DECKHOUSE

Kubernetes Platform

CERTIFIED SECURITY EDITION

Kubernetes и КИИ: нормативы, риски, готовое решение

Спикеры

Степан Чернов

stepan.chernov@flant.ru

Специалист по решениям Deckhouse

Ильдар Гарипов

ildar.garipov@flant.ru

Руководитель отдела информационной безопасности

Запись предыдущего вебинара по теме:

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

Запись

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

АРПП «Отечественный
софт»

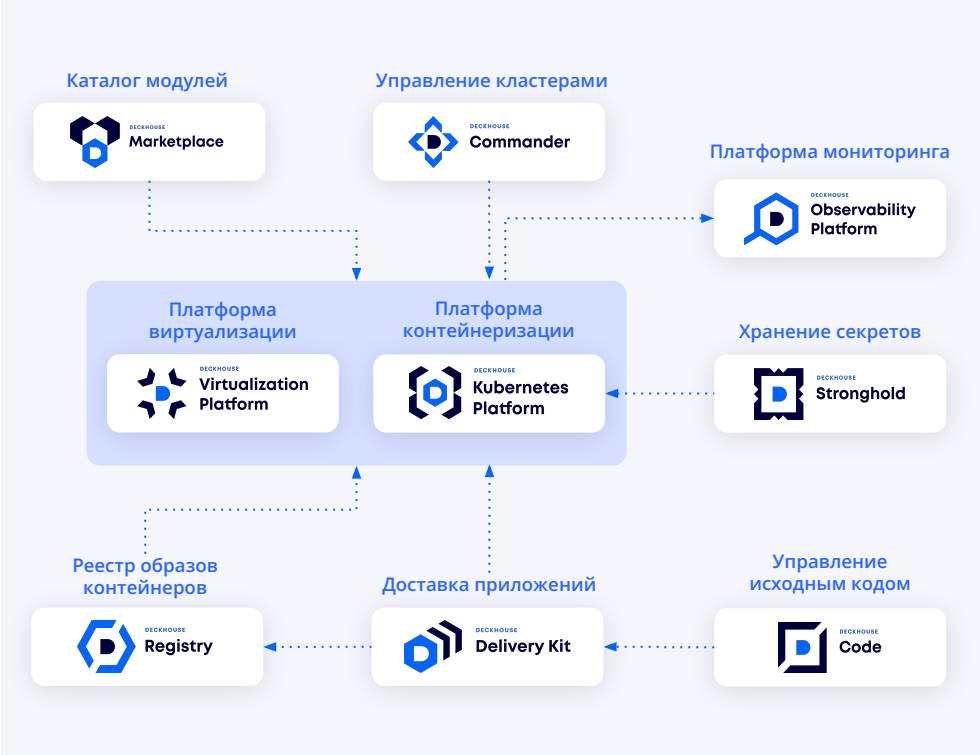
** Рейтинг «Крупнейшие ИТ-вендоры в банках», TAdviser, 2024 год*

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

Deckhouse
by Flant

Экосистема продуктов Deckhouse

- Все продукты экосистемы — **в реестре российского ПО**
- Единый канал **технической поддержки** по всем продуктам
- Высокая **доступность и отказоустойчивость** всех компонентов «из коробки»
- Глубокая **интеграция** продуктов экосистемы между собой
- **Централизация** управления, мониторинга и контроля над всей экосистемой через единый UI
- Сквозное применение лучших практик **DevSecOps** на всех этапах процесса непрерывной поставки ценности



DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

История импортозамещения в ИТ

обсуждается ещё с 2014 года

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

1 **2015 год**

Постановление от 16 ноября 2015 года № 1236, согласно которому государственные органы не могут закупать зарубежное программное обеспечение при наличии отечественных аналогов, включённых в реестр ПО.

2 **2016 год**

Постановление от 16 сентября 2016 года № 925. Устанавливается приоритет товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами.

3 **2018 год**

Директива о полном переходе государственных компаний на отечественное ПО до 2021 года.

4 **2021 год**

Минцифры РФ предложило перевести объекты критической информационной инфраструктуры на преимущественное использование российского ПО с 1 января 2023 года и российского оборудования с 1 января 2024 года.

Федеральный закон от 26.07.2017 № 187-ФЗ *

- Здравоохранение
- Наука
- Транспорт
- Связь
- Энергетика
- Банковский сектор и финансы
- Топливно-энергетический комплекс
- Атомная энергетика
- Оборонная и ракетно-космическая промышленность
- Горнодобывающая промышленность
- Металлургическая и химическая промышленность
- Недвижимое имущество

** "О безопасности критической информационной инфраструктуры Российской Федерации"*

Указ Президента Российской Федерации от 30.03.2022 № 166

«О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»

Установлен запрет на закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ иностранного ПО, в том числе в составе ПАК, в целях его использования на ЗОКИИ.

