Общество с ограниченной ответственностью «Ребреин»
ИНН 7727409582, ОГРН 1197746106161
Адрес: 123056, город Москва, Большая Грузинская ул, д. 36а стр. 5а, офис 13

Утверждено
Приказом № ПР-1 от 17.06.2025 г.

Генеральный директор

_____ Фролкина Е.А.
«17» июня 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
– ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«УПРАВЛЕНИЕ СЕКРЕТАМИ И БЕЗОПАСНОСТЬЮ ИНФРАСТРУКТУРЫ С VAULT»

Срок реализации: 1 месяц
Количество часов: 52 акад. ч.
Форма обучения: заочная форма
Формат обучения: с применением исключительно дистанционных технологий
Возраст обучающихся: для лиц старше 17 лет, имеющих или получающих среднее профессиональное и (или) высшее образование

Москва, 2025 г.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая дополнительная профессиональная программа – программа программа повышения квалификации «Управление секретами и безопасностью инфраструктуры с Vault» (далее – Программа) разработана в соответствии с:

- Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказом Министерства образования и науки РФ от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Постановлением Правительства РФ от 11.10.2023 № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
- Профессиональным стандартом 06.026 «Системный администратор информационно-коммуникационных систем», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 26.10.2020 года № 60580;
- ФГОС высшего образования – бакалавриат по направлению 09.03.02 Информационные системы и технологии, утв. приказом Минобрнауки России от 19.09.2017 №926;
- Локальными нормативными актами ООО «Ребреин».

В данной программе учтены основные идеи формирования универсальных учебных действий учащихся и соблюдена преемственность с программами высшего и/или среднего профессионального образования.

Направленность программы: Программа имеет техническую направленность.

Адресат:
Программа адресована специалистам, которые отвечают за безопасность и управление инфраструктурой:

- Системные администраторы — освоят практики централизованного хранения секретов, управления ключами и паролями, что позволит повысить отказоустойчивость и управляемость инфраструктуры.
- DevOps-инженеры — научатся автоматизировать выдачу и ротацию секретов, а также интегрировать Vault с CI/CD-процессами, системами мониторинга и оркестраторами контейнеров.
- Cloud-инженеры — получат навыки управления доступом приложений к облачным сервисам, базам данных и внешним ресурсам.
- Специалисты по безопасности — смогут использовать Vault для построения политики контроля доступа, ведения аудита операций и снижения рисков утечек данных.

Требования к входным знаниям обучающегося:
Для успешного освоения программы слушателям рекомендуется:

- иметь опыт администрирования Linux-систем (работа с файловой системой, пользователями, сетевыми сервисами);
- знать основы сетевых технологий (протоколы TCP/IP, модель взаимодействия клиент–сервер, базовые принципы маршрутизации и DNS);
- разбираться в принципах работы контейнеризации и оркестраторов (Docker, Kubernetes на базовом уровне);
- понимать основы CI/CD и процессов автоматизации инфраструктуры;

- иметь базовые представления о принципах информационной безопасности (аутентификация, авторизация, управление доступом, шифрование).

Актуальность реализации:

Современные инфраструктуры становятся всё более распределёнными и сложными: микросервисы, облачные платформы и контейнерные оркестраторы требуют безопасного управления доступом и секретами. Использование файлов, вручную прописанных ключей или «жёстко зашитых» паролей ведёт к высоким рискам компрометации данных. HashiCorp Vault сегодня является одним из наиболее востребованных инструментов для централизованного и безопасного управления секретами в масштабируемых системах. Его внедрение позволяет снизить вероятность утечек, повысить уровень автоматизации и соответствовать требованиям информационной безопасности.

Отличительные особенности программы:

- Фокус на практическом применении Vault — от базовых концепций до интеграции с Kubernetes и CI/CD.
- Подробный разбор различных Secret Engines, включая KV, Database, PKI, Transit и LDAP.
- Изучение механизмов аутентификации и контроля доступа, которые позволяют гибко выстраивать политику безопасности.
- Освещение тем высокой доступности и отказоустойчивости Vault, а также механизмов резервирования.
- Включение аспектов мониторинга и аудита, необходимых для построения защищённой и прозрачной инфраструктуры.

Объем и срок освоения программы: 52 академ. ч. в течение 1 мес.

