Deckhouse
Stronghold

Совершенно секретно

или Не всё тайное становится явным

О вендоре Deckhouse

Deckhouse
ФЛАНТ

17+
лет опыта
в Open Source

С 2017
года используем
Kubernetes в production

№1
контрибьютор в проекты
CNCF из России

550+
сотрудников

>260
компаний-пользователей

№1
в рейтинге вендоров систем
мониторинга и управления ИТ-
инфраструктурой *

Реестр
российского ПО

Лицензии и сертификаты
ФСТЭК России

АРПП «Отечественный
софт»

* Рейтинг «Российский рынок систем мониторинга и управления ИТ-инфраструктурой», TAdviser, 2026

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

* Продукт находится в активной фазе разработки, готовится выход релизной версии

Что такое секреты и почему их важно защищать

Deckhouse
Stronghold

Что можно считать секретами?

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

Секреты могут быть:

Пользовательскими

Инфраструктурными

Количество секретов непрерывно растёт

С ростом сложности цифровых цепочек поставок **разрастание секретов становится ахиллесовой пятой** для организаций любого размера и уровня безопасности*

* По данным отчёта The State Of Secrets Sprawl 2026 компании GitGuardian

Не все компании хранят секреты безопасно*

Интересный факт

Около 64% валидных секретов, скомпрометированных в 2022 году, так и **не были отозваны** к 2026 году**

80 %

ИТ/DevOps-команд не обеспечивают безопасного хранения секретов

65 %

уверены, что в их инфраструктуре более 500 секретов

60 %

сталкивались с утечками секретов

25 %

хранят секреты более чем на 10 ресурсах и обмениваются ими

* По данным отчёта Secrets Management: The Next Big Security Threat For Businesses компании 1Password

** По данным отчёта The State Of Secrets Sprawl 2026 компании GitGuardian

Ручное управление секретами — дорого и долго

Из-за утечки секретов компании несут не только репутационные, но и финансовые потери — средний ущерб от одной утечки оценивается в 11,5 млн руб.*

61 % DevOps-команд признались, что разработка продуктов ведётся с задержкой в связи с низким качеством процессов управления секретами**

80 % отметили, что слишком заняты, чтобы уделять должное внимание секретам**

25 минут в день тратит один сотрудник ИТ- и DevOps-команд на ручное управление секретами, что приводит к большим годовым издержкам**

* По данным отчёта «Оценка ущерба от утечек информации и затрат на ликвидацию последствий» группы ЦИРКОН и ГК Infowatch

