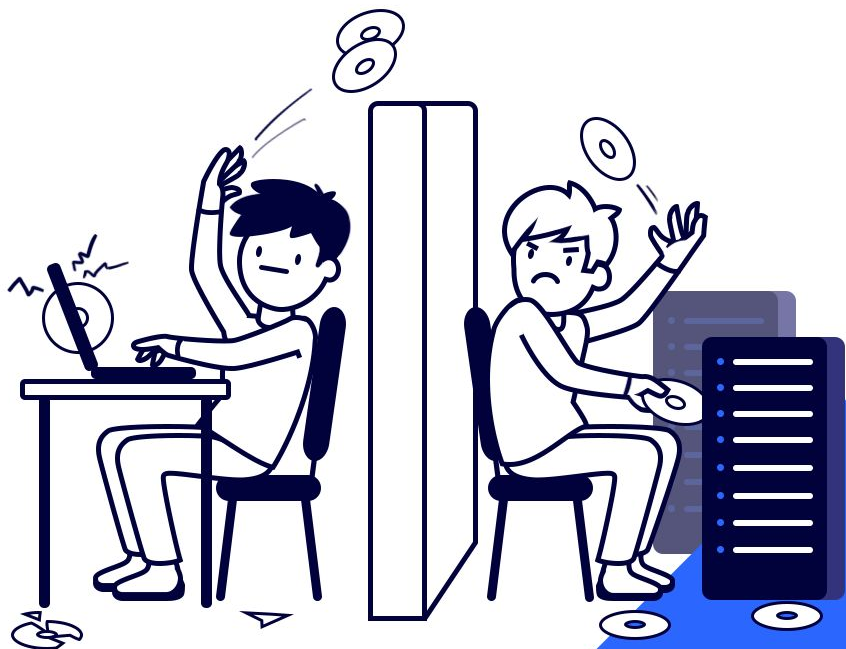
1 Контейнеры



2 Системы оркестрации



3 DevOps-методология

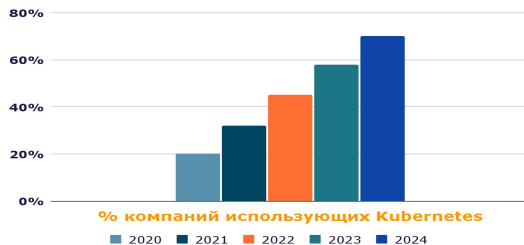


Аналитика

По данным «Инфосистемы Джет»,

более **45%** российских компаний уже используют контейнеры в production

<https://habr.com/ru/company/ietinfosystems/blog/539404/>



По прогнозам IDC,



К **2024** году **70%** всех компаний в мире будут применять приложения в контейнерах

IDC Container Infrastructure Software Market Analysis, April 2020

beeline cloud



Среда управления контейнерами

<i>Сделать самостоятельно на базе Open Source</i>	<i>Использовать готовые платформы</i>	
<ul style="list-style-type: none">❓ Команда и экспертиза?❓ Бюджет на R&D?❓ Время?❓ Готовность к риску?	 <ul style="list-style-type: none">❓ Законно и безопасно?❓ Как покупать?❓ Гарантия поддержки?❓ Как получать обновления?	 <ul style="list-style-type: none">✓ Надежность✓ Прогноз бюджета и сроков✓ Экспертная поддержка✓ Российский вендор✓ Российское Облако✓ Скорость развертывания✓ Неограниченные масштабируемые ресурсы

