DECKHOUSE

Kubernetes Platform

CERTIFIED SECURITY EDITION

Обновления и внедрения: что нового в DKP CSE, кейсы и последние требования ФСТЭК России

Спикеры

Константин Аксёнов

konstantin.aksenov@flant.ru

Директор департамента разработки Deckhouse

Ильдар Гарипов

ildar.garipov@flant.ru

Руководитель отдела информационной безопасности

План вебинара

Действующая нормативная база и требования в отношении значимых объектов КИИ

Новые функции DKP CSE и две редакции — Lite и Pro

Примеры использования DKP CSE в промышленной эксплуатации

Планы по дальнейшему развитию платформы

Новости о сертификации других продуктов экосистемы Deckhouse

Подведение итогов и ответы на вопросы

О вендоре Deckhouse

15+
лет опыта
в Open Source

С 2017
года используем
Kubernetes в production

400+
сотрудников

№1
контрибьютор в проекты
CNCF из России

>240
компаний-
пользователей

В топе
вендоров ИТ-решений для
банков* и промышленности**

Реестр
российского ПО

Лицензии
и сертификат
ФСТЭК России

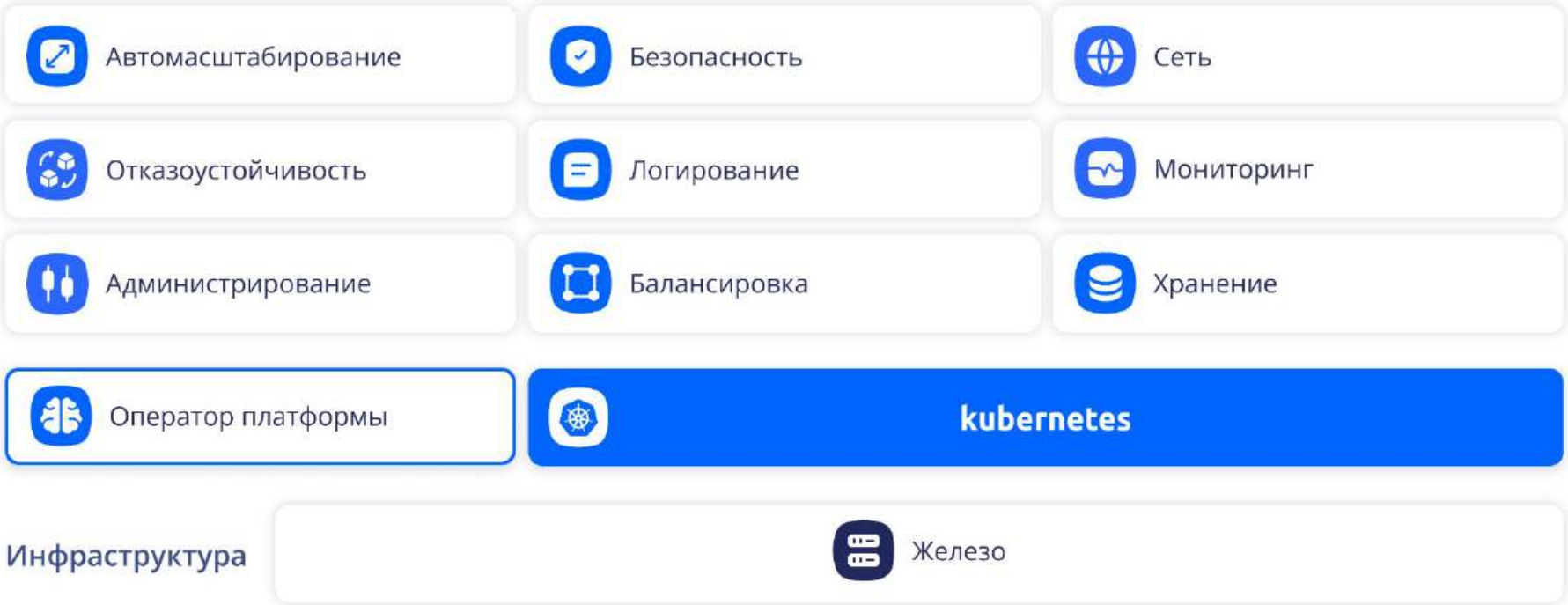
Ассоциация разработки ПО
«Отечественный софт»

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

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

Deckhouse
by Flant

Состав Deckhouse Kubernetes Platform CSE



DKP CSE vs запуск контейнеров средствами ОС

	DKP CSE	Сертифицированная ОС с ванильным K8s	Сертифицированная ОС с Docker
Оркестратор контейнеров	✓	✓	✗
Container engine	✓	✓	✓
Автоконфигурирование управляющих компонентов Kubernetes	✓	✗	✗
Преднастроенная сеть и готовые варианты балансировки	✓	✗	✗
Управление конфигурацией узлов кластера	✓	✗	✗
Встроенный мониторинг и логирование	✓	✗	✗
Масштабирование приложений по любым метрикам	✓	✗	✗
Управление хранилищем и различные возможности хранения	✓	✗	✗
Отказоустойчивая конфигурация и резервирование «из коробки»	✓	✗	✗
… и ещё несколько десятков тесно связанных модулей для production ready-решения	✓	✗	✗

Сертификат ФСТЭК России № 4860 от 4 октября 2024 г.

