Deckhouse
ФЛАНТ

Подтверждённая безопасность секретов: Deckhouse Stronghold получил сертификат ФСТЭК России

Deckhouse
ФЛАНТ

Спикеры

Владимир Девятайкин

Менеджер продукта
Deckhouse Stronghold

vladimir.devyataykin@flant.com

Ильдар Гарипов

Руководитель отдела
информационной безопасности

ildar.garipov@flant.com

План вебинара

01 О Фланте и вендоре Deckhouse

02 Почему секреты нужно хранить безопасно

03 Функциональные возможности продукта

04 Где может применяться Deckhouse Stronghold CSE

05 Путь получения сертификации ФСТЭК России

06 Безопасная разработка при сертификации Deckhouse Stronghold

07 Функции безопасности

08 Варианты инсталляции и формат поставки

09 Планы по развитию

10 Q&A-сессия

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

Express 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

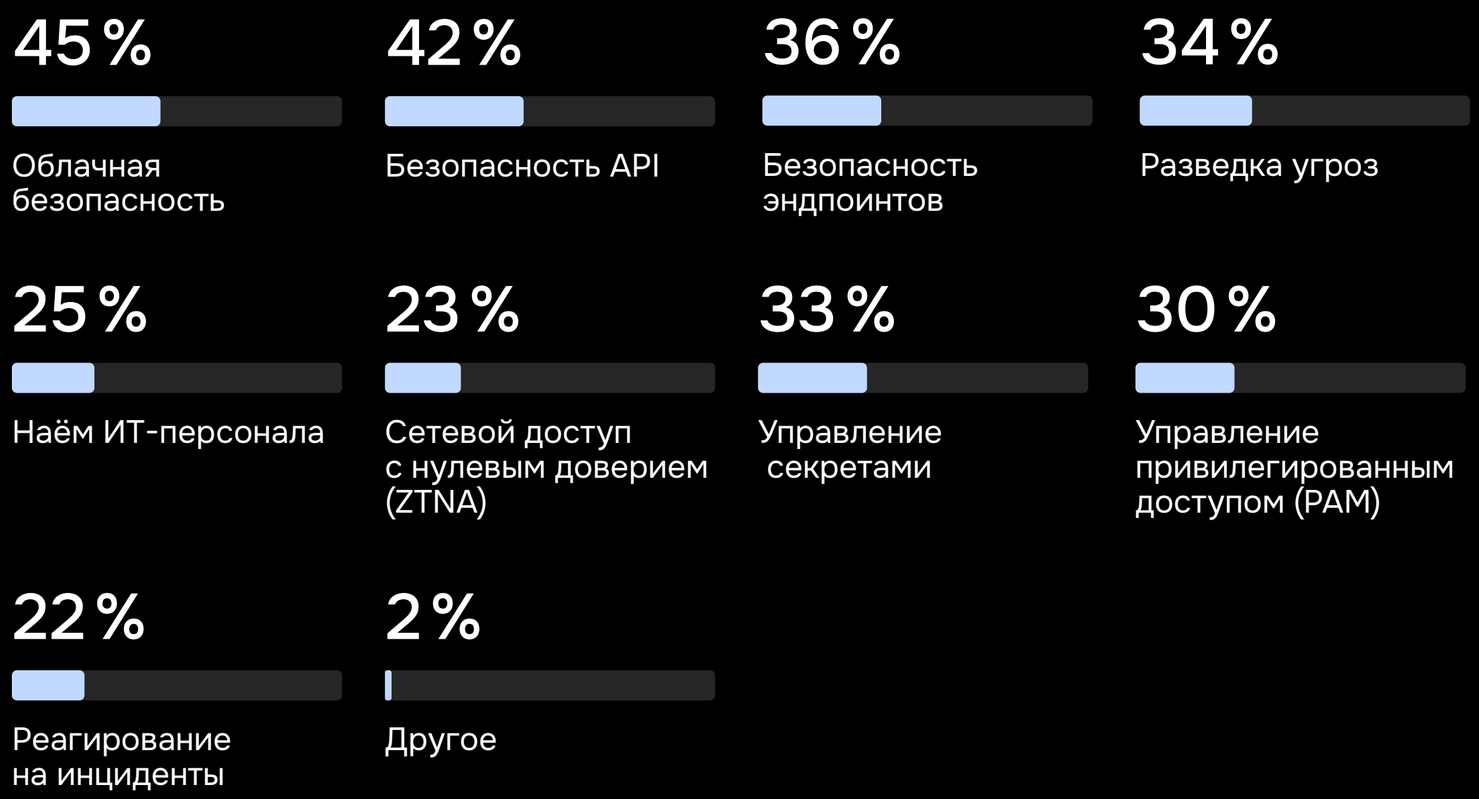
**Рейтинг «Крупнейшие ИТ-вендоры в промышленности», T-Adviser, 2024 год

Что можно считать секретами?

