

Введение

В современном мире компании сталкиваются с необходимостью безопасного хранения и управления конфиденциальными данными, такими как пароли, токены доступа и криптографические ключи. Утечка такой информации может привести к серьезным последствиям, включая финансовые потери, репутационный ущерб и юридические санкции. Ручное управление секретами или использование устаревших методов, таких как хранение данных в текстовых файлах, увеличивает риски утечек и затрудняет контроль доступа.

Даже актуальные решения, такие как HashiCorp Vault [1] или AWS Secrets Manager [2], часто оказываются сложными в настройке и интеграции, требуют значительных ресурсов и не всегда предоставляют достаточную гибкость для адаптации под конкретные бизнес-задачи. Это создает потребность в более простых, но при этом надежных и масштабируемых решениях, которые могли бы обеспечить безопасное хранение данных, гибкое управление доступом и удобство использования для сотрудников.

Цели и задачи:

Цель работы – разработка веб-приложения, предоставляющего централизованное решение для безопасного хранения и управления корпоративными секретами. Оно будет использовать ролевую модель доступа (RBAC [3]), интеграцию с Keycloak [4] для аутентификации и многофакторную аутентификацию (MFA [5]). Уникальной особенностью является использование изолированных рабочих пространств, где пользователи могут гибко управлять правами доступа к секретам.

Основные задачи разработки включают реализацию следующей функциональности:

- Управление секретами: Создание, редактирование и удаление конфиденциальных данных (пароли, токены, ключи) с настройкой срока действия.
- Ролевая модель доступа (RBAC): Гибкое управление правами пользователей в рамках рабочих пространств.
- Рабочие пространства: Изолированные области для хранения и управления секретами с возможностью добавления пользователей и назначения ролей.
- Интеграция с Keycloak: Авторизация и аутентификация пользователей через единую систему.
- Журнал аудита: Логирование всех действий пользователей для обеспечения прозрачности и безопасности.
- Уведомления через Telegram-бота [6]: Оперативное информирование о событиях, таких как изменения в секретах или истечение их срока действия.

- Шифрование данных: Защита конфиденциальной информации с использованием AES-256.

1. Глава 1. Предметная область и существующие решения

1.1. Описание предметной области

В современном мире, где информационные технологии играют ключевую роль в бизнесе и повседневной жизни, безопасность данных становится одной из самых актуальных проблем. Корпоративные секреты, такие как пароли, SSH-ключи, токены доступа и сертификаты, являются критически важными элементами, обеспечивающими функционирование ИТ-инфраструктуры. Утечка таких данных может привести к серьезным последствиям, включая финансовые потери, репутационный ущерб и даже юридические санкции. В связи с этим, управление корпоративными секретами становится важной задачей для любой организации, стремящейся минимизировать риски и обеспечить безопасность своих данных.

Однако управление секретами вручную или с использованием устаревших методов (например, хранение паролей в текстовых файлах) сопряжено с множеством вызовов. Это и сложность контроля доступа, и риск утечек, и трудности с аудитом и мониторингом. В условиях растущих киберугроз и ужесточения требований к защите данных, компании нуждаются в современных инструментах, которые помогут им эффективно управлять секретами и обеспечивать их безопасность.

Для пользователей, таких как ИТ-администраторы и сотрудники компаний, приложение предоставляет удобный и безопасный способ управления корпоративными секретами. Оно упрощает процесс хранения и доступа к конфиденциальной информации, снижая риск ошибок и утечек. Ролевая модель доступа позволяет администраторам гибко настраивать права для различных пользователей и команд, что обеспечивает соблюдение принципа минимальных привилегий. Кроме того, интеграция с системами аутентификации, такими как Keycloak, и поддержка многофакторной аутентификации (MFA) повышают уровень безопасности.

Для компаний, которые будут использовать это приложение, оно предоставляет не только удобство, но и уверенность в безопасности своих данных. Приложение позволяет минимизировать риски утечек, упростить управление учетными данными и обеспечить соответствие требованиям внутреннего и внешнего аудита. Ведение журналов аудита и возможность экспорта логов позволяют компаниям оперативно реагировать на инциденты и анализировать действия пользователей.