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, 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

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4860

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 4 октября 2024 г.

Выдан: 4 октября 2024 г. Переоформлен: 16 декабря 2024 г.
Действителен до: 4 октября 2029 г.

Настоящий сертификат удостоверяет, что **программное обеспечение «Deckhouse Platform Certified Security Edition»**, разработанное и производимое АО «Флант», является средством контейнеризации, соответствует требованиям по безопасности информации, установленным в документах «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 и «Требования по безопасности информации к средствам контейнеризации» (ФСТЭК России, 2022) – по 4 классу защиты, при выполнении указаний по эксплуатации, приведенных в формуляре RU.86432418.00001-01 30 02-1.

Сертификат выдан на основании технического заключения от 26.08.2024, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «КБ-Лаб» (аттестат аккредитации от 29.12.2020 № СЗИ RU.0001.01БИ00.Б041), экспертного заключения от 02.09.2024, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001), и технического заключения от 15.11.2024, оформленного испытательной лабораторией ООО «КБ-Лаб».

Заявитель: АО «Флант»
Адрес: 115088, г. Москва, ул. Угрешская, д. 12, стр. 4, офис 47А
Телефон: (495) 721-1027

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах субъектов информатизации допускается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Deckhouse Kubernetes Platform
Certified Security Edition

Первая полноценная платформа контейнеризации, сертифицированная ФСТЭК России, которая позволяет обеспечить:

- безопасность информации на значимых объектах критической информационной инфраструктуры до 1-й категории значимости включительно
- безопасность персональных данных в информационных системах до 1-го уровня защищённости включительно
- безопасность информации в государственных информационных системах до 1-го класса защищённости
- безопасность 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

Требования ФСТЭК России

- государственные информационные системы;
- информационные системы персональных данных;
- информационные системы, являющиеся объектами критической информационной инфраструктуры;
- отраслевые/ведомственные информационные системы;
- изменения нормативных требований.

Государственные информационные системы

Требования к государственным информационным системам установлены приказом **ФСТЭК России от 11 февраля 2013 г. № 17**, согласно п.11 *«для обеспечения защиты информации … применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации».*

Информационные системы персональных данных

Ст. 19 Федерального закона **«О персональных данных»** от 27.07.2006 № 152-ФЗ устанавливает требование: *«обеспечение безопасности персональных данных достигается … применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации».*

Разберемся с термином «процедура оценки соответствия».

Формы подтверждения соответствия

Согласно Федеральному закону от 27.12.2002 № 184-ФЗ **«О техническом регулировании»** обязательное подтверждение соответствия осуществляется в формах:

- принятия декларации о соответствия;
- обязательной сертификации.

Если с обязательной сертификацией все ясно и вопросов не возникает, то что же такое декларация соответствия?

Декларация соответствия

Согласно ст. 24 Федерального закона от 27.12.2002 № 184-ФЗ *«Декларирование соответствия осуществляется по одной из следующих схем:*

- *принятие декларации о соответствии на основании собственных доказательств;*
- *принятие декларации о соответствии на основании собственных доказательств, доказательств, полученных с участием органа по сертификации и (или) аккредитованной испытательной лаборатории (центра)».*

Фактически владельцу ИС необходимо выполнить работу испытательной лаборатории самостоятельно и сформировать доказательную базу, достаточную для использования решения для защиты информации.

Процедура оценки соответствия

Идём далее, приказом **ФСТЭК России № 21 от 18.02.2013** установлено, что меры по обеспечению безопасности персональных данных реализуются средствами защиты информации, прошедшими в установленном порядке процедуру оценки соответствия, в тех случаях, когда **применение таких средств необходимо для нейтрализации актуальных угроз безопасности** персональных данных.

В сертифицированном средстве защиты приведём перечень угроз безопасности, которым противодействует СЗИ, что подтверждается в рамках сертификационных испытаний и фиксируется в техусловиях.

Угрозы безопасности информации

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

Информационная система — объект КИИ

В соответствии с п. 18 приказа **ФСТЭК России № 235**:
*«Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться сертифицированные на соответствие требованиям по безопасности средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приёмки в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ **"О техническом регулировании"**».*

Меры по обеспечению безопасности ЗОКИИ*

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 ПО Deckhouse Platform CSE они представлены.

Данную таблицу можно использовать при проектировании системы безопасности ЗОКИИ.

**ЗОКИИ — значимый объект критической информационной инфраструктуры*

Отраслевые требования по защите информации

Положение **Центрального банка Российской Федерации от 17 августа 2023 года № 821-П** «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

Методические рекомендации Банка России по нейтрализации организациями финансового рынка угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой от 08.10.2024 № 18-МР.

В указанных документах требуется использование сертифицированных средств защиты информации.

Защита конфиденциальной информации

При создании системы защиты информации необходимо учитывать все нормативные требования.

Считаем целесообразным применение сертифицированной версии **ПО Deckhouse Platform CSE** для защиты конфиденциальной информации

Изменения нормативных требований ФСТЭК России

Проходит регистрацию в Минюсте России приказ ФСТЭК России **«Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»**.