- Пароли
- Токены
- Ключи API
- SSH-ключи
- Сертификаты

Защита секретов входит в топ-5 направлений развития ИБ

Какие направления наиболее приоритетны для вашей стратегии кибербезопасности?



По данным отчёта The State of Secrets Management 2024 компании Akeyless

Безопасность

Защита секретов входит в топ-5 направлений развития ИБ

33 %*

респондентов считают безопасность секретов одним из важнейших приоритетов

* По данным отчёта The State of Secrets Management 2024 компании Akeyless

Ручное управление секретами

Фрагментация секретов

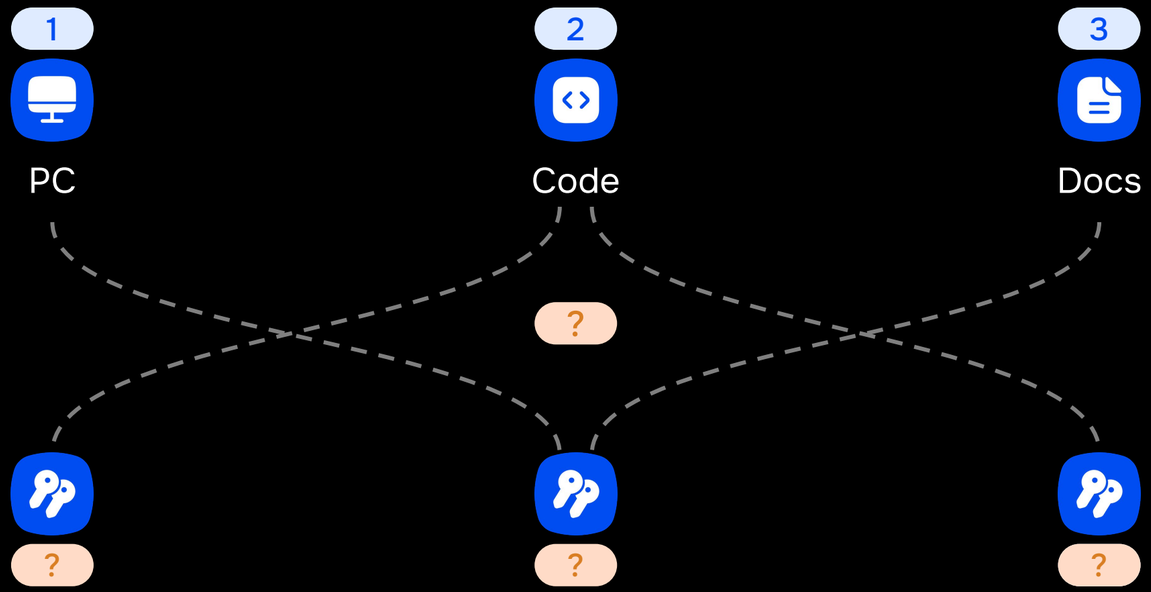
Секреты организации хранятся хаотично и в небезопасных местах