Production-ready-платформа включает



Контроль:
мониторинг и алертинг



Масштабирование:
вертикальное/горизонтальное



Управление сетью и DNS



Балансировка нагрузки

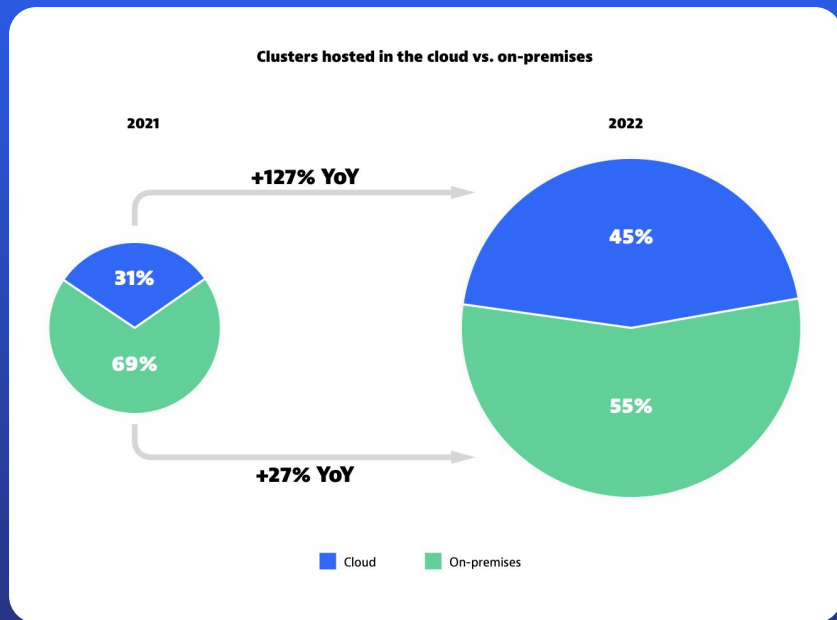


Средства
информационной безопасности

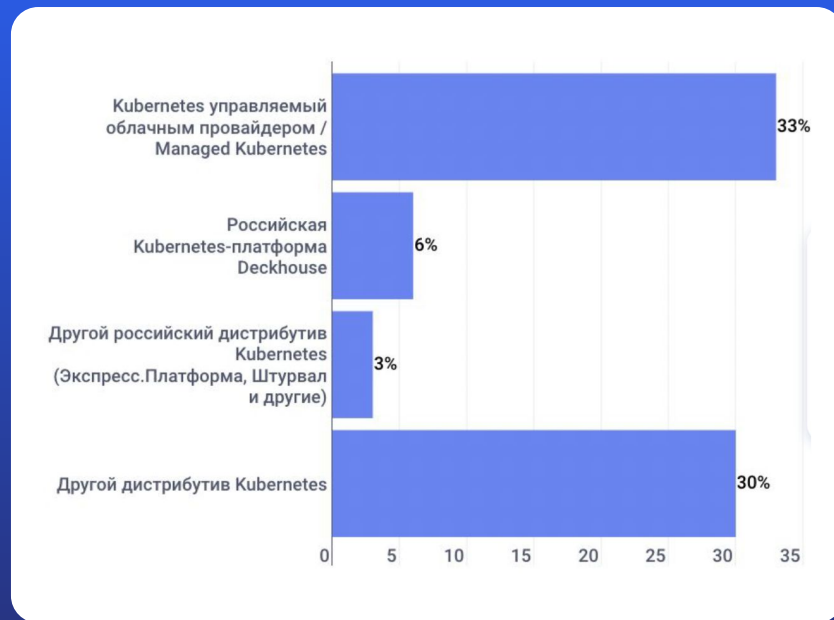


Запускается на «железе»,
VM, в облаках, а также в гибридных средах

Где больше кластеров: в облаке или «на площадке»?



Источник: «Kubernetes in the wild: 2023»,
Dynatrace.



Источник: «Исследование состояния DevOps в России», 2023,
Экспресс 42

Опыт эксплуатации Deckhouse

>6

лет эксплуатации

Зрелый продукт, сотни проектов

>250

Kubernetes-кластеров

Функционируют под управлением Deckhouse

>50

разработчиков

Талантливые разработчики
и заботливая поддержка

99.99%

SLA по всем кластерам

Фактические
значения

24/7

поддержка

Круглосуточная помощь
в любой ситуации



beeline cloud



Альфа-Лизинг



TINKOFF



Все инструменты .ru

отпбанк
Банк готовых решений

Больше историй успеха:

<https://deckhouse.ru/success-stories/>



Как использовать Kubernetes:

