

# Содержание

<b>Проблемы</b> .....	3
<b>Выгоды</b> .....	3
<b>Назначение</b> .....	3
<b>Компоненты решения</b> .....	3
<b>Обратная связь</b> .....	4



# ITI01 Hashicorp Vault

Инфраструктурные услуги, через тсл

## Проблемы

1. Необходимость выполнения требований информационной безопасности, предусматривающих недопустимость хранения логинов и паролей в открытом виде на сервере.
2. Слабая защищенность логинов и паролей технических учётных записей в базовой коробочной версии серверного приложения ADVANTA.

## Выгоды

1. Повышаем безопасность системы.
2. Пароли не хранятся в конфигах. В БД ADVANTA открыто хранится только хэш для доступа к Hashicorp Vault.
3. Решение Hashicorp Vault реализовано на основе ПО с открытым исходным кодом.

## Назначение

1. Начиная с версии ADVANTA 3.30, чтобы повысить безопасность хранения секретов (паролей, токенов/маркеров-доступа, API-ключей, закрытых криптографических ключей и т.п.) можно настроить подключение системы ADVANTA к СУБД или сервису Active Directory через сервис хранения секретов HashiCorp Vault. В этом случае в системе или файлах конфигурации не будут храниться пароли к сервисам и службам компании. Решение на основе ПО с открытым исходным кодом.

## Компоненты решения

HashiCorp Vault - это инструмент для управления секретами и обеспечения безопасности данных в облачной инфраструктуре. Его основное назначение - помочь организациям безопасно управлять доступом к конфиденциальной информации. Основные функциональные возможности:

1. Управление секретами:
  - a. Хранение различных типов секретов (пароли, API-ключи, SSH-ключи, RSA-токены, OTP)
  - b. Динамическая генерация доступа для сервисов
  - c. Возможность ротации и отзыва доступа
  - d. Централизованный контроль над всеми секретами
2. Управление доступом:
  - a. Аутентификация пользователей (как людей, так и машин)
  - b. Роль-based access control (RBAC) для человеческих пользователей
  - c. Временные токены для ограниченного доступа
  - d. Детальное логирование действий

- 3. Шифрование данных:
  - a. Защита данных при передаче (TLS)
  - b. Шифрование данных в состоянии покоя (AES 256-бит CBC)
  - c. Централизованное управление ключами
  - d. Возможность обновления ключей в распределенной инфраструктуре
- 4. Практическое применение:
  - a. Безопасное хранение учетных данных баз данных
  - b. Управление API-ключами для различных сервисов
  - c. Контроль доступа к конфиденциальной информации
  - d. Защита секретов при миграции в облако
  - e. Интеграция с CI/CD процессами

HashiCorp Vault особенно полезен для организаций, которые хотят улучшить безопасность своих облачных решений без ущерба для рабочих процессов разработки и эксплуатации. Это бесплатный open-source продукт с дополнительным enterprise-функционалом для крупных организаций.

Компонент	Стоимость / трудоемкость
1. ПО Hashicorp Vault	Бесплатное ПО
2. Работы по настройке силами ОИТ	От 40 часов
3. Разработка технической документации Варианты: а) краткая схема взаимодействия компонентов системы или б) подробный технический проект	От 40 часов

Ссылки:

[Настройка хранения строк подключения в Hashicorp Vault \(Wiki\)](#)

## Обратная связь

**\*\*Узнайте о возможностях платформы и подберите лучшее решение на базе ADVANTA\*\***

[Хочу так же](#)

From:

<https://wiki.a2nta.ru/> - **Wiki [3.x]**

Permanent link:

<https://wiki.a2nta.ru/doku.php/opportunities/services/infrastructure/iti01>

Last update: **20.01.2026 09:23**