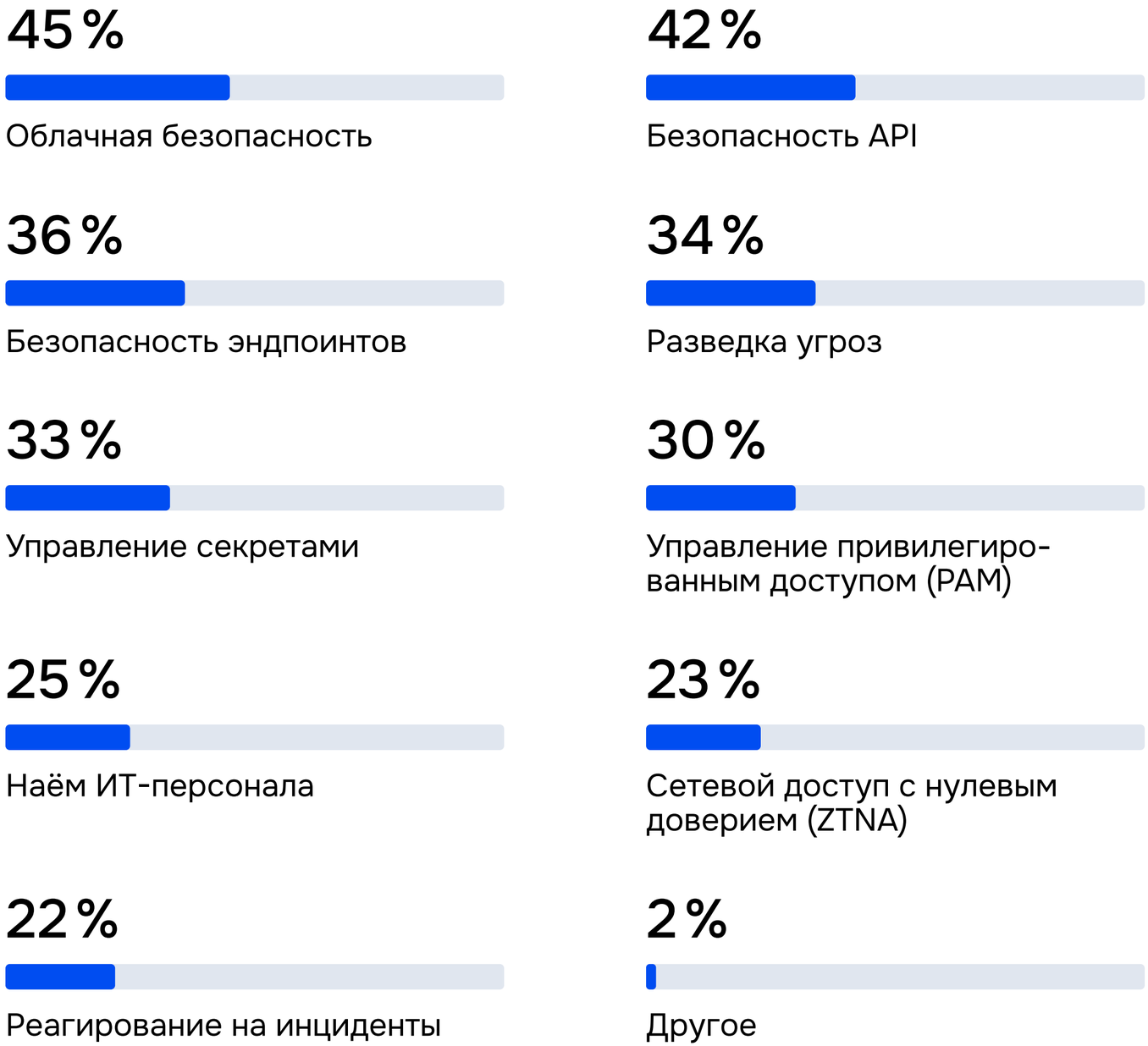
** По данным отчёта Secrets Management: The Next Big Security Threat For Businesses компании 1Password

Ручное управление секретами — дорого и долго

Количество секретов	1–100	100–500	Более 500
Количество сотрудников, чел.	1	2	4
Общие трудозатраты в день, ч.	0,25	2	8
Общие трудозатраты в год, ч.	62	496	1984
Издержки в год, руб.	124 000	992 000	3 968 000