Доступ к материалам Программы у обучающихся остаётся и после окончания периода обучения. Это позволяет повторять изученный материал в удобное время, восполнять пробелы в знаниях, а также возвращаться к практическим заданиям при решении рабочих задач. Такой формат способствует более глубокому закреплению навыков и поддерживает профессиональное развитие выпускников даже после завершения обучения.

Выдаваемый документ о квалификации: удостоверение о повышении квалификации и/или сертификат об успешном освоении программы.

Цели и задачи программы:

Цель курса — сформировать у слушателей целостное понимание принципов работы HashiCorp Vault и освоить практические навыки управления секретами, аутентификацией, контролем доступа и интеграцией Vault с различными сервисами и инфраструктурными решениями.

Программа направлена на решение следующих основных задач:

Обучающие:

- дать знания о принципах централизованного управления секретами и их жизненным циклом;
- познакомить с архитектурой HashiCorp Vault и механизмами аутентификации;
- научить применять Secret Engines (KV, Database, PKI, Transit, LDAP, Kubernetes) для решения практических задач;
- сформировать умения интеграции Vault с Kubernetes, CI/CD-процессами и облачными сервисами;
- освоить методы мониторинга, аудита и обеспечения отказоустойчивости Vault.

Развивающие:

- развить навыки проектного и системного мышления при построении безопасной инфраструктуры;
- сформировать умение анализировать угрозы, оценивать риски и применять инструменты Vault для их минимизации;
- развить практические компетенции работы с современными инструментами DevOps и Cloud-инженерии.

Воспитательные:

- способствовать формированию культуры ответственного отношения к вопросам информационной безопасности;
- воспитать понимание важности защиты данных и управления доступом на основе политик;
- привить стремление к использованию лучших практик в области безопасного администрирования и автоматизации.

Планируемые результаты:

Знания:

- принципы централизованного управления секретами и их жизненного цикла;
- архитектуру и основные компоненты HashiCorp Vault;
- методы аутентификации (Token, AppRole, LDAP и др.) и их особенности;
- различия между статическими и динамическими секретами;
- принципы построения высокодоступных кластеров и организации резервного копирования;
- возможности интеграции Vault с Kubernetes и CI/CD-процессами.

Умения:

- устанавливать и настраивать HashiCorp Vault, выполнять инициализацию и разблокировку хранилища;
- настраивать различные методы аутентификации и интегрировать их с инфраструктурой;
- разрабатывать и применять политики доступа, включая сложные сценарии;
- работать с KV Secret Engine (v1/v2), Database Secrets Engine, а также с PKI, Transit, LDAP, Kubernetes Secret Engines;
- настраивать мониторинг метрик Vault и аудит использования секретов;
- интегрировать Vault с Kubernetes при помощи Vault Agent, External Secrets Operator и других инструментов.

Навыки:

- установка и эксплуатация Vault в продуктивных средах;
- проектирование и администрирование отказоустойчивых конфигураций;
- практическое применение механизмов шифрования, управления сертификатами и ключами;
- обеспечение безопасности инфраструктуры через контроль доступа и аудит действий;
- автоматизация процессов управления секретами в DevOps- и Cloud-средах.

Перечень профессиональных компетенций, на получение которых направлено обучение:

На основе профстандарта 06.026 «Системный администратор информационно-коммуникационных систем»:

- B/02.5 Обеспечение работы технических и программных средств информационно-коммуникационных систем;
- C/05.6 Выполнение обновления программного обеспечения сетевых устройств информационно-коммуникационных систем;
- C/08.6 Планирование и проведение работ по распределению нагрузки между имеющимися ресурсами, снятию нагрузки на сетевые устройства информационно-коммуникационных систем перед проведением регламентных работ, восстановлению штатной схемы работы в случае сбоев.

Таким образом, в результате освоения программы у обучающихся формируются следующие профессиональные компетенции:
- ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем;
- ОПК-6. Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий;
- ОПК-7. Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем.

Организационно-педагогические условия реализации программы дополнительного профессионального образования

Язык реализации образовательной программы: обучение проводится на русском языке.

Форма обучения: заочная форма.

Особенности реализации программы: программа реализуется с использованием электронного обучения и исключительно дистанционных образовательных технологий.