Настоящий приказ вступает в силу с **1 сентября 2025 г.** и отменяет действие приказа **ФСТЭК России № 17**, будет использоваться для защиты всех ИС государственных органов, государственных унитарных предприятий, государственных учреждений и требует обязательного применения сертифицированных средств защиты информации.

Изменения в формате поставки

Компонент	Вид поставки
Дистрибутив ПО	В электронном виде на USB-накопителе (для первичной поставки) либо в электронном виде из registry (при обновлении)
Формуляр	На бумаге
Технические условия	В электронном виде на USB-накопителе
Руководство администратора	В электронном виде на USB-накопителе
Руководство пользователя	В электронном виде на USB-накопителе

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 приказа **ФСТЭК России № 118**, опциональные модули расширяют функциональные возможности и могут быть использованы по выбору пользователя, исходя из потребностей и сценариев использования.

Обязательные и опциональные модули позволяют нам создавать такие **редакции CSE**, как **Lite** и **Pro**. В обеих редакциях передаются права на использование всех обязательных модулей, в **Pro** дополнительно передаются права на использование опциональных модулей.

https://deckhouse.ru/products/kubernetes-platform/certified-security-edition/updates/

Редакции Lite и Pro

	Certified Security Edition Lite	Certified Security Edition Pro
Веб-интерфейс платформы	✕	✓
Инфраструктура		
Интеграция с публичными облаками	✕	Планируется: Yandex Cloud
Интеграция с частными облаками	Планируется: zVirt	Планируется: Openstack zVirt Базис.DynamiX
Безопасность		
Интеграция с внешним хранилищем секретов	✕	✓
Управление SSL-сертификатами	✕	✓
Сетевые возможности		
Встроенный балансировщик для сервисов в режиме BGP	✕	✓
Кэширование DNS на каждом узле кластера	✕	✓
Возможность объединения кластеров в режиме мультикластера или федерации	✕	✓
Визуализация сетевого стека кластера в случае, если включён Cilium CNI	✕	✓

🕒 — *планируется к включению*

Редакции Lite и Pro

	Certified Security Edition Lite	Certified Security Edition Pro
Хранение данных		
Встроенное локальное программно-определяемое хранилище	✗	✓
Встроенное реплицируемое программно-определяемое хранилище	✗	🕒
Возможность делать снимки дисков в локальном программно-определяемом хранилище	✗	🕒
Возможность делать снимки дисков в реплицируемом программно-определяемом хранилище	✗	🕒
Возможность выбрать выделенную сеть для репликации данных в реплицируемом программно-определяемом хранилище	✗	🕒
Интеграция с внешним хранилищем данных на базе Ceph или NFS	✗	✓
Интеграция с внешними хранилищами: TATLIN.UNIFIED, Huawei, HPE	✗	🕒
Виртуализация		
Возможность запуска виртуальных машин в одном окружении с контейнерами	✗	🕒
Расширенные возможности Deckhouse Virtualization Platform	✗	🕒

🕒 — *планируется к включению*

Редакции Lite и Pro

	Certified Security Edition Lite	Certified Security Edition Pro
Наблюдаемость		
Мониторинг сетевого взаимодействия между всеми узлами кластера, а также (опционально) до дополнительных внешних узлов	✗	✓
Статистика по доступности (SLA) для компонентов кластера и DKP	✗	🕒
Возможность подключить расширенный мониторинг объектов в кластере (несколько десятков дополнительных метрик с готовыми оповещениями и описаниями алертов)	✗	✓
Автоматическая настройка системы мониторинга для сбора метрик с бизнес-приложений	✗	✓
Прочее		
Режим автоматического выделения ресурсов для приложения на основе исторического потребления	✗	✓
Регулярное автоматическое перераспределение приложений по узлам кластера для оптимизации использования вычислительных ресурсов	✗	✓
Автоматическое управление аннотациями и лейблами на пространствах имён	✗	✓
Автоматический перезапуск пользовательских приложений при изменении их конфигурации (применяется для приложений, которые не умеют самостоятельно динамически обновлять конфигурацию)	✗	🕒

🕒 — *планируется к включению в 2024/25*

Сравнение редакций Deckhouse Kubernetes Platform

	Community Edition	Basic Edition	Standard Edition	Enterprise Edition	Certified Security Edition
Поддержка российских ОС	✗	✓	✓	✓	✓
Развёртывание в закрытом контуре	✗	✗	✓	✓	✓
Интерфейс администратора	✗	✗	✓	✓	🕒
Интеграция с частным облаком на базе OpenStack или VMware	✗	✗	✗	✓	🕒
Enterprise Security	✗	✗	✗	✓	✓
Service mesh в режиме мультикластера или федерации	✗	✗	✗	✓	🕒
Сертификация ФСТЭК России	✗	✗	✗	✗	✓
Расширенная техническая поддержка (24/7)	✗	✗	✓	✓	✓

🕒 — *планируется к включению в 2024/25*

слайд из презентации с вебинара «Deckhouse Kubernetes Platform: возможности использования после сертификации в ФСТЭК России — практическое руководство» от 18 октября 2024

Наши успехи с момента получения первого сертификата

Октябрь 2024	1	Получен сертификат соответствия на DKP CSE v1.58
Декабрь 2024	2	Получен сертификат соответствия на DKP CSE v1.64
Апрель 2025	3	Получен сертификат соответствия на DKP CSE v1.67
Май 2025	4	Готовимся к сертификации следующей версии в III квартале 2025
2026 год	**5**	**Паритет по функциям между Enterprise и Certified Security**

Подсистема «Кластер Kubernetes»

Поддерживаемые версии Kubernetes — 1.27 и 1.29.