Установлен запрет на использование иностранного ПО на ЗОКИИ.

Указ Президента Российской Федерации от 30.03.2022 № 166

Во исполнение поручения Указа Президента № 166 Правительством утверждены следующие документы:

- Постановление Правительства РФ от 22.08.2022 № 1478, устанавливающее требования к импортозамещению ПО на значимых объектах КИИ;
- Постановление Правительства РФ от 14.11.2023 № 1912, устанавливающее требования к доверенным программно-аппаратным комплексам в составе значимых объектов КИИ.

Указ Президента Российской Федерации от 01.05.2022 № 250

«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Установлен запрет на использование средств защиты информации, произведённых «недружественными странами».

Указ Президента Российской Федерации от 07.05.2024 № 309

«О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»

В Указе Президента Российской Федерации от 7.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» особое внимание уделено вопросу импортозамещения в информационно-технологической сфере.

В контексте развития ИТ-инфраструктуры Российской Федерации приоритетное значение имеют цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы» и «Технологическое лидерство».

К 2030 году предполагается достичь показателя в 95 % доли использования российского программного обеспечения в государственных органах, государственных корпорациях, государственных компаниях и организациях с долей участия Российской Федерации, превышающей 50 %, а также в их дочерних компаниях.

Федеральный закон
от 07.04.2025 № 58-ФЗ

«О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»

усиливает требования в части технологической независимости, предполагается, что Правительство РФ установит:

- порядок и сроки перехода на использование требуемых программно-аппаратных средств и отечественного ПО;
- порядок осуществления мониторинга за использованием требуемых программно-аппаратных средств и отечественного ПО.

Вступает в силу 1 сентября 2025 года

Ответственность за нарушение требований КИИ

Риск/инцидент	Контролирующий орган	Последствия
Инцидент, повлекший негативные последствия	ФСБ России МВД России	Административная ответственность Уголовная ответственность
Нарушены правила категорирования	ФСТЭК России Отраслевые регуляторы	Административная ответственность
Не создана система безопасности	ФСТЭК России	Административная ответственность

Ответственность за нарушение требований КИИ

Уголовная и административная ответственность, помимо общих норм, связанных с наказанием за совершение киберпреступлений (статьи 272–274 УК РФ) и правонарушений в сфере защиты информации (статьи 13.11, 13.12, 13.13, 13.14, 13.14.1, 19.7 КоАП РФ), имеет ряд специализированных в части КИИ составов.

УК РФ, статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

КоАП РФ, статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

КоАП РФ, статья 19.7.15. Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Продукты Deckhouse в реестре российского ПО

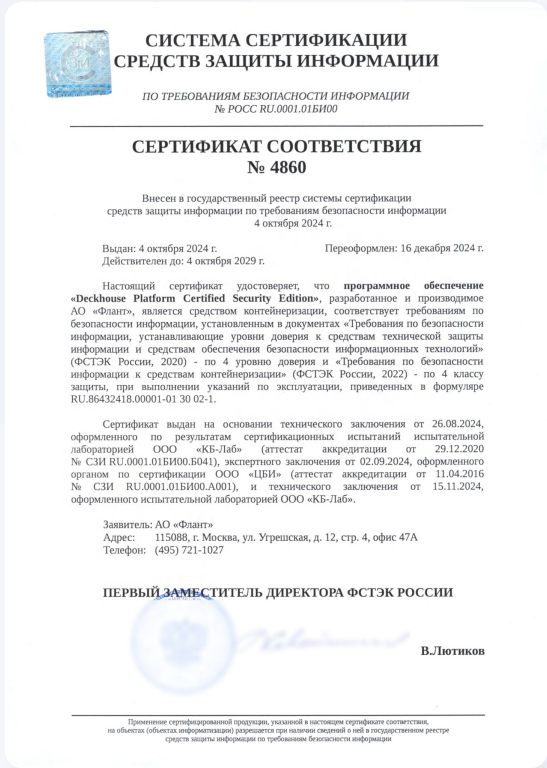
Deckhouse Kubernetes Platform	Акционерное общество «Флант»	02.12 Системы контейнеризации и контейнеры	21.12.2021	12338
Deckhouse Code	Акционерное общество "Флант"	04.02 Средства версионного контроля исходного кода 04.04 Среды разработки, тестирования и отладки	06.05.2025	27871
Deckhouse Commander	Акционерное общество "Флант"	05.02 Дополнительные программные модули (плагины)	20.12.2024	25598
Deckhouse Virtualization Platform	Акционерное общество "Флант"	02.04 Средства виртуализации 05.02 Дополнительные программные модули (плагины)	15.11.2024	24689
Deckhouse Stronghold	Акционерное общество "Флант"	05.02 Дополнительные программные модули (плагины) 03.01 Средства защиты от несанкционированного доступа к информации 03.12 Средства управления доступом к информационным ресурсам	24.04.2024	22339
Deckhouse Delivery Kit	Акционерное общество "Флант"	02.12 Системы контейнеризации и контейнеры	14.06.2024	22881
Deckhouse Observability Platform	АКЦИОНЕРНОЕ ОБЩЕСТВО "ФЛАНТ"	02.08 Средства мониторинга и управления	30.01.2023	16426