Условия набора: на обучение принимаются все желающие лица, оплатившие обучение и заключившие договор об образовании. Обучение проходит в индивидуальном формате без формирования учебных групп. Обучающийся самостоятельно определяет время освоения Программы.

Формы проведения занятий:
- занятия в текстовом формате;
- практическая работа;
- самостоятельная работа с литературой;
- индивидуальные вопросы.

Материально-техническое оснащение

Материальное обеспечение программы

Занятия проводятся в системе дистанционного обучения «Rebrain». Каждый обучающийся и педагог оснащены доступом к системе дистанционного обучения: https://rebrainme.com/.

У педагога дополнительного профессионального образования имеется необходимое оборудование средства для реализации программы: ноутбук с подключением к интернету, программное обеспечение.

Методическое обеспечение программы

Программа обеспечена:

- учебно-методическими материалами (текстовые занятия, полезными материалами);
- практическими заданиями.

Кадровое обеспечение:

К реализации программы в качестве педагогов дополнительного образования допускаются лица:

1) отвечающее одному из требований:

а) имеющее высшее образование или среднее профессиональное образование в рамках укрупненных групп специальностей и направлений подготовки высшего образования и специальностей среднего профессионального образования «Образование и педагогические науки»;

б) имеющее высшее образование либо среднее профессиональное образование в рамках иных укрупненных групп специальностей и направлений подготовки высшего образования и специальностей среднего профессионального образования при условии его соответствия дополнительной общеобразовательной общеразвивающей программе, реализуемой ООО «Ребреин», и получение при необходимости дополнительного профессионального образования педагогической направленности;

в) успешно прошедшее промежуточной аттестации не менее чем за два года обучения по образовательным программам высшего образования по специальностям и направлениям подготовки, соответствующей направленности дополнительной общеобразовательной общеразвивающей программе;

2) не имеющее ограничений на занятие педагогической деятельностью, установленных законодательством Российской Федерации;

3) прошедшее обязательный предварительный (при поступлении на работу) и периодические медицинские осмотры (обследования), а также внеочередные медицинские осмотры (обследования) в порядке, установленном законодательством Российской Федерации.

Реализация Программы также возможна лицами, привлекаемыми на условиях гражданско-правового договора в соответствии с действующим законодательством РФ.

2. УЧЕБНЫЙ ПЛАН

№ п/п	Наименование модуля	Количество часов			Формы контроля / аттестация
		Всего	Теория	Практика	
1	Модуль 1 “Онбординг”	2	1	1	Входное тестирование
2	Модуль 2 “HashiCorpVault”	43	15	28	Практическое задание
3	Итоговая аттестация	8		8	Итоговое практическое задание

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

№ п/п	Наименование модуля	1 неделя	2 неделя	3 неделя	4 неделя
1	Модуль 1 “Онбординг”	1			

2	Модуль 2 “HashiCorpVault”	12	13	13	5
3	Итоговая аттестация				8 | А

4. РАБОЧАЯ ПРОГРАММА

Модуль 1. Онбординг
Теория 1 академ. ч. Практика 1 академ. ч.
Модуль состоит из следующих тем:

Тема 1: Онбординг

В модуле обучающемуся предоставляется вводный конспект, содержащий общую информацию о программе, структуре курса, форматах взаимодействия с материалами и ожидаемых результатах обучения.

Предусмотрено прохождение входного тестирования, включающего 7 вопросов, направленных на закрепление информации из онбординга. В рамках темы обучающийся выполняет задание по целеполаганию: формулирует свою цель прохождения программы, указывает желаемые навыки по окончании обучения, а также оценивает текущий уровень своих знаний, выбрав один из предложенных вариантов.

Модуль 2. HashiCorpVault
Теория 15 академ. ч. Практика 28 академ. ч.

Модуль состоит из следующих тем:
Тема 1: Введение в управление секретами
Содержание: Понятие «секреты». Утечка секретных данных. Решение проблемы утечек — инструменты для хранения секретов. Способы установки HashiCorp Vault. Практическое задание.

Тема 2: Архитектура Hashicorp Vault
Содержание: Основные компоненты архитектуры Vault и их взаимодействие. Инициализация Vault. Механизм блокировки/разблокировки хранилища. Практическое задание.