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

Недавние кейсы

BINANCE

Код и пароли Binance были доступны на GitHub в течение нескольких месяцев

Источник: securitylab.ru

Mercedes-Benz

Исходные коды Mercedes-Benz утекли из-за случайно раскрытого токена GitHub

Источник: хакер.ru

GitLab

В публичных репозиториях GitLab оказалось более 17 000 секретов

Источник: bleepingcomputer.com

Использование секретов становится более массовым

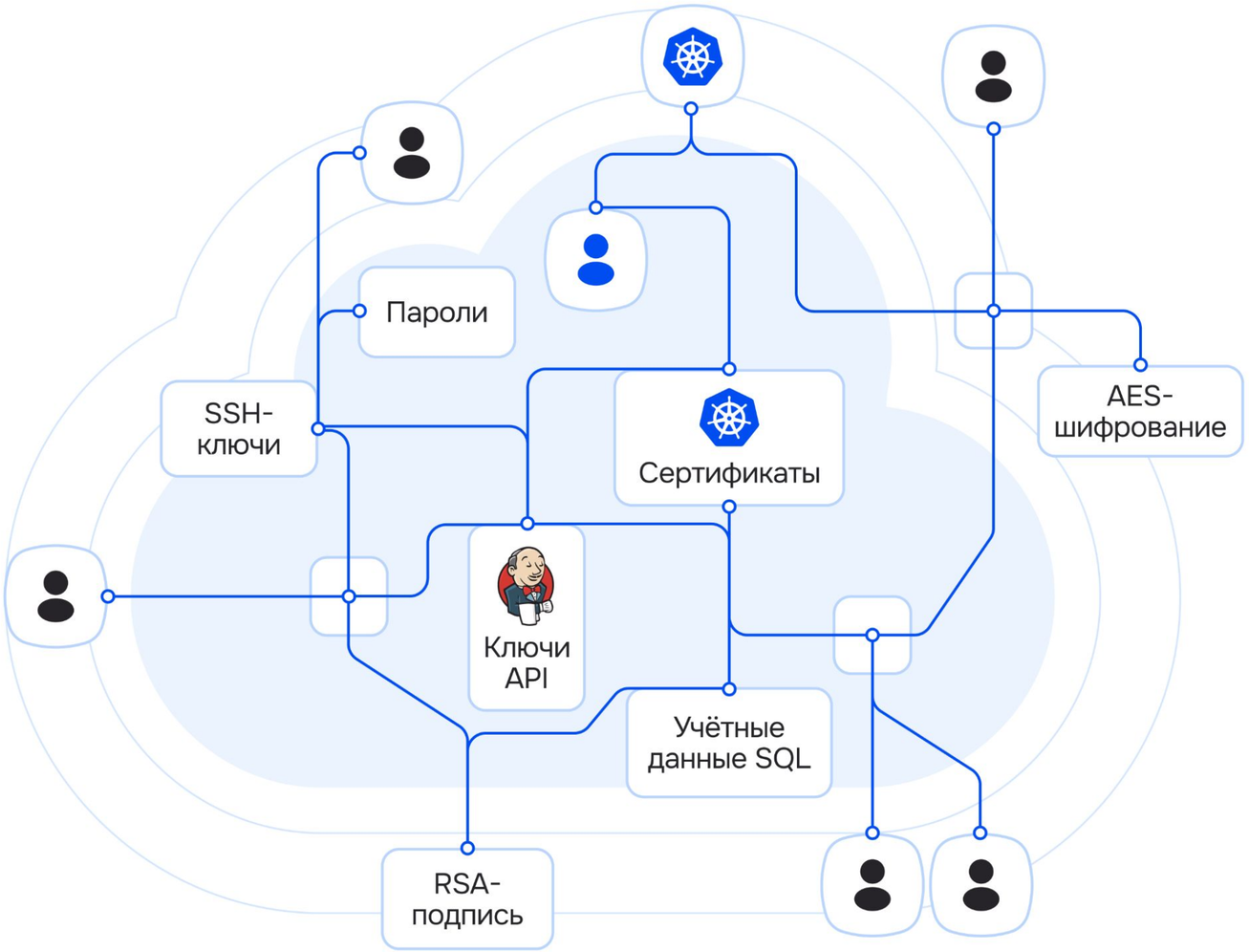
Основные тренды, влияющие на рост количества секретов:

01 Контейнеризация

02 Гибридные и мультиоблака

03 DevOps, DevSecOps, MLOps, CI/CD и автоматизация

04 Технологии Zero Trust



Важно!

Хранилища секретов и менеджеры паролей — это **не одно и то же**

Менеджеры паролей vs Хранилища секретов

Критерий	Менеджеры паролей	Хранилища секретов
Основная аудитория	Люди	Приложения, сервисы
Что хранят	Пароли к сайтам и сервисам, заметки, карточки	API-ключи, токены, сертификаты, SSH-ключи, пароли к БД, динамические секреты
Главная задача	Упростить человеку хранение и ввод паролей	Безопасно управлять жизненным циклом секретов (создание, изменение, ротация)
Сценарий использования	Войти в почту, CRM, GitHub, банковский сервис	Дать приложению доступ к базе данных, облаку, Kubernetes и сертификатам
Способ доступа	Веб-интерфейс, браузерное расширение, мобильное приложение	API, CLI, агенты, интеграции с приложениями и CI/CD, SDK

Менеджеры паролей vs Хранилища секретов

Критерий	Менеджеры паролей	Хранилища секретов
Интеграция с приложениями	Слабая или косвенная	Высокая, через API
Работа с сертификатами и ключами	Ограничена	Да, включая PKI, SSH, KMS/HSM-сценарии
Принцип доступа	Человек сам аутентифицируется в UI и получает доступ к секретам	Секреты выдаются по политике, по запросу и с TTL
Примеры решений	Passwork, 1Password, Bitwarden, KeePass	Vault, Stronghold, OpenBao, Infisical

Как правильно хранить секреты

В репозитории с секретами или репозитории приложений

В системе управления конфигурациями

В системе деплоя (Jenkins, Teamcity)