NoOps-подход

Вы занимаетесь тем, что действительно важно

Масштабирование

Резервные узлы
в «горячем» резерве

Соответствие требованиям

Kubernetes CIS Benchmark,
PCI SSC, настройка аудита
событий Kubernetes API

“Кластер под ключ”

Предоставляется
кластер с полным
набором
дополнительных
модулей

Observability

Быстрая настройка
мониторинга ваших
приложений

Контроль

Встроенные политики
безопасности
и сканирование
на уязвимости



beeline cloud

beeline cloud в цифрах:

100+

Облачных сервисов и решений

2000+

Клиентов из разных отраслей бизнеса

99,95%

Облачный SLA

6

ЦОДов в РФ уровня Tier III

5

Независимых интернет-провайдеров

Secure by Design
УЗ-1 152-ФЗ

Публичное облако

ГИС К1,
ИСПДн УЗ-1

Изолированный сегмент

ГОСТ Р
57580.1-2017

Первый уровень защиты информации

PCI DSS
3.2.1

Соответствие стандарту

ФСБ,
ФСТЭК

Лицензии

Партнеры

kaspersky



MULTIFACTOR



UserGate



positive technologies



ARENADATA



radware

COMMUNIGATE
SYSTEMS



Ф Л А Н Т

О нашей инфраструктуре

Cloud Director 10

Панель управления облаком

- Средства самообслуживания (self-service)
- Автоматизация рутинных задач
- Режим коллективной аренды (multi-tenancy)

vCenter 7x

Платформа управления виртуализацией

- Высокая доступность
- Мониторинг
- DRS

VMware ESXi

Гипервизор корпоративного уровня

- Программно-определяемый ЦОД
- Кластер высокой доступности

Изолированное обслуживание (NSX)

Платформа виртуализации сети

- Воспроизведение полной модели сети программным образом

СХД

- Высокопроизводительные SSD- и флэш-накопители
- Интерфейс подключения 2 x 32G FC (SAN)

ЦОД Tier III

- Сертификация Uptime Institute
- Дублирование критичных компонентов на физическом уровне

High-End сетевое оборудование

- Leaf-Spine-топология
- Высокая производительность
- Неблокирующая пропускная способность

High-End серверное оборудование

Надежные серверы с многократным запасом ресурсов

- Гиперконвергентная инфраструктура
- Масштабируемые процессоры Intel® Xeon® 3-го поколения
- Software Guard Extensions (Intel® SGX)

Сервисы beeline cloud

Cloud Compute

Публичное облако

Виртуальная инфраструктура (IaaS) для создания цифровых продуктов

Cloud backup

Резервное копирование

Резервное копирование в облако локальной инфраструктуры и персональных данных

Cloud NGFW

Межсетевой экран нового поколения

Комплексная защита сетевого периметра с использованием межсетевого экрана поколения Next-Generation

MFA

Многофакторная аутентификация

Сервис многофакторной аутентификации для защиты доступа к корпоративным ресурсам и веб-приложениям

Private Platform

Частное облако

Self-service-платформа для управления частным облаком

Cloud MailGate

Сервис корпоративных коммуникаций

Комплексная платформа коммуникаций для корпоративного общения

DDoS Protection

Защита от DDoS-атак

Непрерывная защита от DDoS-атак любого уровня сложности

Cloud BI

Облачный сервис аналитики данных

Сервис визуализации и аналитики данных в облаке для подхода Business Intelligence

Cloud 152

Инфраструктура под Ф3-152

Размещение и обработка персональных данных в защищенном облаке Ф3-152

Cloud Workspace

Платформа офисного пространства

Инструменты и бизнес-приложения для общения, хранения данных и совместной работы

Web Application Firewall

Защитный межсетевой экран для приложений

Защита веб-приложений от SQL-инъекций, XSS-скриптинга и прочих OWASP-угроз

Cloud Kubernetes Clusters

Enterprise-Kubernetes кластеры

Кластеры Kubernetes для больших инсталляций на гарантированных ресурсах

Managed Kubernetes

Управление кластерами Kubernetes

Сервис для оперативного развертывания кластеров Kubernetes любой конфигурации

SSL VPN

Удаленный доступ по технологии SSL VPN

Сервис шифрования каналов связи для защищенного удаленного доступа к корпоративным ресурсам

