



Первая сертифицированная
ФСТЭК России платформа
контейнеризации



DECKHOUSE

**Kubernetes
Platform**

CERTIFIED SECURITY EDITION



DECKHOUSE

**Kubernetes
Platform**

CERTIFIED SECURITY EDITION

Deckhouse Kubernetes Platform Certified Security Edition

Первая 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.

Сертификат ФСТЭК России № 4860 от 4 октября 2024 г.

- Соответствие требованиям по безопасности информации к средствам контейнеризации (утверждены [приказом ФСТЭК России № 118 от 4 июля 2022 г.](#)) — по 4-му классу защиты
- Соответствие 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
- С октября 2024 года выпущено уже [три версии](#) сертифицированной редакции DKP



**СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БН00

**СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4860**

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

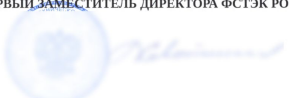
Выдан: 4 октября 2024 г. Переоформлен: 16 декабря 2024 г.
Действителен до: 4 октября 2029 г.

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 указанных 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.0001.01БН00.Б041), экспертного заключения от 02.09.2024, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БН00.А001), и технического заключения от 15.11.2024, оформленного испытательной лабораторией ООО «КБ-Лаб».

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

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



В. Лютиков

Примечание: сертифицированной редакции, указанной в настоящем сертификате соответствии, по объектам (объектам информации) подлежат при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Защита информации на значимых объектах КИИ* **



Здравоохранение



Наука



Транспорт



Связь



Энергетика



Банковский сектор
и финансы



Топливо-энергетический
комплекс



Атомная энергетика



Оборонная
и ракетно-космическая
промышленность



Горнодобывающая
промышленность



Металлургическая
и химическая
промышленность



Недвижимое имущество

* до 1-й категории значимости включительно согласно [приказу ФСТЭК России № 239](#) от 25 декабря 2017 г.

«Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

** Список отраслей регламентирован в пункте 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ

«О безопасности критической информационной инфраструктуры Российской Федерации»



Требования ЦБ РФ по защите информации для финансовых организаций

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 персональных данных*



Операторы сотовой связи



Банки и финансовые учреждения



Центры верификации данных



Медицинские и образовательные учреждения



Интернет-провайдеры



Страховые компании



Транспортные компании



Ретейл



Государственные и муниципальные органы власти

** в ИС до 1-го уровня защищённости включительно согласно приказу ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»*

Защита информации в ГИСах*

1 Федеральные и региональные органы исполнительной власти

3 Органы государственной власти субъектов Российской Федерации

2 Министерства и ведомства

4 Органы местного самоуправления и другие

** до 1-го класса защищённости включительно согласно приказу ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методическому документу от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»*



Изменения нормативных требований ФСТЭК России для госпредприятий

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.

Защита информации в автоматизированных системах управления*



Топливо-энергетический комплекс



Химическая промышленность



Транспортные системы



Системы водоснабжения



Коммунальные службы



Металлургия



Добыча природных ресурсов



Атомная энергетика



Здравоохранение

** до 1-го класса защищённости включительно согласно приказу ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты 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»*

Состав Deckhouse Kubernetes Platform CSE



Автомасштабирование



Безопасность



Сеть



Отказоустойчивость



Логирование



Мониторинг



Администрирование



Балансировка



Хранение



Оператор платформы



Kubernetes

Инфраструктура



Железо

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	✓	✗	✗

**Выпускаем обновления
сертифицированной
версии регулярно!**



**Deckhouse
Kubernetes
Platform**

CERTIFIED SECURITY EDITION

1

Октябрь 2024

Получен сертификат соответствия на DKP CSE v1.58

2

Декабрь 2024

Получен сертификат соответствия на DKP CSE v1.64

3

Апрель 2025

Получен сертификат соответствия на DKP CSE v1.67

4

Июль 2025

Готовимся к сертификации следующей версии
в III квартале 2025

5

2026 год

Паритет по функциям между Enterprise
и Certified Security

Статус и планы на 2025 по дополнительной сертификации

Q2 — Готово!

Дополнить сертифицированную версию DKP CSE функционалом управления секретами в рамках текущей сертификации



Результат:

Реализована возможность использовать Deckhouse Stronghold (лицензируется отдельно) для управления секретами в составе сертифицированной версии платформы DKP CSE

Q3

Расширить сертификат на соответствие требованиям к средствам виртуализации в соответствии с [приказом ФСТЭК России №187 от 27 октября 2022 г.](#)



Результат:

Возможность использовать DVP CSE (лицензируется отдельно) в качестве сертифицированной виртуализации для построения защищённой инфраструктуры

Q4

Расширить сертификат на соответствие требованиям к межсетевым экранам в соответствии с приказом ФСТЭК России №9 от 9 февраля 2016 г. и методическим документом [«Профиль защиты межсетевых экранов типа «Б» четвёртого класса защиты»](#)



Результат:

Возможность использовать сетевые политики в составе DKP CSE в качестве сертифицированного межсетевого экрана для изоляции контуров в рамках построения защищённой инфраструктуры

Внесение изменений и обновления DKP CSE

- Новые версии DKP CSE выпускаем примерно раз в квартал. Информацию обо всех версиях DKP CSE, а также инструкции по обновлению размещаем на сайте по адресу: <https://deckhouse.ru/products/kubernetes-platform/certified-security-edition/updates/>
- 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
- При внесении в DKP CSE изменений, не связанных с функциями безопасности, испытания проводятся самостоятельно силами вендора
- Находимся в процессе получения сертификата соответствия процедурам разработки безопасного программного обеспечения (РБПО). Сертификат позволит проводить все испытания самостоятельно
- 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 (актуально для версии DKP CSE 1.67 и более поздних)

Процесс устранения уязвимостей DKP CSE

- 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)
- Доработка DKP CSE, в том числе разработка обновлений или разработка мер по защите информации, нейтрализующих недостаток, выполняется в течение 60 дней с момента выявления недостатка
- Сообщить об уязвимости в DKP CSE можно через форму на сайте по адресу: <https://deckhouse.ru/report-request/>

Будем рады ответить на ваши вопросы!

✉ contact@deckhouse.ru

☎ +7 (495) 721-10-27

🌐 deckhouse.ru



[Блог](#)



[RuTube](#)



[Telegram](#)