

Deckhouse Stronghold CSE

Безопасность без компромиссов

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.

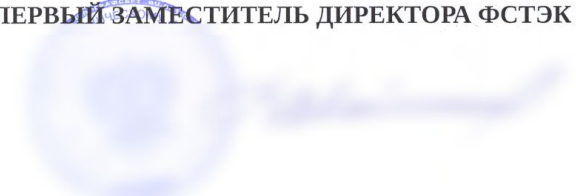
Выдан: 10 февраля 2026 г.
Действителен до: 10 февраля 2031 г.

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**

Защита информации на значимых объектах КИИ*

 Здоровоохранение


 Наука

 Транспорт


 Связь

 Энергетика

 Metallургия


 Топливо-
энергетический
комплекс

 Атомная энергетика

 Банковский сектор
и финансы

 Горнодобывающая
промышленность

 Химическая
промышленность

 Оборонная
и ракетно-космическая
промышленность

* 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. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Защита ПДн, обрабатываемых операторами*



Операторы
сотовой связи



Банки и финансовые
учреждения



Центры верификации
данных



Медицинские
и образовательные
учреждения



Государственные
и муниципальные
органы власти



Интернет-провайдеры



Транспортные компании



Ретейл и e-commerce



Страховые компании

* 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*



Федеральные и региональные органы исполнительной власти



Органы государственной власти субъектов Российской Федерации



Министерства и ведомства



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»

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»

Дорожная карта

H1'2026

Дополнить сертифицированную версию Deckhouse Stronghold функцией шифрования ГОСТ в части seal wrap с использованием внешнего криптопровайдера (КриптоПро CSP) 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

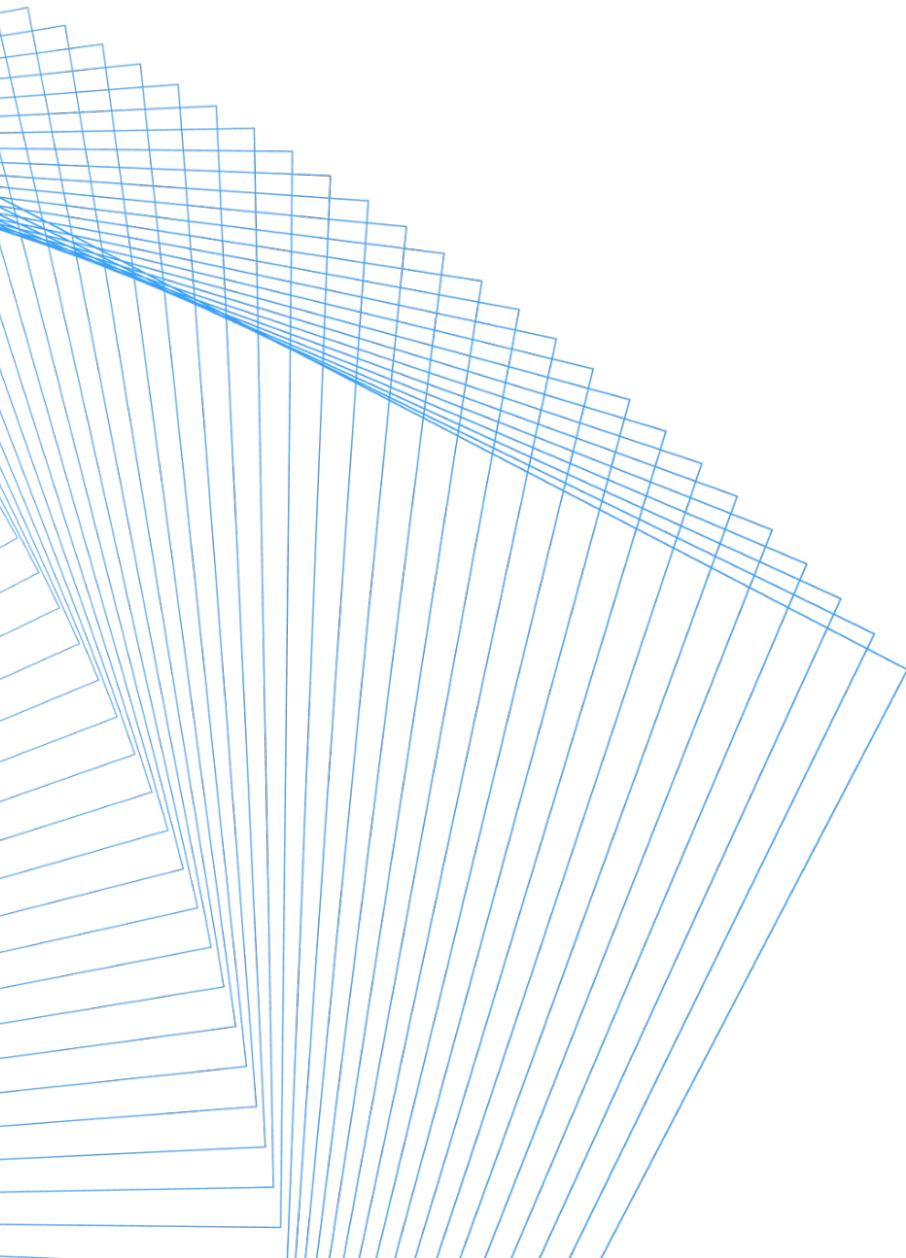
Провести оценку влияния среды функционирования в соответствии с требованиями ПКЗ-2005, направленную на проверку того, как компоненты встроенного средства криптографической защиты информации (СКЗИ) взаимодействуют с компонентами Deckhouse Stronghold

Результат:

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

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 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



Процесс устранения уязвимостей 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

Вебинар

Подтверждённая безопасность секретов: Deckhouse Stronghold получил сертификат ФСТЭК России



Вебинар



Владимир Девятайкин

Менеджер продукта
Deckhouse Stronghold



Ильдар Гарипов

Руководитель отдела
информационной безопасности

Документ

Перечень угроз ИБ

и соответствующих им функций ИБ СЗИ
Deckhouse Stronghold CSE



Документ

Документ

Меры по обеспечению безопасности для 30 КИИ

и соответствие реализации данных мер
в Deckhouse Stronghold CSE



Документ

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

Ответы на часто задаваемые вопросы

01 Какие среды исполнения поддерживаются?

Deckhouse Stronghold CSE можно запустить в различных сертифицированных средах (платформа контейнеризации: Deckhouse Kubernetes Platform CSE; операционные системы: РЕД ОС, ALT Linux, Astra Linux Special Edition).

02 Как происходит миграция с Deckhouse Stronghold EE на Deckhouse Stronghold CSE?

На сайте опубликована документация [🔗](#) по переходу с Deckhouse Stronghold EE на Deckhouse Stronghold CSE.

Процедура перехода между редакциями отработана.

Вам необходимо обратиться к нам в сервисную поддержку.

Сервисная команда отработает по каждому конкретному запросу.

Далее по стандартной инструкции запускается процесс миграции.

Переключение происходит практически без прерываний.

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 касаются 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 касаются, в том числе, но не ограничиваясь, функциональных характеристик, описания, коммерческих условий и возможности разработки, релиза и распространения программных продуктов.