Модуль cni-cilium

- Продвинутые сетевые функции, отказоустойчивый egress gateway в режиме с Virtual IP
- Переход с cni-flannel на cni-cilium

Модуль cilium-hubble

- Визуализация сетевого стека кластера

Модуль metallb

- Возможность настроить балансировку TCP-трафика на узлы кластера

Модуль istio

- Поддержка mTLS для защиты внутреннего трафика и другие функции из Enterprise-версии

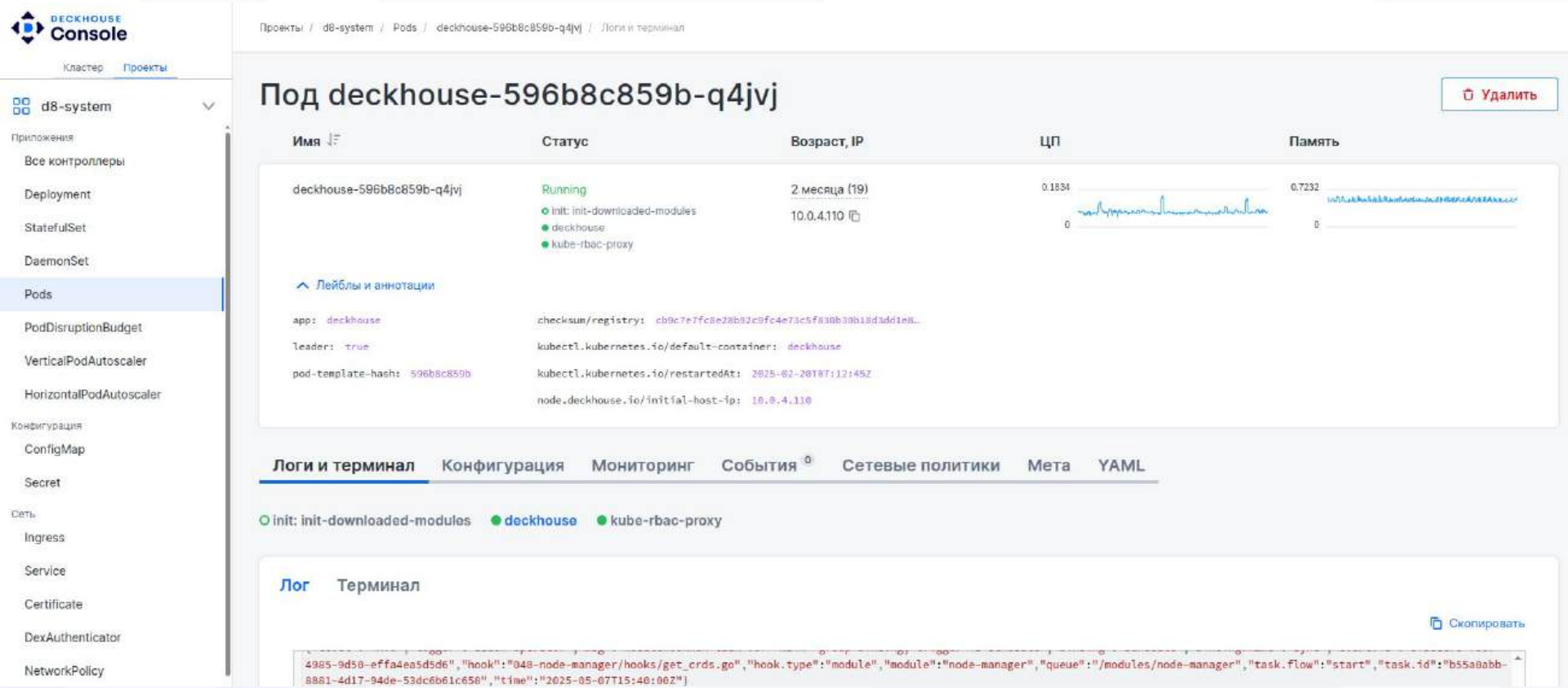
Модуль node-local-dns

- Кэширующий DNS-сервер на каждом узле кластера

Подсистема «Deckhouse»