Тема 3: Аутентификация в Vault: Token
Содержание: Что такое аутентификация в Vault. Разница аутентификации систем и пользователей. Механизм аутентификации Token. Практическое задание.

Тема 4: Аутентификация в Vault: приложения и пользователи
Содержание: Механизм аутентификации в Vault для приложений AppRole. Два механизма аутентификации в Vault для пользователей UserPass, LDAP. Другие механизмы аутентификации Github, Kubernetes, JWT. Практическое задание.

Тема 5: Удостоверение и контроль доступа
Содержание: политики доступа, их структуру и синтаксис. Применение политик к путям и ресурсам. Наследование политик и использование wildcards. Мониторинг и аудит доступа. Создание политик для сложных сценариев. Применение политик к различным методам аутентификации. Практическое задание.

Тема 6: Введение в Secret Engines. KV Secret Engine

Содержание: Статические и динамические типы секретов, и зачем их разделяют. Секретные движки в Vault. Как создавать и управлять секретами с помощью KV Secret Engine. Практическое задание.

Тема 7: Динамические секреты и Database Secrets Engines
Содержание: Разница статических и динамических секретов. Преимущества динамических секретов. Как работают динамические секреты. Database Secrets Engines. Практическое задание.

Тема 8: Secrets Engines: PKI, Transit, LDAP, Kubernetes
Содержание: LDAP. PKI и сертификат CA в Vault. Transit. Kubernetes. Практическое задание.

Тема 9: Высокодоступность и резервирование в Vault
Содержание: принципы работы высокодоступных систем. Архитектуру высокодоступного кластера Vault. Особенности настройки HA-кластера. Виды резервного копирования. Особенности настройки резервного копирования в Vault. Процесс восстановления данных из резервной копии. Практическое задание.

Тема 10: Мониторинг и аудит
Содержание: зачем нужен мониторинг и аудит в системах управления секретами. Какие метрики важно отслеживать. Какие встроенные и внешние инструменты мониторинга и аудита пригодятся в работе. Что такое аудит-логи и какие данные они содержат. Практическое задание.

Тема 11: Интеграция Vault с Kubernetes
Содержание: основные концепции интеграции Vault с Kubernetes. Обзор способов подключения Vault в Kubernetes. Установку и настройку Vault в Kubernetes различными способами: Vault Agent, External Secrets Operator, Vault Secrets Operator. Практическое задание.

Модуль направлен на формирование у обучающихся базовых и продвинутых навыков работы с Vault. Каждая тема модуля включает текстовое занятие с теоретическим материалом и пошаговыми инструкциями, после изучения которого предлагается практическое задание. Практические задания рассчитаны на 1-2 академических часа. Выполнение заданий предполагает отправку решения на проверку через личный кабинет обучающегося. Критерии оценки прописаны в описании к каждому заданию. В случае корректного выполнения выставляется зачёт. Если работа содержит ошибки, задание возвращается на доработку. При повторной неудачной попытке (после двух доработок) обучающийся получает «незачёт».

Итоговая аттестация.
Блок посвящён выполнению финального практического задания без предварительного теоретического блока.

5. МЕТОДИЧЕСКИЕ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Программа обеспечена системой дистанционного обучения https://rebrainme.com/.

Педагогические технологии:
- технология дифференцированного обучения;

- технология разноуровневого обучения;
- технология развивающего обучения;
- технология проблемного обучения;
- технология дистанционного обучения.

Методы обучения:
- словесный, наглядный практический;
- объяснительно – иллюстративный;
- частично-поисковый, исследовательский проблемный;
- игровой, дискуссионный.

Электронно-библиотечные ресурсы и системы, информационно-справочные системы:
1. Научная электронная библиотека eLIBRARY.RU.
2. Собственные учебные материалы: https://rebrainme.com/courses/vault
3. Официальная документация Vault [Электронный ресурс]: https://developer.hashicorp.com/vault/docs

6. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Оценочные материалы:

Для отслеживания результатов освоения программы среди слушателей проводится текущий контроль, промежуточный контроль и итоговое оценивание.

Текущий контроль

Осуществление текущего контроля проводится после занятий в виде написания практических заданий или тестирований. Тематика и условия выполнения практических заданий расписаны в личном кабинете обучающегося в СДО. Педагог проверяет решение и принимает решение о принятии решения (зачет), о необходимости доработать решение или о незачете. Если промежуточный контроль представлен в виде тестирования, подсчет верных ответов и выставление оценки «зачёт» и «незачёт» происходят в автоматическим решиме в СДО.