Отсутствие контроля

ИТ-отделы и DevOps-команды не могут их контролировать

Риск утечки

Появляются уязвимости, возрастает риск компрометации и утечки секретов



Хранение секретов с помощью Deckhouse Stronghold

Централизованное решение

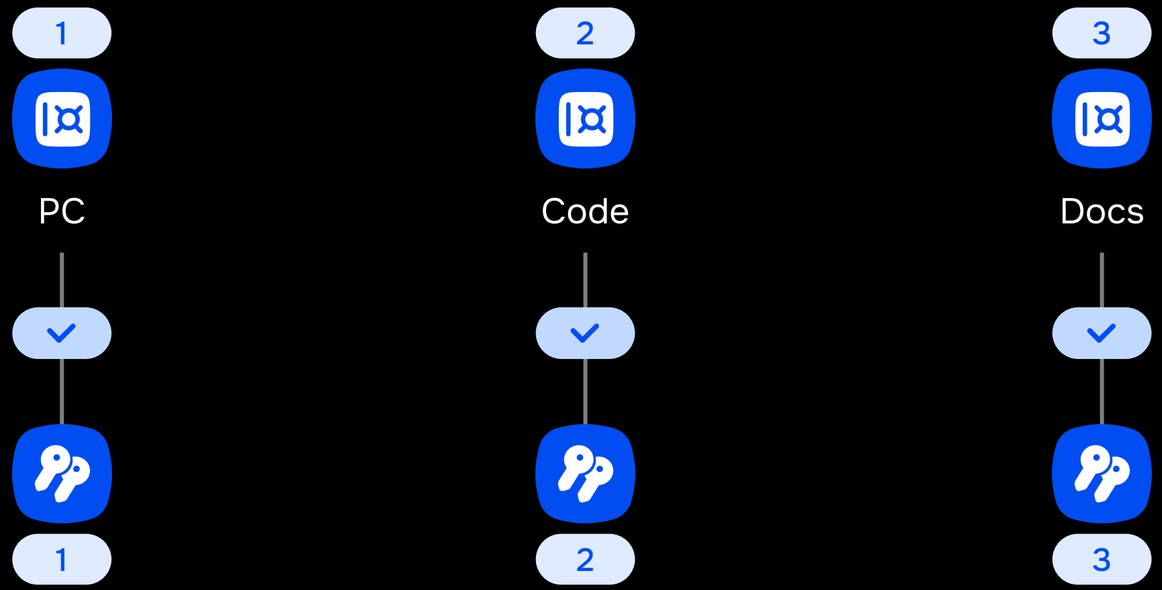
для безопасного хранения секретов

Лёгкое управление

жизненным циклом секретов и ролями доступа к ним

Полное шифрование данных

даже если кто-то украдёт физический сервер, он не сможет получить доступ к секретам



Какие задачи мы помогаем решать

- Выполнить требования НПА (ФЗ-152, ФЗ-149, ФЗ-187)
- Выполнить требования ГОСТ Р 56939-2024
- Сформировать единый подход к управлению секретами
- Реализовать переход на отечественное ПО
- Изменить структуру расходов на управление секретами (↓OPEX)
- Компенсировать нехватку экспертизы и ресурсов персонала

Deckhouse professional services

Услуги по внедрению и адаптации решений экосистемы Deckhouse, миграции приложений и оптимизации управления их жизненным циклом

Глубокая экспертиза

Одна из лучших в РФ экспертиза в Kubernetes и Deckhouse, прямой доступ к разработчикам и поддержке L3 Deckhouse

Time-to-value

Использование отработанных методологий и лучших практик для быстрого и надежного внедрения Deckhouse, максимально быстрый возврат инвестиций

Адаптация

Настройка и оптимизация Deckhouse под уникальные потребности бизнеса, ИТ и ИБ

Реализация «под ключ»

От сбора и аудита требований до проектирования, внедрения, интеграции и передачи знаний

Передача знаний

Зрелый подход к оформлению документации, вебинары для администраторов и пользователей Deckhouse, обучение и сертификация в Deckhouse Academy