Модуль console

- Графический интерфейс платформы


DECKHOUSE Console
Кластер
Проекты
d8-system
Приложения
Все контроллеры
Deployment
StatefulSet
DaemonSet
Pods
PodDisruptionBudget
VerticalPodAutoscaler
HorizontalPodAutoscaler
Конфигурация
ConfigMap
Secret
Сеть
Ingress
Service
Certificate
DexAuthenticator
NetworkPolicy
Проекты / d8-system / Pods / deckhouse-596b8c859b-q4jvj / Логи и терминал
Под deckhouse-596b8c859b-q4jvj
Удалить
Имя
Статус
Возраст, IP
ЦП
Память
deckhouse-596b8c859b-q4jvj
Running
init: init-downloaded-modules
deckhouse
kube-rbac-proxy
2 месяца (19)
10.0.4.110
0.1834
0
0.7232
0
Лейблы и аннотации
app: deckhouse
leader: true
pod-template-hash: 596b8c859b
checksum/registry: cb9c7e7fc8e28b92c9fc4e73c5f830b30b18d3dd1e8...
kubectl.kubernetes.io/default-container: deckhouse
kubectl.kubernetes.io/restartedAt: 2025-02-20T07:12:45Z
node.deckhouse.io/initial-host-ip: 10.0.4.110
Логи и терминал
Конфигурация
Мониторинг
События 0
Сетевые политики
Мета
YAML
init: init-downloaded-modules
deckhouse
kube-rbac-proxy
Лог
Терминал
Скопировать
4985-9d50-effa4ea5d5d6","hook":"048-node-manager/hooks/get_crds.go","hook.type":"module","module":"node-manager","queue":"/modules/node-manager","task.flow":"start","task.id":"b55a0abb-8881-4d17-94de-53dc6b61c658","time":"2025-05-07T15:40:00Z"}

Подсистема «Deckhouse»

Модуль console

- Графический интерфейс платформы

Модуль documentation

- Возможность просмотра веб-версии документации

Как настроить?

Deckhouse состоит из оператора Deckhouse и модулей. Модуль — это набор из Helm-чарта, хуков Addon-operator'а, правил сборки компонентов модуля (компонентов Deckhouse) и других файлов.

Deckhouse конфигурируется с помощью:

- **Глобальных настроек.** Глобальные настройки хранятся в ресурсе `ModuleConfig/global`. Эти настройки можно рассматривать как специальный модуль `global`, который нельзя отключить.
- **Настроек модулей.** Настройки каждого модуля хранятся в ресурсе `ModuleConfig`, имя которого совпадает с именем модуля (в kebab-case).
- **Кастомных ресурсов.** Некоторые модули настраиваются с помощью дополнительных кастомных ресурсов.

Пример набора кастомных ресурсов конфигурации Deckhouse:

```
# Глобальные настройки.
apiVersion: deckhouse.io/v1alpha1
kind: ModuleConfig
metadata:
  name: global
spec:
  version: 1
  settings:
    modules:
      publicDomainTemplate: "%s.kube.company.my"
```

Подсистема «Мониторинг»

Grafana версии 10

Модуль extended-monitoring

- Расширенный мониторинг объектов в пространстве имён. Например, можно настроить порог мониторинга 5xx кодов на Ingress или места в PV пода.
- Доступность образов в регистри
- Срок действия пользовательских сертификатов

Модуль monitoring-custom

- Упрощение настройки сбора метрик с Service или Pod

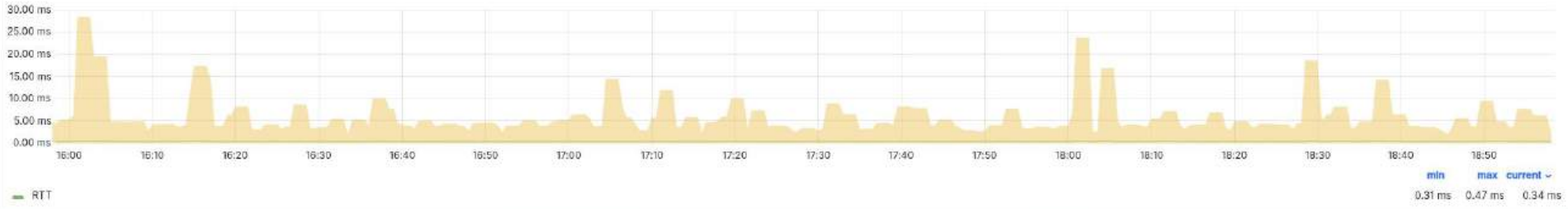
Модуль monitoring-ping

- Мониторинг сетевого взаимодействия между узлами кластера, а также до любых внешних узлов

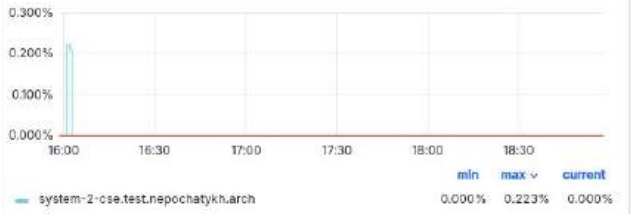
From all nodes

Destination Node	Avg packet loss	Avg mean RTT	Avg mean deviation
system-2-cse.test.nepochatykh.arch	0.002%	0.32 ms	0.12 ms
worker-2-cse.test.nepochatykh.arch	0.000%	0.33 ms	0.12 ms
worker-1-cse.test.nepochatykh.arch	0.000%	0.34 ms	0.13 ms
system-1-cse.test.nepochatykh.arch	0.000%	0.35 ms	0.13 ms
kube-master-1-cse.test.nepochatykh.arch	0.000%	0.37 ms	0.16 ms