Только на серверах, на которых работает ваш сервис

Только на личном компьютере

В отдельном хранилище секретов

Ручное управление секретами

Фрагментация секретов

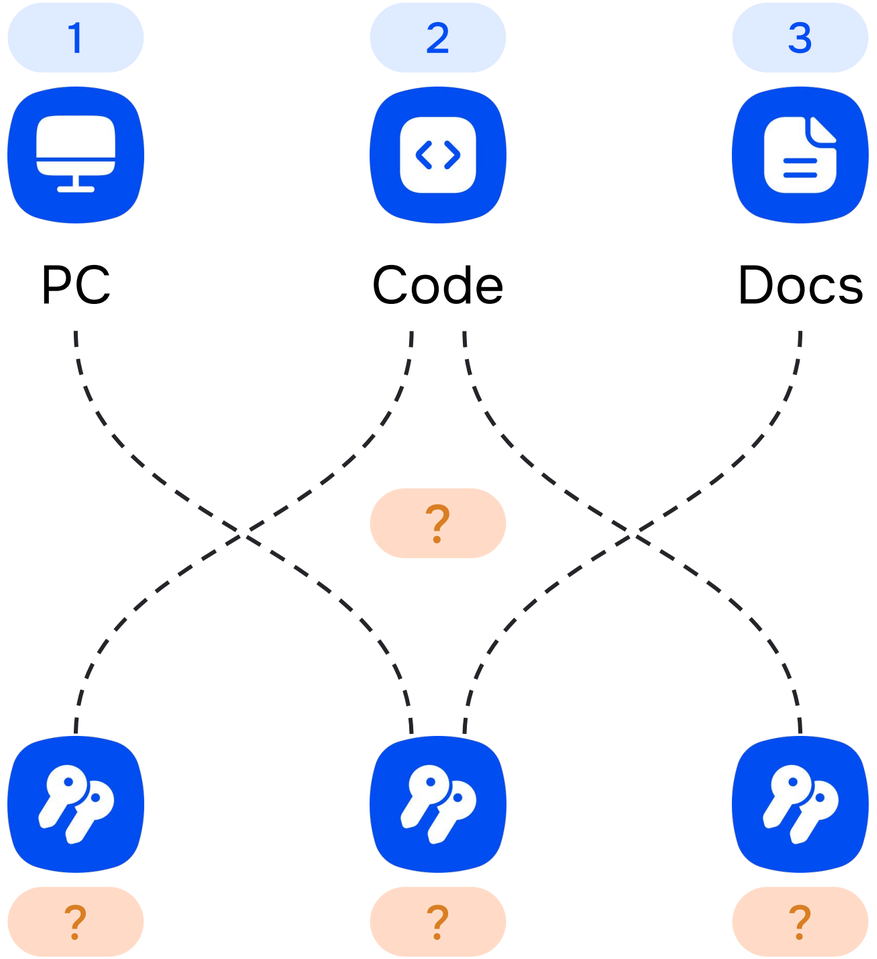
Секреты организации хранятся
хаотично и в небезопасных местах