Deckhouse Stronghold
CERTIFIED SECURITY EDITION

Интервью

Распаковка AM Live. Deckhouse Stronghold: безопасная работа с секретами

Владимир Девятайкин

Менеджер продукта
Deckhouse Stronghold

Доклад

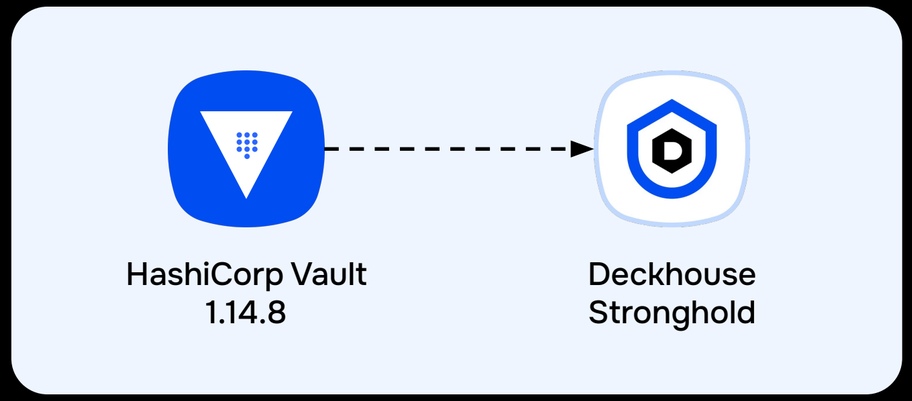
Успех секрета: как доставлять секреты в приложения безопасно и без головной боли

Максим Киселев

Руководитель разработки
Deckhouse Stronghold

Что такое Deckhouse Stronghold

Решение для централизованного управления жизненным циклом секретов. Защищает пароли, ключи API, сертификаты, SSH-ключи, токены и другие конфиденциальные данные от утечек, а также обеспечивает безопасную доставку секретов в приложения.



Мы **не копируем** HashiCorp Vault,
мы **переосмысливаем** хранилище секретов
и **создаём стандарт** для российского рынка

Сравнение с конкурентами

	Stronghold CSE	Vault EE	Vault CE	OpenBao
Пространства имён (namespaces)	✓	✓	✗	✓
Межкластерная репликация данных	✓	✓	✗	✗
Автоматическое резервное копирование данных по заданному расписанию	✓	✓	✗	✗
Поддержка внешних HSM для двойного шифрования данных	✓	✓	✗	✓
Безопасный auto unseal без использования внешних KMS	✓	✗	✗	✗
Управление AppRole, OIDC/JWT Role в UI	✓	✗	✗	✗
Встроенная безопасная доставка секретов в приложения	✓	✗	✗	✗
Сертификация ФСТЭК России	✓	✗	✗	✗

