Deckhouse
ФЛАНТ

чек-лист

Чек-лист для самостоятельной проверки ПО

Соответствует ли ваша система управления секретами требованиям к использованию на ЗО КИИ?

Использование системы управления секретами в инфраструктуре ЗО КИИ предполагает соответствие ряду требований к защите информации и применяемому ПО.
На практике не все организации могут быстро оценить, закрыты ли ключевые критерии.

Настоящий чек-лист разработан для самостоятельной оценки соответствия системы управления секретами требованиям законодательства. Он охватывает ключевые аспекты: идентификацию и аутентификацию, модель разграничения доступа, аудит событий безопасности, механизмы ротации секретов, требования к безопасной разработке и наличие сертификации.

Чек-лист поможет вам выявить потенциальные несоответствия и определить зоны для доработки.

- [ ] Идентификация и аутентификация пользователей и сервисов осуществляются через централизованную IDM/AD/LDAP-систему либо доверенные механизмы (OIDC, SAML)
- [ ] Средствами системы реализована ролевая модель управления доступом (RBAC) с поддержкой принципа минимальных привилегий
- [ ] Поддерживается разграничение доступа к секретам на уровне политик (по путям, типам секретов, операциям чтения/записи)
- [ ] Реализован механизм строгой аутентификации приложений (AppRole, OIDC/JWT, mTLS и др.) без хранения статических секретов в открытом виде
- [ ] Обеспечиваются централизованные регистрация и хранение событий безопасности (аудит действий пользователей и сервисов)
- [ ] Предусмотрены механизмы ротации, отзыва и автоматического обновления скомпрометированных секретов

При разработке ПО ваша организация руководствуется требованиями безопасной разработки ПО (SSDLC, анализ уязвимостей, регулярные обновления безопасности)

ПО включено в реестр российского ПО

ПО имеет сертификат соответствия требованиям безопасности информации ФСТЭК России

ПО является самостоятельным продуктом и имеет собственный сертификат соответствия (не является частью комплексного сертифицированного решения)

Deckhouse Stronghold разработан с учётом требований российского законодательства и отраслевых стандартов (149-ФЗ, 152-ФЗ, 187-ФЗ и ГОСТ Р 56939–2024) и обеспечивает централизованный контроль над секретами инфраструктуры.

Решение находится в реестре российского ПО и полностью соответствует требованиям Минцифры России, что позволяет реализовать необходимые механизмы защиты и снизить регуляторные и операционные риски в защищённых контурах.

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

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

Записаться на консультацию