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

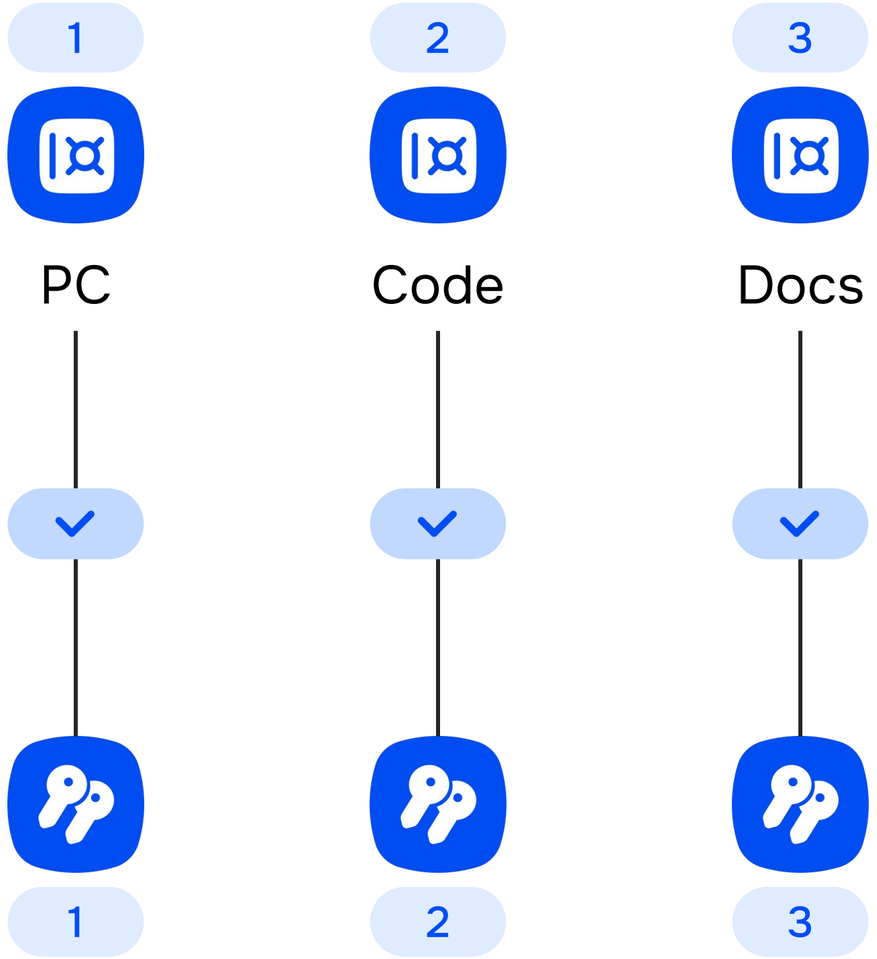
для безопасного хранения секретов

Лёгкое управление

жизненным циклом секретов
и ролями доступа к ним

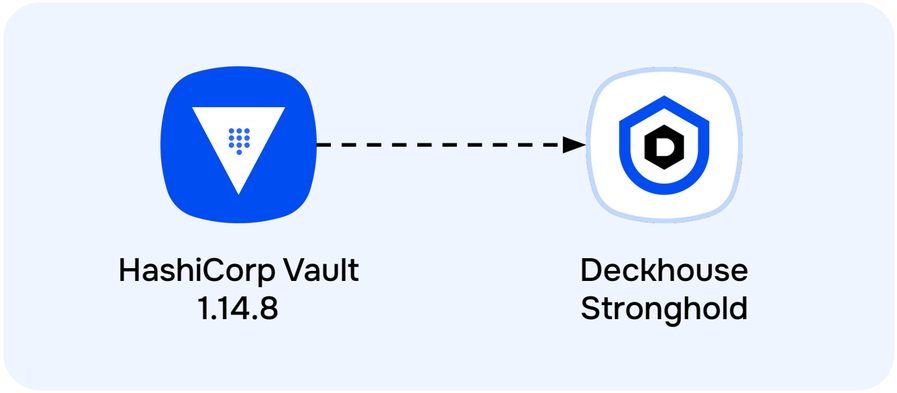
Полное шифрование данных

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



Что такое Deckhouse Stronghold

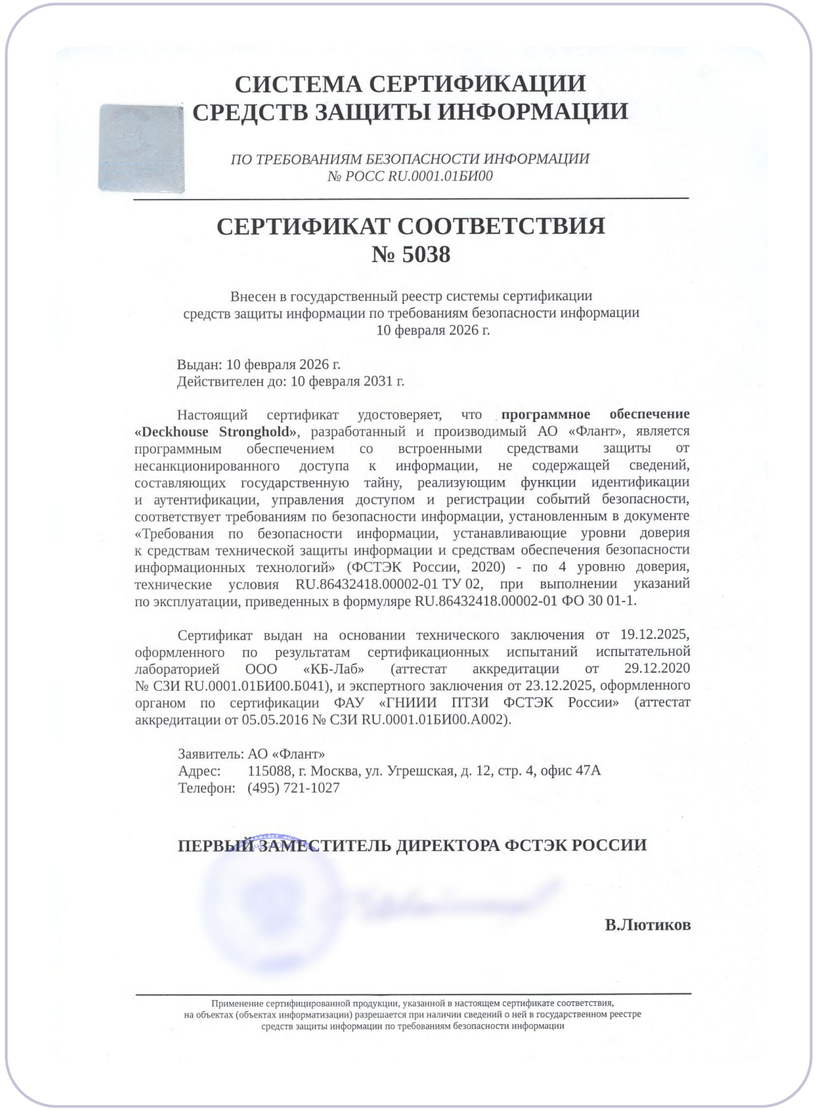
Решение для централизованного управления жизненным циклом секретов. Защищает пароли, ключи API, сертификаты, SSH-ключи, токены и другие конфиденциальные данные от утечек, а также обеспечивает безопасную доставку секретов в приложения.



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

Сертификат ФСТЭК России № 5038 от 10 февраля 2026 г.

- 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



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

Deckhouse Stronghold

CERTIFIED SECURITY EDITION

Сертифицированное ФСТЭК России решение для безопасного управления жизненным циклом секретов

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**

Какие задачи мы помогаем решать

Требования регуляторов

- 149-ФЗ, 152-ФЗ, 187-ФЗ
- Указы Президента РФ № 166 и 250
- Требования КИИ, ЗО КИИ, ГИС, ИСПДн

РБПО

- ГОСТ Р 56939-2024
- Приказы ФСТЭК России № 117 и 239

Импортозамещение

- HashiCorp Vault
- OpenBao

Безопасность

- Повышение уровня защищенности ИТ-инфраструктуры