Путь получения сертификации ФСТЭК России

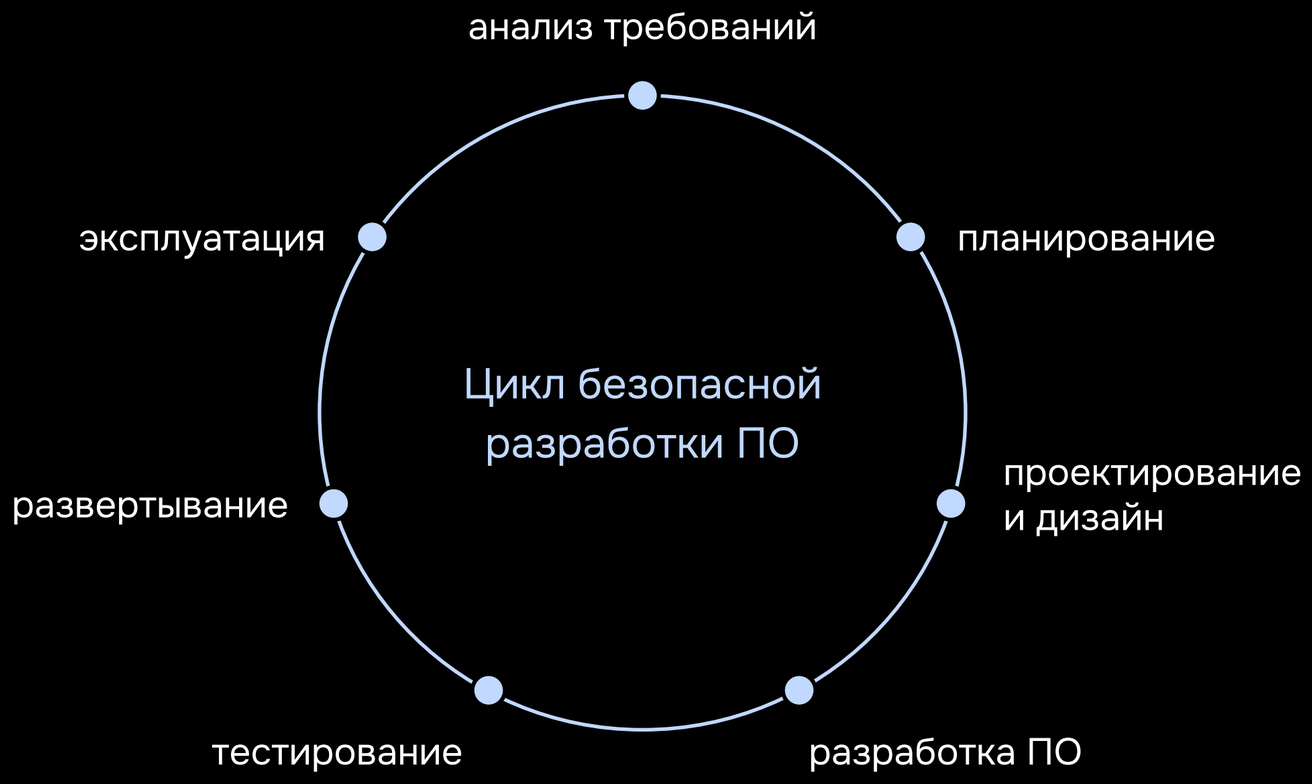
Deckhouse Stronghold

CERTIFIED SECURITY EDITION

Использование системного подхода

- Несколько продуктов в экосистеме Deckhouse имеют сертификаты соответствия ФСТЭК России
- Сертифицировать отдельно продукты без единых процессов безопасной разработки - долго и дорого
- Внедрение цикла безопасной разработки и сертификация продуктов

Безопасная разработка при сертификации Deckhouse Stronghold



Безопасная разработка при сертификации Deckhouse Stronghold

Требования ГОСТ Р 569393-2024

Анализ требований

- 5.3 Формирование и предъявление требований безопасности к ПО

Планирование

- 5.1 Планирование процессов разработки безопасного ПО
- 5.2 Обучение сотрудников

Проектирование и дизайн

- 5.4 Управление конфигурацией ПО
- 5.6 Разработка, уточнение и анализ архитектуры ПО
- 5.7 Моделирование угроз и разработка описания поверхности атаки

Безопасная разработка при сертификации Deckhouse Stronghold

Требования ГОСТ Р 569393-2024

Разработка ПО

- 5.5 Управление недостатками и запросами на изменение ПО
- 5.8 Формирование и поддержание в актуальном состоянии правил кодирования
- 5.9 Экспертиза исходного кода
- 5.10 Статический анализ исходного кода
- 5.12 Использование безопасной системы сборки ПО
- 5.13 Обеспечение безопасности сборочной среды ПО
- 5.14 Управление доступом и контроль целостности кода при разработке ПО
- 5.15 Обеспечение безопасности используемых секретов
- 5.16 Использование инструментов композиционного анализа
- 5.17 Проверка кода на предмет внедрения вредоносного ПО через цепочки поставок

Безопасная разработка при сертификации Deckhouse Stronghold

Требования ГОСТ Р 569393-2024

Тестирование

- 5.11 Динамический анализ кода программы
- 5.18 Функциональное тестирование
- 5.19 Нефункциональное тестирование

Развертывание

- 5.20 Обеспечение безопасности при выпуске готовой к эксплуатации версии ПО
- 5.21 Безопасная поставка ПО пользователям

Эксплуатация

- 5.22 Обеспечение поддержки ПО при эксплуатации пользователями
- 5.23 Обеспечение реагирования на информацию об уязвимостях
- 5.24 Поиск уязвимостей в эксплуатирующемся ПО
- 5.25 Обеспечение безопасности при выводе ПО из эксплуатации