Реестр

Сертификат ФСТЭК России № 4860 от 04.10.2024

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
- после получения сертификата соответствия были проведены 2 процедуры внесённых изменений и получено согласование ФСТЭК России



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 (объектах информатизации) разрешается 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.

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.*

Deckhouse Kubernetes Platform в цифрах

7 лет
эксплуатации
первая российская K8s-платформа

240+
клиентов
доверяют нам развитие своего бизнеса

200+
сертифицированных партнёров

1000+
кластеров
под управлением Deckhouse

99,97 %
фактический SLA
по кластерам под нашим управлением

150+
сертификатов «Администратор DKP»
выдано инженерам из 85 компаний

Deckhouse Kubernetes Platform — больше, чем Kubernetes

	Deckhouse Kubernetes Platform	Vanilla Kubernetes
Развёртывание кластера Kubernetes	✓	✓
Настройка ОС на узлах	✓	✗
Автоконфигурирование управляющих компонентов Kubernetes	✓	✗
Преднастроенная сеть и готовые варианты балансировки	✓	✗
Интеграция и управление нижележащей инфраструктурой	✓	✗
Управление хранилищем и различные возможности хранения	✓	✗
Масштабирование кластера и приложений по любым метрикам	✓	✗
Преднастроенная безопасность на уровне платформы	✓	✗
Интерфейс администратора	✓	✗
Отказоустойчивая конфигурация и резервирование «из коробки»	✓	✗
… и ещё несколько десятков тесно связанных модулей для production ready-решения	✓	✗

Deckhouse Kubernetes Platform — полное соответствие приказу ФСТЭК № 118

	Deckhouse Kubernetes Platform
Идентификация и аутентификация пользователей	✓
Изоляция контейнеров	✓
Выявление уязвимостей в образах контейнеров	✓
Проверка корректности конфигурации контейнеров	✓
Контроль целостности контейнеров и их образов	✓
Регистрация событий безопасности	✓
Ролевой метод управления доступом (RBAC)	✓

7 шагов к безопасности в Kubernetes

1. Корректная конфигурация кластера Kubernetes
2. Управление пользователями и доступами
3. Сканирование образов
4. Сетевая безопасность
5. Контроль над запускаемыми приложениями
6. Управление секретами
7. Аудит и регистрация событий

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

Контроль конфигураций на соответствие CIS Benchmark

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

Раз в сутки все кластеры проверяются на соответствие рекомендациям CIS Benchmark* и результаты проверки выводятся на дашборд подсистемы мониторинга.

Проверяются:

- Все **компоненты управляющего слоя** Kubernetes
- Настройки **аутентификации и авторизации**
- Настройки **логирования и аудита**
- Конфигурация **рабочих узлов**
- **Корректность политик:** безопасности, операционных и сетевых
- **Работа с секретами** в кластере

** Полный перечень проверок*

Единый центр аутентификации

- **Безопасный доступ** к API кластера, всем веб-интерфейсам и пользовательским приложениям.
- Возможность создания **локальных пользователей и групп**. Простая выдача конфигурации подключения.
- Интеграция с **внешними провайдерами аутентификации** (LDAP, Active Directory, OIDC и другие).
- Контроль доступа к ресурсам платформы, настройка **правил авторизации и ограничения доступа** к любым системам по IP и группам пользователей.
- Аутентификация для сторонних приложений.
- Взаимная достоверная **аутентификация сервисов и шифрование** трафика (mTLS).

Авторизация и разделение прав доступа

- Управление доступом с помощью **стандартной ролевой модели Kubernetes** на уровне пространств имён кластера или всего кластера.
- **Семь преднастроенных ролей** с тщательно продуманными правами на любой случай.
- Возможность создавать свои **собственные кастомные роли**, используя готовые наборы из нескольких десятков высокоуровневых capabilities.
- Создание технических сервисных учётных записей и управление ими для взаимодействия различных информационных систем друг с другом.
- Гибкие **политики авторизации для сервисов** (*service mesh*).
- Возможность предоставлять **доступ к избранным сервисам при объединении кластеров** в режиме федерации (*service mesh*).