- Оптимизация процессов управления секретами

Выполнение требований законодательства по защите конфиденциальной информации

Ситуация

Законодательство по защите КИ непрерывно развивается, появляются новые требования

Проблемы

Как разобраться в законах и выполнить необходимые требования?

Решение

Deckhouse Stronghold соответствует всем необходимым требованиям законодательства (ФЗ-152, ФЗ-149, ФЗ-187)

Переход на российское ПО

Ситуация

Западные вендоры ушли, оставив без поддержки

Проблемы

Какое ПО выбрать на замену? Какому вендору довериться?

Решение

Deckhouse Stronghold находится в реестре отечественного ПО (№ 22339 от 24.04.2024), полностью соответствует требованиям Минцифры России и имеет надёжную техническую поддержку от вендора

Отсутствие контроля и единого подхода

Ситуация

Бизнес развивается, вместе
с тем растёт и количество
секретов

Проблемы

Где хранятся секреты?
Надёжно ли они защищены?
Не случится ли утечка?

Решение

Deckhouse Stronghold хранит
все секреты в едином месте
в зашифрованном виде, благодаря чему
даже физическое хищение серверов
не позволит злоумышленникам получить
к ним доступ

Оптимизация трудозатрат персонала

Ситуация

Сотрудники тратят слишком много рабочего времени на ручное управление секретами

Проблемы

Как оптимизировать ресурсы и сфокусироваться на более профильных задачах?