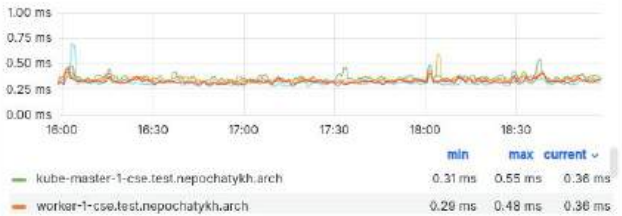
Average mean RTT with min/max



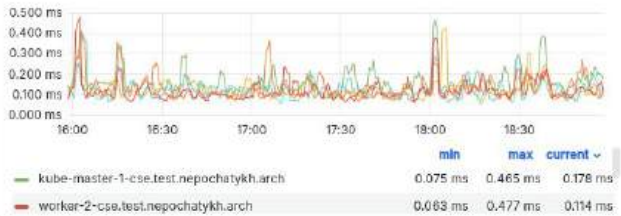
Mean packet loss



Mean RTT



Mean deviation



Подсистема «Масштабирование и управление ресурсами»

Модуль vertical-pod-autoscaler

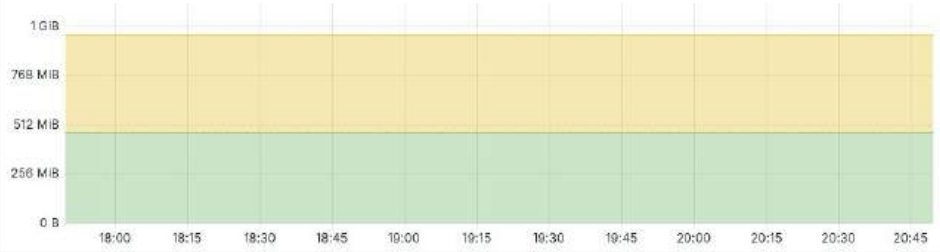
- Вертикальное масштабирование ресурсов

Memory

Usage by controller

Usage by state

Over-requested by controller



Under-requested by controller

Подсистема «Масштабирование и управление ресурсами»

Модуль vertical-pod-autoscaler

- Вертикальное масштабирование ресурсов

Модуль descheduler

- Алгоритмы оптимизации размещения подов на узлах кластера

Подсистема «Хранение данных»

Модуль csi-ceph

- Динамическое управление хранилищем и использование StorageClass на основе RBD (RADOS Block Device) или CephFS

Модуль csi-nfs

- Работа с NFS (Network File System) с возможностью подключения сетевых файловых хранилищ и управления ими в Kubernetes

Модуль sds-node-configurator

- Настройка LVM на узлах кластера: обнаружение блочных устройств и создание/обновление/удаление соответствующих им ресурсов BlockDevice

Модуль sds-local-volume

- Локальное блочное хранилище на базе LVM: создание StorageClass в Kubernetes с помощью ресурса LocalStorageClass

Подсистема «Безопасность»

Модуль cert-manager

- Заказ и управление сертификатами из различных источников, включая самоподписанные сертификаты

Модуль stronghold

- Организация безопасного хранилища данных, управления жизненным циклом хранения данных

Модуль secrets-store-integration

- Высокоуровневый интерфейс работы с секретами из внешних хранилищ через CSI

Безопасность Stronghold

В рамках сертификации ФСТЭК России по 4-му уровню доверия Stronghold проходит комплексную проверку защищённости различными методами тестирования:

Статический анализ исходных текстов

Тестирование на проникновение

Динамический анализ исходных текстов

Фаззинг-тестирование

АО «Флант» выстраивает процессы безопасной разработки ПО согласно ГОСТ Р 56939-2024

РОССИЙСКИЙ ФЕДЕРАЛЬНЫЙ
ГЕОЛОГИЧЕСКИЙ ФОНД

Пример использования DKP CSE в промышленной эксплуатации

Федеральная государственная информационная система **«Единый фонд геологической информации о недрах»** (ФГИС «ЕФГИ») работает и успешно прошла аттестацию на контейнерной инфраструктуре, созданной на Deckhouse Kubernetes Platform CSE.

DECKHOUSE

Kubernetes Platform

CERTIFIED SECURITY EDITION

Другие примеры использования DKP CSE

- Несколько десятков успешных пилотов
- Выходим на промышленную эксплуатацию в одном из топ-10 банков РФ
- Проект миграции в транспортной отрасли России в завершающей стадии
- CSE-редакцию выбирают крупные компании для построения контейнерной инфраструктуры в ЗОКИИ, например ДОМ.РФ
- Готовится к релизу совместный ПАК со Скала^р

Deckhouse CSE — планы развития на Q2–Q4 2025

Модуль	Возможности
cloud-providers	Развёртывание в сертифицированных облаках и системах виртуализации
terraform-manager	Инструмент для отслеживания дрифта конфигураций инфраструктуры кластера