Этапы сертификации

Январь 2025

Анализ требований, определение сертифицируемых функций безопасности

Январь – сентябрь 2025

Доработка Deckhouse Stronghold

Март 2025

Решение ФСТЭК России о сертификации Deckhouse

Сентябрь 2025

Согласование ПМИ с органом по сертификации

Октябрь – Декабрь 2025

Сертификация Deckhouse

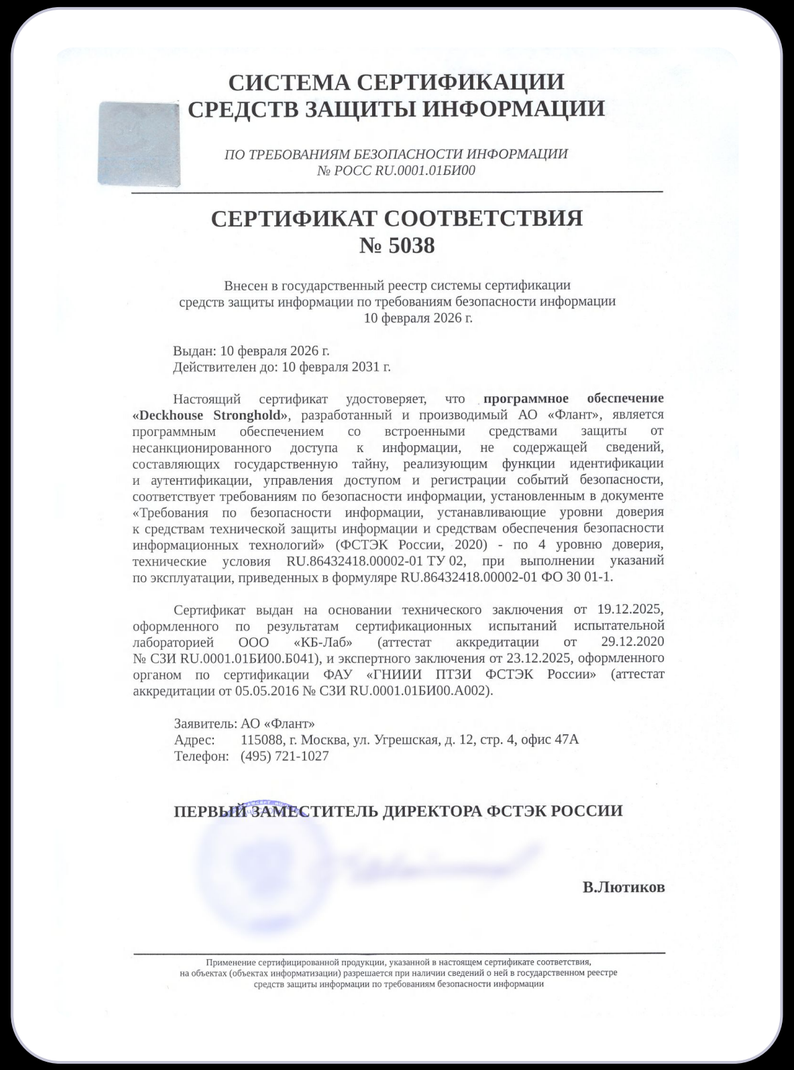
Декабрь 2025

Получение заключения от органа по сертификации

Февраль 2026

Получен сертификат соответствия

Сертификат ФСТЭК России № 5038 от 10 февраля 2026 г.



СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 5038

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
10 февраля 2026 г.

Выдан: 10 февраля 2026 г.
Действителен до: 10 февраля 2031 г.

Настоящий сертификат удостоверяет, что **программное обеспечение «Deckhouse Stronghold»**, разработанный и производимый АО «Флант», является программным обеспечением со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации, управления доступом и регистрации событий безопасности, соответствует требованиям по безопасности информации, установленным в документе «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, технические условия RU.86432418.00002-01 ТУ 02, при выполнении указаний по эксплуатации, приведенных в формуляре RU.86432418.00002-01 ФО 30 01-1.

Сертификат выдан на основании технического заключения от 19.12.2025, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «КБ-Лаб» (аттестат аккредитации от 29.12.2020 № СЗИ RU.0001.01БИ00.Б041), и экспертного заключения от 23.12.2025, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

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

- 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

- Соответствие техническим условиям RU.86432418.00002-01 ТУ 02

Функции безопасности

Deckhouse Stronghold Certified Security Edition (CSE) реализует следующие функции безопасности

- Идентификация и аутентификация пользователей (ИАФ)
- Управление доступом субъектов доступа к объектам доступа (УПД)
- Регистрация событий безопасности (РСБ)
- Обеспечение доступности информации (ОТД)

Deckhouse Stronghold

CERTIFIED SECURITY EDITION

Позволяет обеспечить:

01 Безопасность информации на значимых объектах критической информационной инфраструктуры до 1-й категории значимости **включительно**

02 Безопасность персональных данных в информационных системах до 1-го уровня защищённости **включительно**

03 Безопасность информации в государственных информационных системах до 1-го класса защищённости **включительно**

04 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**

Сертифицированное ФСТЭК России решение
для безопасного управления жизненным циклом секретов