Решение

Deckhouse Stronghold автоматизирует процессы хранения секретов и управления ими — это экономит в среднем 105 рабочих дней персонала в год

Deckhouse Stronghold помогает	Вы получаете
Исключить риски утечек конфиденциальной информации	Защиту бизнеса от финансовых и репутационных потерь
Оптимизировать трудозатраты персонала (команды DevOps и DevSecOps, сотрудники ИБ, разработчики)	Возможность фокусироваться на более профильных задачах
Сократить Time to Market и время интеграции при разработке собственных продуктов и сервисов	Своевременный запуск продуктов, соответствующих требованиям ИБ
Снизить издержки, возникающие вследствие ручного управления секретами	Уменьшение операционных расходов (OPEX) на ИБ

Возможные сценарии использования

01 Управление ЖЦ секретов

- Создание, хранение, доставка, отзыв и ротация секретов
- Безопасная выдача секретов приложениям и сервисам по политике доступа, с возможностью контроля, кто и когда получил нужные данные
- Шифрование «из коробки»

02 Управление инфраструктурой открытых ключей (PKI)

- Хранение сертификатов и ключей, включая списки отзыва, и управление их жизненным циклом

03 Секреты для CI/CD

- Безопасная передача секретов в пайплайны сборки и деплоя, чтобы не хранить их в переменных окружения, репозиториях или конфигурационных файлах
- Удобная интеграция с процессами автоматической сборки и доставки ПО, где пайплайны получают только те секреты, которые нужны им в конкретный момент

04 Управление динамическими секретами

- Создание временных учётных данных для доступа разработчиков и приложений к базам данных PostgreSQL, MySQL и MongoDB

Для кого полезно:

- Команды DevOps и DevSecOps
- Сотрудники подразделений ИБ
- Разработчики

Сравнение с конкурентами

	Stronghold	Vault EE	Vault CE	Аналог 1	Аналог 2
Репликация данных (KV, performance, DR)	✓	✓	✗	✗	✗
Автоматическое резервное копирование данных по заданному расписанию	✓	✓	✗	✓	✗
Шифрование root-ключа через HSM	✓	✓	✗	✓	✗
Двойное шифрование данных через HSM (с поддержкой ГОСТ-шифрования)	✓	✗	✗	✗	✗
Безопасный auto unseal хранилища без использования внешних KMS	✓	✗	✗	✗	✗
Управление AppRole, OIDC/JWT Role через веб-интерфейс	✓	✗	✗	✗	✗
Поддержка протоколов аутентификации (FIDO2/Passkeys, SAML2)	✓	✓	✗	✗	✗
Поддержка управляемых ключей (managed keys)	✓	✓	✗	✗	✗

Сравнение с конкурентами

	Stronghold	Vault EE	Vault CE	Аналог 1	Аналог 2
Управление конфигурацией через GitOps-плагин	✓	✗	✗	✗	✗
Просмотр операционных логов, аудит-логов и их фильтрация через веб-интерфейс	✓	✗	✗	✗	✗
Встроенная безопасная доставка секретов в приложения	✓	✗	✗	✓	✗
Сертификация ФСТЭК России	✓	✗	✗	✗	✓
Оценка влияния СКЗИ (ПКЗ-2005)	✓	✗	✗	✗	✗

В процессе реализации

Нам доверяют

Deckhouse Stronghold уже используется в production в различных отраслях

- Государственный сектор
- Топливно-энергетический комплекс
- Банковский сектор и финансы
- Транспорт
- Ритейл и e-commerce
- ИТ-компании

Публичные кейсы

Пассворк КВАНТ PremiumBonus

Deckhouse
Stronghold

Мы умеем хранить секреты!

Telegram

RuTube

Блог

contact@deckhouse.ru

+7 (495) 721-10-27

deckhouse.ru

Отказ от ответственности

Информация, изложенная в настоящем материале/презентации, представлена в ознакомительных целях и не является ни основанием для принятия коммерчески значимых решений, ни персональным либо публичным предложением к заключению каких-либо соглашений или договоров.

В связи с тем, что планы и решения касаемо возможностей осуществления процесса разработки и релиза указанных программных продуктов и/или их отдельных модулей остаются на усмотрение АО «Флант», настоящим мы не предоставляем каких-либо явных и/или подразумеваемых заверений об обстоятельствах либо гарантий касаемо, в том числе, но не ограничиваясь, функциональных характеристик, описания, коммерческих условий и возможности разработки, релиза и распространения программных продуктов.