Secure Email Gateway

Защита электронной почты

Шлюз безопасности для защиты электронной почты от различных угроз, включая спам, фишинг и все виды вредоносных вложений

Cloud Arenadata DB

Аналитическая СУБД в облаке

Массово-параллельная СУБД Greenplum в облаке для аналитической работы с данными

Кейс

Ситуация

- Крупная финансовая организация разрабатывает приложение для обработки платежей
- В разработке участвуют множество систем хранения и передачи данных
- Нагрузка свыше миллиона транзакций в секунду, целевой RPS – 1 000 000

Проблема

- Долго и сложно масштабировать инфраструктуру, построенную на виртуальных машинах, под растущие запросы клиентов
- Необходимо упростить обеспечение безопасности передачи данных от системы к системе на back-end'e
- Трудно встроить приложение в уже существующую инфраструктуру из-за огромного legacy

Решение

- Использование микросервисной архитектуры в облаке
- Использование kubernetes как сервис на виртуальной инфраструктуре
- Переход на практики devops для быстрого перевода кода в prod
- Использование масштабируемой архитектуры

Выгода

- Скорость разработки вырастает в 2 раза
- Автоматическое масштабирование в облаке позволит повысить отказоустойчивость и не пропустить ни одной транзакции
- Сервисы обеспечения безопасности защитят трафик и работу с данными клиентов
- Перевод CAPEX в OPEX и экономия до 20% бюджетов

Deckhouse в облаке beeline cloud



Гарантированные ресурсы



Тест-драйв 1 месяц



Поддержка Terraform



Мониторинг на базе Prometheus и Grafana



Актуальные версии Kubernetes



Широкий набор модулей для настройки кластера



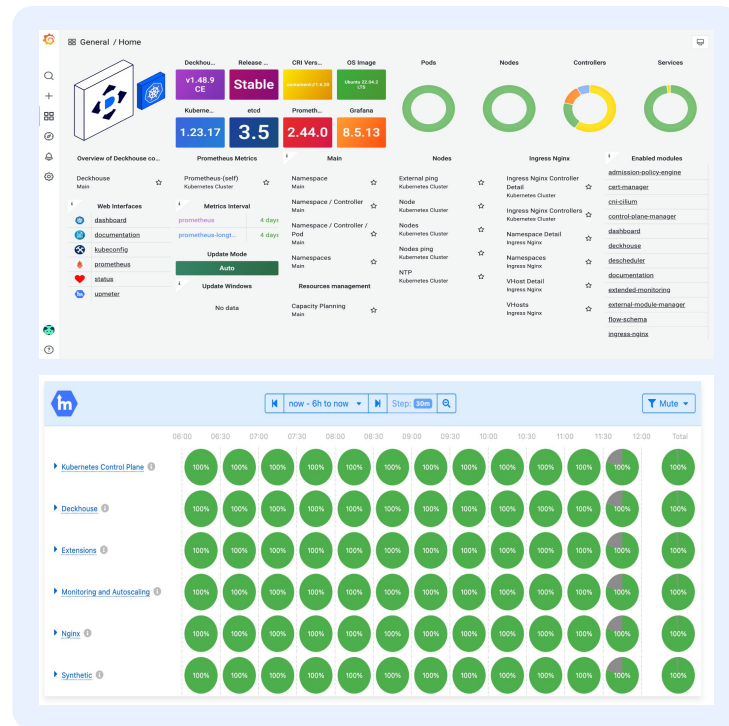
Автоматическое масштабирование и восстановление данных



API для взаимодействия с компонентами системами



Централизованное управление кластерами Kubernetes с помощью Deckhouse Commander



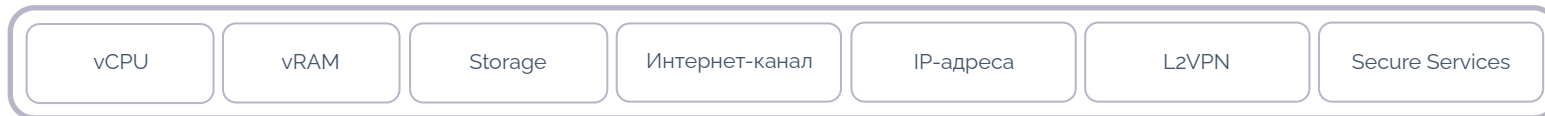
Состав платформы Cloud Kubernetes Clusters

Cloud Kubernetes Clusters

Платформа Deckhouse от Flant



Инфраструктура



Какие задачи решает?