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 01.05.2022 № 250

«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

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

Deckhouse Stronghold для выполнения требований ГОСТ Р 56939-2024

В соответствии с пунктом 5.15 Стандарта при разработке программного обеспечения необходимо обеспечить **безопасность использования секретов**, а также для хранения, управления и предоставления секретов и**спользовать систему управления секретами.**

Deckhouse Stronghold позволяет определить:

01 Порядок предоставления доступа к секретам

02 Типы секретов, сроки их эксплуатации, действия при компрометации

03 Порядок формирования, хранения и ротации секретов

04 Требования к системам хранения секретов

Применение Deckhouse Stronghold для выполнения требований безопасной разработки ПО

Приказ ФСТЭК России № 117

В случае самостоятельной разработки оператором (обладателем информации) программного обеспечения, предназначенного для использования в информационных системах, должны быть реализованы меры, предусмотренные разделами 4 и 5 ГОСТ Р 56939-2024.

В случае привлечения оператором (обладателем информации) для разработки программного обеспечения подрядной организации по решению руководителя (ответственного лица) в техническое задание на разработку программного обеспечения могут быть включены требования по разработке безопасного программного обеспечения в соответствии с ГОСТ Р 56939-2024.

Приказ ФСТЭК России № 239

В случае если в ходе проектирования подсистемы безопасности значимого объекта предусмотрена разработка программного обеспечения, в том числе программного обеспечения средств защиты информации, такая разработка проводится в соответствии со стандартами безопасной разработки программного обеспечения.

Внесение изменений и обновления Deckhouse Stronghold CSE

01 Новые версии Deckhouse Stronghold CSE выпускаем примерно раз в полгода. Информацию о новых версиях Deckhouse Stronghold CSE, а также инструкции по обновлению размещаем на нашем сайте

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

03 При внесении в Deckhouse Stronghold CSE изменений, не связанных с функциями безопасности, испытания проводим самостоятельно

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

Внесение изменений и обновления Deckhouse Stronghold CSE

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

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

03 Сообщить об уязвимости в Deckhouse Stronghold CSE можно через форму на сайте по адресу: deckhouse.ru/report-request

Поддерживаемые среды исполнения

Платформенное исполнение

Deckhouse Kubernetes Platform CSE

Standalone-исполнение

РЕД ОС, ALT Linux, Astra Linux Special Edition

Формат поставки

Компонент	Вид поставки
Дистрибутив ПО	В электронном виде на USB-накопителе
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
Копия сертификата	На бумаге

Дорожная карта

H1’2026

Дополнить сертифицированную версию Deckhouse Stronghold функцией шифрования ГОСТ в части seal wrap с использованием внешнего криптопровайдера и в части TLS

Результат:

Реализована возможность использовать российские криптографические алгоритмы для шифрования секретов, а также обеспечивать зашифрованный обмен данными между сервером и клиентом

H2’2026-2027

Провести оценку влияния среды функционирования в соответствии с требованиями ПКЗ-2005, направленную на проверку того, как компоненты встроенного средства криптографической защиты информации (СКЗИ) взаимодействуют с компонентами Deckhouse Stronghold

Результат:

Получено положительное заключение испытательной лаборатории и переданы материалы в ФСБ России для оформления заключения о признании решения соответствующим требованиям по эксплуатации СКЗИ

Deckhouse Stronghold
CERTIFIED SECURITY EDITION

Хотите настроить в своем проекте безопасное хранилище секретов, соответствующее требованиям ФСТЭК России?

Оставьте заявку на консультацию — проведём персональное демо Deckhouse Stronghold CSE и ответим на все вопросы.

Чек-лист для самостоятельной проверки ПО (pdf)

Оставить заявку на консультацию

+7 (495) 721-10-27

deckhouse.ru

Промокод от Deckhouse Академии

CSE15*

Этот промокод даёт скидку 15% на курс «Инструменты безопасности в Deckhouse Kubernetes Platform» от Deckhouse Академии

Присылайте промокод на почту
contact@deckhouse.ru

Курс «Инструменты безопасности в Deckhouse Kubernetes Platform»

Все курсы Deckhouse Академии

* Промокод действует до 12 апреля 2026 года включительно

DECKHOUSE CONF 2026

АПР’09 2026° | Main Stage