Тема 2: Архитектура Hashicorp Vault
Практическая работа

Вам будет предоставлено две виртуальные машины, находящиеся в одной подсети. На каждой из них установлен Vault по пути /usr/local/bin/vault, а файл конфигурации находится по пути /etc/vault.d/vault.hcl.

Распределение ролей:
- vault-architecture-1 – сервер, который будет выполнять функцию автоматизированного unseal (распечатывающего сервиса) для основного инстанса Vault. Важно: на этом сервере необходимо настроить прослушивание на адресе 0.0.0.0. (полный путь к ключу должен быть таким transit/keys/autounseal)
- vault-architecture-2 – основной сервер Vault, который будет разблокирован с помощью сервиса, настроенного на vault-architecture-1.

В процессе выполнения задания изменяйте файлы конфигурации. Перезапуск Vault можно производить командой:
sudo systemctl restart vault

Процесс работы:

1. Инициализируйте Vault на сервере vault-architecture-1 с использованием 7 ключей unseal, из которых 5 будут использоваться для разблокировки хранилища. Запишите root-токен в файл /tmp/vault_token.
2. Выполните процесс unseal, используя ключи, которые были получены на предыдущем шаге.
3. На сервере vault-architecture-1 (распечатывающем сервере) настройте автоматизацию процесса unseal для основного инстанса Vault с использованием механизма Transit SE. В качестве руководства для настройки используйте подробную инструкцию от HashiCorp. При настройке автоматизации используйте имя unseal-ключа autounseal.

Тема 8: Secrets Engines: PKI, Transit, LDAP, Kubernetes
Практическая работа
Root Token для выполнения заданий: hvs.OAA9HASUDAH7b7TZ9NUbAOAu

Задание 1. Импортируйте промежуточный CA в PKI движок и выпустите конечный сертификат
1. Включите PKI Secrets Engines по пути rebrain-pki/.
2. Настройте максимальный срок жизни сертификата 1 год (8760 часов) при помощи команды tune.
3. Создайте сертификат CA в файле /opt/certs/bundle.pem, со следующим содержимым [...]

Итоговое оценивание
В конце программы обучающиеся сдают итоговую аттестацию.

Финальный проект
Финальное задание для построения базовой высокодоступной инфраструктуры Vault в кластере Kubernetes.

Представьте, что вы работаете в IT-отделе крупной технологической компании. Ваш руководитель возвращается с конференции, на которой обсуждали последние достижения в области управления секретами и безопасности. Во время встречи он делится своими впечатлениями:

Я вчера участвовал в секции о современных подходах к защите данных и управления доступом. Выступающие рассказывали о том, как HashiCorp Vault может централизовать хранение секретов, обеспечить безопасную передачу данных, упростить доступ к базам данных и интеграцию с облачными сервисами. У нас сейчас каждый департамент по-своему управляет ключами и паролями, и это полный хаос. Нам нужно внедрить Vault, чтобы унифицировать подходы, а также улучшить мониторинг и аудит безопасности. Это твоя задача. Сделай так, чтобы мы стали эталоном для других компаний!

Будет использован кастомный Helm Chart vault-0.29.0.tgz, лежащий в папке /home/user/.

Задание:
1. Создайте необходимые namespaces — vault, monitoring и mongodb.
2. Разверните отказоустойчивый кластер с Raft backend. При правильной настройке Helm Chart не запустится без инизиализации прометея, поэтому для начала раскатаем его.
3. Добавьте все необходимые репозитории для Helm:

```
helm repo add prometheus-community https://prometheus-community.github.io/helm-charts
helm repo update
helm install -n monitoring prometheus prometheus-community/kube-prometheus-stack
[...]
```

Результаты текущего контроля и итогового оценивания отображаются в личном кабинете слушателя в системе дистанционного обучения https://rebrainme.com/.

По результатам сдачи текущего контроля и итогового оценивания педагог даёт обратную связь слушателям, отмечает их сильные стороны и обращает внимание на зоны для развития. При необходимости педагог может повторить пройденные темы со слушателями, если установлен факт плохого закрепления и усвоения темы у слушателей.