Кроме того, приложение обеспечивает баланс между простотой использования и индивидуальностью. Оно предлагает гибкие настройки, такие как создание рабочих пространств, настройка прав доступа и интеграция с Telegram-ботом для уведомлений, что делает его удобным для различных сценариев использования. При этом оно сохраняет высокий

уровень безопасности, что особенно важно для компаний, работающих с конфиденциальной информацией.

В современном контексте, где информационная безопасность становится критически важной, такие инструменты играют ключевую роль в обеспечении устойчивости бизнеса. Они помогают компаниям минимизировать риски, связанные с утечками данных, и обеспечивают соответствие требованиям регуляторов. Таким образом, данное приложение не только решает актуальные проблемы, но и способствует формированию культуры безопасности в организациях, что делает его ценным инструментом в современной ИТ-инфраструктуре.

1.2. Описание существующих решений

На рынке уже существует множество решений, таких как HashiCorp Vault, AWS Secrets Manager, 1Password [7] и другие, которые предлагают различные подходы к хранению и защите секретов. Однако каждое из этих решений имеет свои ограничения, будь то сложность настройки, высокая стоимость или недостаточная гибкость интеграции с корпоративными системами. В данной части я проведу сравнительный анализ моего приложения с ключевыми конкурентами, чтобы выделить его преимущества и определить нишу, в которой оно может быть наиболее востребованным.

1.2.1. Описание приложения HashiCorp Vault

HashiCorp Vault — это комплексное, но гибкое приложение для хранения и управления секретами. Взаимодействие с ним осуществляется через веб-интерфейс, API или командную строку. HashiCorp Vault предназначено для безопасной работы с конфиденциальными данными, такими как учетные данные, ключи API, сертификаты и токены доступа. Приложение широко используется в корпоративной среде, обеспечивая централизованный контроль и защиту секретов.

Для работы с HashiCorp Vault пользователи могут зарегистрироваться и войти в систему через различные методы аутентификации. Поддерживаются интеграции с LDAP, OAuth (например, Keycloak), JWT [8], GitHub и другими провайдерами, что позволяет использовать существующую инфраструктуру безопасности. Доступ к хранилищу строго регулируется с помощью ролей и политик (RBAC), что позволяет гибко управлять правами пользователей и сервисов.

Внутри HashiCorp Vault пользователи могут создавать изолированные пространства (namespaces) для хранения секретов. Добавление и управление секретами происходит через веб-интерфейс, API или CLI, где можно задать параметры, такие как имя, значение, время жизни (TTL) и метаданные. HashiCorp Vault поддерживает автоматическую ротацию ключей, обеспечивая дополнительный уровень безопасности.

Доступ к секретам можно получить через API-запросы или интерфейс приложения. Однако, чтобы предотвратить несанкционированное использование, HashiCorp Vault позволяет выдавать временные токены, которые автоматически истекают через заданный промежуток времени. Политики доступа гибко настраиваются, позволяя ограничивать права пользователей на чтение, изменение или удаление данных.

Помимо базового хранения секретов, HashiCorp Vault предоставляет дополнительные функции, такие как динамическая выдача учетных данных. Это означает, что приложение может создавать временные пароли для баз данных или облачных сервисов, которые автоматически удаляются после использования. Также поддерживается встроенное шифрование и дешифрование данных, что позволяет безопасно передавать информацию между сервисами без хранения открытых ключей.

Для бизнеса HashiCorp Vault предлагает расширенные возможности, включая интеграцию с облачными платформами AWS, Azure и GCP. Организации могут развертывать приложение в режиме высокой доступности, распределяя нагрузку между несколькими узлами. Для дополнительной защиты можно использовать аппаратные модули безопасности (HSM) для хранения криптографических ключей.

Таким образом, HashiCorp Vault — это надежное решение для защиты секретов, обеспечивающее централизованное управление доступом и безопасность конфиденциальных данных. Оно подходит как для небольших команд, так и для крупных организаций, которым необходим высокий уровень контроля и защиты информации.

1.2.2. Описание приложения AWS Secrets Manager

AWS Secrets Manager — это облачный сервис для безопасного хранения и управления конфиденциальными данными, такими как пароли, ключи API, учетные данные для баз данных и другие секреты. Сервис интегрирован с экосистемой AWS и предоставляет удобный способ автоматизации ротации секретов, аутентификации и доступа к защищенным данным.