Варианты развёртывания в 2025

Kubernetes Platform

Подсистемы платформы

Управление сетью | Мониторинг и алертинг | Журналирование

Управление сертификатами | Хранение данных | Резервное копирование

Управление виртуальными машинами

Сканирование образов

Политики безопасности

Контроль конфигураций

Механизм модулей

Инфраструктурно независимый фундамент платформы

Веб-интерфейс пользователя

Железо

На выделенных серверах, в том числе в закрытых контурах без доступа в интернет

Облако

В публичных облаках: Selectel, beeline cloud, VK Cloud, Yandex Cloud и других

Виртуализация

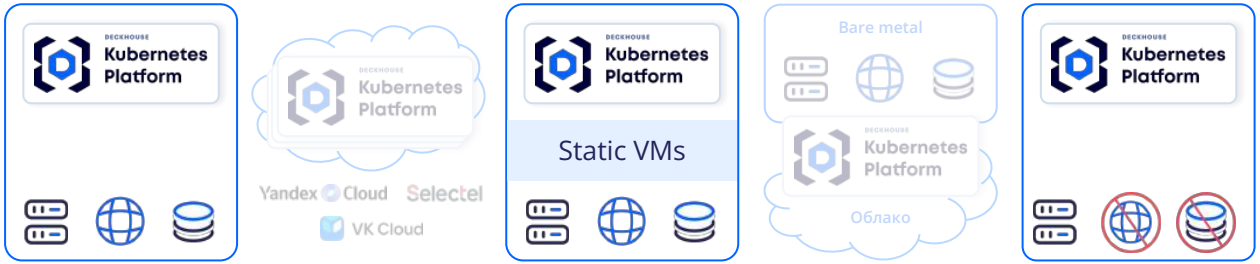
В приватных облаках, поверх любой виртуализации, в том числе без доступа в интернет

Гибрид

В гибридной модели: статическая часть кластера на железе плюс динамический скейлинг в облако

EDGE

В удалённых инсталляциях с плохой сетевой связностью и дефицитом ресурсов



Инфраструктура

Варианты развёртывания в 2025

Железо

На выделенных серверах, в том числе в закрытых контурах без доступа в интернет

Облако

В аттестованных и частных облаках: Selectel, Yandex Cloud, Private Cloud от VK и др.

Виртуализация

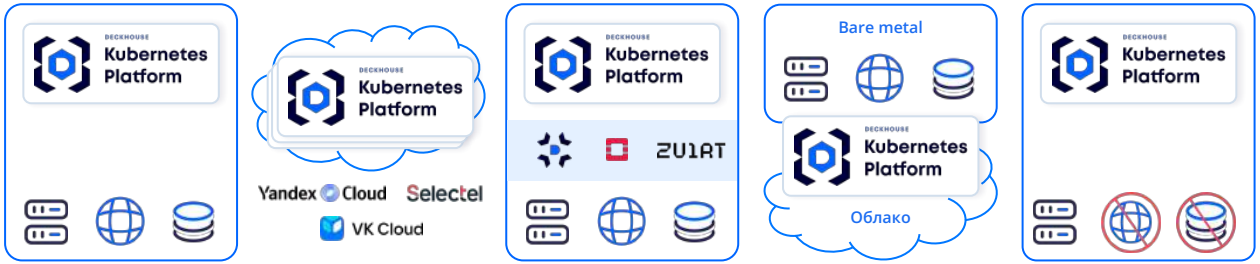
В приватных облаках, поверх любой виртуализации, в том числе без доступа в интернет

Гибрид

В гибридной модели: статическая часть кластера на железе плюс динамический скейлинг в облако