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

Мультиарендность на базе проектов

- Проекты — типовые **изолированные друг от друга окружения**, созданные по заранее подготовленному шаблону.
- Полная **изоляция ресурсов и политик доступа** между проектами обеспечивает безопасную мультиарендность и даёт разработчикам возможность запускать приложения без влияния на другие проекты.
- Возможность устанавливать **квоты на ресурсы** и ограничения для каждого проекта предотвращает избыточное использование ресурсов.
- Разработчики могут запрашивать у администраторов проекты, созданные по готовым шаблонам, что позволяет **быстро начать разработку нового приложения**.

Сканирование образов на уязвимости

- Регулярная **проверка пользовательских образов в runtime на известные CVE** (включая уязвимости Astra Linux, РЕД ОС и ALT Linux).
- Возможность **блокирования выката приложений** в случае нахождения Critical- и High-уязвимостей.
- Возможность **конвертации отчётов об уязвимостях** из базы CVE в формат данных из базы БДУ ФСТЭК и вывода их в отчёт.
- Возможность подключения встроенной в DKP базы данных уязвимостей для **проверки образов бизнес-приложений на этапе сборки** (сама проверка при этом осуществляется сторонними средствами).

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

Сетевая безопасность

1. CNI с поддержкой сетевых политик **для всех компонентов** кластера
2. Возможность настройки **Deny all** по умолчанию

А также:

- Глобальные политики на весь кластер
- Хостовые политики
- Визуализация сетевых соединений
- Редактор для сетевых политик

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

Политики безопасности и операционные политики

- Возможность использовать одну из трёх предустановленных политик безопасности **Pod Security Standards** или настроить собственные политики.
- Набор **операционных политик** и лучших практик для безопасной работы ваших приложений:
  - Разрешить только **доверенные registry**
  - Обязательно **прописывать ресурсы**
  - **Использовать пробы**
  - Ограничить **количество ревизий**
  - Указывать **priority class**
  - Запретить использовать **тег latest**
  - Проверка **подписей образов контейнеров**

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

Управление секретами

- Возможность доставки секретов для приложения из **внешних подключаемых хранилищ секретов** (модуль secrets-store-integration).
- **Встроенное решение** для безопасного управления жизненным циклом секретов (Deckhouse Stronghold). Лицензируется отдельно!

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

Аудит запущенных приложений и обнаружение угроз безопасности

- Анализ событий **ядра Linux**.
- Аудит **вызовов API Kubernetes**.
- Обнаружение **событий безопасности** по установленным правилам:
  - Попытки применения **уязвимостей из базы CVE и запуска криптовалютных майнеров.**
  - Запущенные **оболочки командной строки**.
  - Контейнеры, работающие в **привилегированном режиме.**
  - Монтирование **небезопасных путей** (например, /proc) в контейнеры.
  - Попытки **чтения секретных данных** из, например, /etc/shadow.

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

Оповещения о событиях безопасности

- Гибкий **сбор логов** аудита, их обработка и **доставка в SIEM-системы**.
- Встроенные метрики и возможность собирать **любые пользовательские метрики**.
- Удобная **настройка оповещений** о событиях ИБ в кластерах.

DECKHOUSE
Kubernetes Platform
CERTIFIED SECURITY EDITION

скала^р

Машина контейнерной инфраструктуры

В мае 2025 года совместно с «СКАЛА-Р» был выпущен программно-аппаратный комплекс Скала^р MB.K:

- Deckhouse Kubernetes Platform CSE PRO
- Гарантированная совместимость на программном и аппаратном уровне
- Комплексная техническая поддержка и сопровождение высочайшего качества в режиме одного окна
- Готовый продукт для решения задачи по построению инфраструктуры для контейнеров в максимально короткие сроки

Почему Deckhouse Kubernetes Platform

- Первая российская платформа контейнеризации, сертифицированная ФСТЭК России
- Больше половины инсталляций — **в закрытых окружениях** без доступа в интернет
- Первая платформа контейнеризации в реестре российского ПО
- Публичные истории успеха, возможность проведения **референсных встреч**
- Федеральная ГИС, функционирующая на базе нашей Kubernetes-платформы, успешно аттестована регулятором
- Более 200 авторизованных партнёров и более 50 партнёрских продуктов с подтверждённой совместимостью
- 1-й российский дистрибутив Kubernetes, сертифицированный CNCF
- Лидер рейтинга российских Kubernetes-платформ 2025 от IaaSSaaSPaaS

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