AWS Secrets Manager поддерживает несколько методов аутентификации, включая AWS Identity and Access Management [9] (IAM), что позволяет точно настраивать права доступа для пользователей и сервисов. С помощью IAM-политик администраторы могут контролировать, кто может создавать, просматривать, изменять и удалять секреты. Для дополнительной безопасности можно настроить многофакторную аутентификацию (MFA).

Пользователи могут создавать и управлять секретами через AWS Management Console, API или командную строку (AWS CLI). Каждый секрет включает такие параметры, как имя, значение, версии, а также опциональные теги для организации ресурсов. AWS Secrets Manager

автоматически шифрует данные с использованием AWS Key Management Service (KMS), обеспечивая защиту на уровне облачной инфраструктуры.

Получить доступ к секрету можно с помощью API-запросов или SDK, что позволяет легко интегрировать его с приложениями и сервисами. AWS Secrets Manager поддерживает автоматическую ротацию учетных данных для баз данных AWS, включая Amazon RDS, Aurora и Redshift. Это означает, что сервис может периодически изменять пароли без вмешательства пользователя, обновляя их в базах данных и в самом хранилище.

Дополнительно AWS Secrets Manager поддерживает возможность использования кросс-аккаунтного доступа, что полезно для организаций с несколькими AWS-аккаунтами. Это позволяет централизованно управлять секретами и безопасно предоставлять доступ разным командам или сервисам.

Таким образом, AWS Secrets Manager — это надежное облачное решение для управления конфиденциальными данными, обеспечивающее безопасность, автоматизацию и удобную интеграцию с сервисами AWS. Оно идеально подходит для организаций, которые хотят централизованно управлять секретами и минимизировать риски, связанные с утечками данных.

1.2.3. Описание приложения 1Password

1Password — это кроссплатформенное приложение для хранения и управления паролями, конфиденциальными данными и другими секретами. Оно предназначено как для индивидуального, так и для корпоративного использования, обеспечивая надежную защиту учетных данных с помощью сквозного шифрования. Приложение доступно на мобильных устройствах, компьютерах и в виде веб-версии, а также поддерживает интеграцию с браузерами.

Для использования 1Password пользователи создают учетную запись и проходят двухфакторную аутентификацию (2FA) для дополнительной защиты. Вход в систему возможен с помощью мастер-пароля и специального секретного ключа, который генерируется при регистрации и хранится только у пользователя. Организации могут управлять доступом сотрудников через админ-панель.

Внутри 1Password можно создавать безопасные хранилища (vaults), в которых хранятся пароли, кредитные карты, документы, лицензии и другие важные данные. Каждая запись содержит название, логин, пароль, URL-адрес, заметки и дополнительные поля. Все данные зашифрованы с помощью AES-256 и хранятся на серверах 1Password или локально, в зависимости от настроек пользователя.

Доступ к сохраненным данным осуществляется через приложение, браузерные расширения или API. 1Password автоматически заполняет пароли на сайтах и в приложениях, устранив

необходимость запоминания сложных комбинаций. Также есть функция генерации надежных паролей, которая помогает создавать уникальные учетные данные для каждого сервиса.

Приложение поддерживает функцию Watchtower, которая уведомляет пользователей о скомпрометированных паролях, утечках данных и устаревших паролях. Также предусмотрена возможность безопасного обмена учетными данными внутри команды или семьи через общие хранилища.

Для бизнеса 1Password предлагает централизованное управление учетными записями сотрудников, контроль доступа и интеграцию с корпоративными системами, такими как Azure AD, Okta и OneLogin. Администраторы могут настраивать политики безопасности, двухфакторную аутентификацию и мониторить активность пользователей.

Таким образом, 1Password — это простое и удобное решение для защиты конфиденциальной информации, обеспечивающее безопасность личных и корпоративных данных, удобный доступ и простоту управления секретами.