Изолированное управление сервисами

Вы можете разделить приложения на небольшие, независимые друг от друга сервисы и изолированно управлять ими без критического влияния на продукт

1

Стабильная работа при пиковых нагрузках

Актуально в период высокой потребности ваших сервисов и пиковых нагрузках для обеспечения стабильной работы. Приложение автоматически масштабируется с учетом нагрузки

2

Повышение скорости CI/CD-процессов

Автоматизация операций в рамках процесса запуска и тестирования кода в облачной инфраструктуре для уменьшения time-to-market более чем в 2 раза с помощью модуля ArgoCD

3

Что делать с безопасностью и доступностью?

Пользователи

- RBAC и 7 преднастроенных групп с возможность расширения и изменения по правам доступов
- Внешняя аутентификация и авторизация с помощью LDAP/OIDC
- Сквозная аутентификация на базе dex

1

Угрозы

- Анализ уязвимостей и угроз приложений на базе модуля Falco
- L2VPN для подключения по защищенным каналам от кластера K8S до инфраструктуры

2

Доступность

- Автомасштабирование с Autoscaler и отказоустойчивость на базе chaos monkey
- Мониторинг на базе Prometheus и Graphana с готовыми дашбордами и сбор логов Vector и Loki
- Балансировка трафика с помощью Istio

3

Deckhouse в облаке beeline cloud

Директор по ИТ

Служба безопасности

Разработчики

DevOps/SRE

Нет необходимости "раздувать" штат инженеров

Сокращение времени построения всей инфраструктуры

Изоляция данных

Прозрачность процессов

Аудит и логирование системы

Унификация всех процессов разработки и запуска

Автоматизация процессов доставки и запуска приложений

Единый стандарт и среда для запуска приложений

Автоматизация работы с данными

Сокращение количества аварий и инцидентов

Экономия ресурсов

Прозрачность

Автоматизация

Надежность

Решения принимаются на основе данных и цифр

Проверенный временем и заказчиками продукт

Поддержка от российского вендора и на русском языке

Сокращение time-to-market

Встроенные и настраиваемые пользовательские политики безопасности

Сканирование уязвимостей

Управление доступом

Независимые релизы — разработчики могут выкатывать новые версии тогда, когда им это удобно и нужно, без необходимости "записываться" в очередь к эксплуатации, а также без необходимости согласовывать релизные планы с другими командами разработки.

- отказоустойчивость
- автомасштабирование
- предсказуемость функционирования
- простота диагностики проблем
- готовая к production-среда, без необходимости "дорабатывать напильником"
- снижение расходов и оптимизация вычислительной инфраструктуры

Эффективность, удобство, безопасность

Тарификация и условия



Тарификация услуги

Платите как за инфраструктуру и получайте более высокий уровень абстракции:

- Виртуальные ядра
- Оперативная память
- Место на жестком диске
- IP-адреса и выделенный интернет-канал
- Возможность сетевой связности с помощью L2VPN
- При автомасштабировании плата за ресурсы изменяется в зависимости от нагрузки



Deckhouse в beeline cloud

- Продукт с вендорской поддержкой
- SLA 99,95%
- Возможность реализовать сетевую связность
- Выбор конфигурации в зависимости от ваших задач

beeline **cloud**

✉ sales@datafort.ru

☎ +7 (495) 967-80-10

🌐 cloud.beeline.ru



Ф Л А Н Т

✉ sales@flant.ru

☎ +7 (495) 721-10-27

🌐 www.flant.ru

Спасибо
за внимание!