EDGE

В удалённых инсталляциях с плохой сетевой связностью и дефицитом ресурсов



Инфраструктура

Deckhouse CSE — планы развития на Q2–Q4 2025

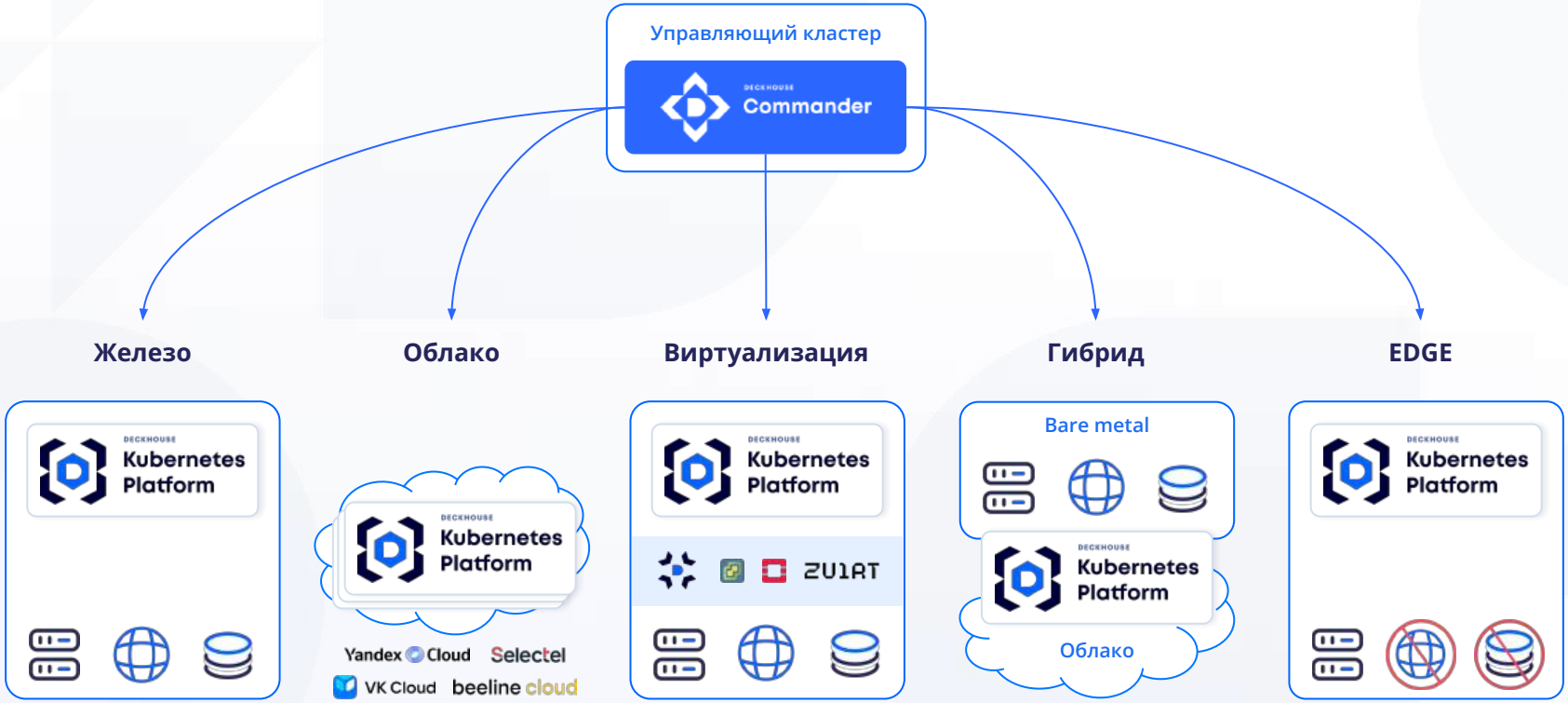
Модуль	Возможности
cloud-providers	Развёртывание в сертифицированных облаках и системах виртуализации
terraform-manager	Инструмент для отслеживания дрифта конфигураций инфраструктуры кластера
upmeter	Статистика по типам доступности для компонентов кластера и DKP


now - 6h to now
Step: 30m
Mute
15:30
16:00
16:30
17:00
17:30
18:00
18:30
19:00
19:30
20:00
20:30
21:00
21:30
Total
Kubernetes Control Plane
Deckhouse
Cluster Configuration
Extensions
Kubernetes Dashboard
Dex
grafana-v10
Longterm Prometheus
Monitoring and Autoscaling
Nginx
100%

Deckhouse CSE — планы развития на Q2–Q4 2025

Модуль	Возможности
cloud-providers	Развёртывание в сертифицированных облаках и системах виртуализации
terraform-manager	Инструмент для отслеживания дрифта конфигураций инфраструктуры кластера
upmeter	Статистика по типам доступности для компонентов кластера и DKP
sds-replicated-volume	Управление реплицируемым блочным хранилищем на базе DRBD
commander	Создание кластеров Kubernetes и управление их жизненным циклом

Deckhouse Commander работает с любой инфраструктурой



Deckhouse CSE — планы развития на Q2–Q4 2025

Модуль	Возможности
cloud-providers	Развёртывание в сертифицированных облаках и системах виртуализации
terraform-manager	Инструмент для отслеживания дрифта конфигураций инфраструктуры кластера
upmeter	Статистика по типам доступности для компонентов кластера и DKP
sds-replicated-volume	Управление реплицируемым блочным хранилищем на базе DRBD
commander	Создание кластеров Kubernetes и управление их жизненным циклом
service-with-healthchecks	Создание балансировщиков с активными проверками работоспособности приложений, запущенных в поде
virtualization	Создание, запуск виртуальных машин и управление ими

Наша цель — в 2026 году сравнять функционально редакции CSE Pro и EE.

Ближайшие планы по расширению действия сертификата

Расширение сертификата на соответствие требованиям к средствам виртуализации в соответствии с требованиями приказа ФСТЭК России от 27 октября 2022 г. № 187.

Добавление в ТУ мер по управлению информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.

Выделение трёх исполнений: Kubernetes+Virtualization, Kubernetes, Virtualization.

Добавление новых модулей в DKP CSE, таких как commander, sds-replicated-volume, terraform-manager, virtualization и др., поддержка cloud-провайдера zVirt.

Над чем работаем?

Какие работы выполняем ещё в рамках оценки соответствия?

Проходим сертификацию Deckhouse Stronghold по требованиям ТУ и приказа **ФСТЭК России № 76 по 4-му уровню доверия**.

Выстраиваем процессы РБПО согласно требованиям **ГОСТ Р 56939-2024**, прошли внешний аудит, планируем в дальнейшем проходить сертификационный аудит.

Спасибо за внимание!

Готовы ответить на ваши вопросы!

contact@deckhouse.ru

+7 (495) 721-10-27

deckhouse.ru

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

Оставьте заявку на пилот Deckhouse Kubernetes Platform Certified Security Edition

Оставить заявку по ссылке