1.2.4. Описание приложения LastPass Enterprise

LastPass Enterprise [10] — это корпоративное решение для хранения, управления и безопасного обмена паролями внутри организаций. Оно позволяет сотрудникам удобно работать с учетными данными, минимизируя риски, связанные с утечками или слабыми паролями. LastPass Enterprise доступен как веб-приложение, desktop приложение, мобильное приложение и расширение для браузеров, что делает его удобным для использования на любых устройствах.

Система аутентификации LastPass Enterprise поддерживает вход через единый мастер-пароль, многофакторную аутентификацию (MFA) и интеграцию с провайдерами единого входа (SSO), такими как Azure AD, Okta и Google Workspace. Администраторы могут централизованно управлять доступом сотрудников, настраивать политики безопасности и контролировать действия в системе через панель управления.

Каждый пользователь получает личное зашифрованное хранилище (vault) для хранения паролей, секретных заметок и других конфиденциальных данных. Пароли можно организовывать в папки, а также делиться ими с коллегами, задавая уровни доступа (только просмотр или редактирование). Все данные зашифрованы с использованием алгоритма AES-256, а расшифровка происходит только на стороне пользователя, обеспечивая нулевое разглашение (Zero-Knowledge Security).

Доступ к паролям осуществляется через веб-интерфейс, мобильные приложения и расширения для браузеров, которые автоматически подставляют учетные данные на сайтах и в приложениях. Также есть встроенный генератор надежных паролей, который помогает создавать уникальные комбинации для каждого ресурса.

LastPass Enterprise предоставляет функции мониторинга безопасности, включая аудит паролей, выявление слабых и повторяющихся паролей, а также уведомления о скомпрометированных учетных данных. Инструмент Dark Web Monitoring анализирует утечки данных и предупреждает пользователей, если их пароли обнаружены в базах взломанных аккаунтов.

Для крупных организаций LastPass Enterprise предлагает детализированные политики доступа, отчеты об использовании и интеграцию с SIEM-системами. Также доступна возможность автоматического предоставления и отзыва доступа при изменении ролей сотрудников.

Таким образом, LastPass Enterprise — это надежное корпоративное решение для управления паролями, которое повышает безопасность организаций, снижает нагрузку на ИТ-отдел и обеспечивает удобный доступ сотрудников к их учетным данным.

1.2.5. Описание разрабатываемого решения

Веб-приложение для хранения корпоративной конфиденциальной информации — это приложение, предназначенное для безопасного управления конфиденциальными данными компаний, такими как SSH-ключи, токены доступа, сертификаты и пароли. Приложение ориентировано на корпоративное использование, обеспечивая строгий контроль доступа к секретам и защиту данных через ролевую модель управления и шифрование.

Приложение поддерживает систему учетных записей с авторизацией через Keycloak, что позволяет интегрировать его в корпоративную инфраструктуру безопасности. Гибкая настройка прав доступа позволяет разграничивать доступ к секретам в зависимости от роли пользователя и рабочего пространства.

Секреты хранятся в изолированных рабочих пространствах, к которым можно добавлять пользователей с различными уровнями прав. Создание, редактирование и удаление секретов происходит через веб-интерфейс, а также с помощью API. Встроенные механизмы логирования фиксируют все действия пользователей, обеспечивая полную прозрачность изменений.

Доступ к секретам осуществляется через веб-приложение и API, а уведомления о действиях с секретами могут отправляться через Telegram-бот. Бот также позволяет просматривать выбранные пользователем уведомления о событиях, что делает систему удобной для оперативного отслеживания изменений.

Приложение поддерживает автоматическое удаление секретов по истечении их срока действия. Для безопасности все данные хранятся в зашифрованном виде.

Для удобства использования веб-интерфейс разработан на React [11] с адаптивной версткой, а серверная часть реализована на Node.js и TypeScript, интеграция с Keycloak упрощает управление авторизацией.

Таким образом, веб-приложение для хранения корпоративных секретов предоставляет безопасную и гибкую платформу для управления конфиденциальной информацией в корпоративной среде, обеспечивая контроль, аудит и удобство работы с секретами.

1.3. Анализ существующих решений

В Таблице 1 представлено сравнение существующих решений и разрабатываемого сервиса.

Таблица 1 – Сравнение существующих и разрабатываемого решений

| Параметр | HashiCorp Vault | AWS Secrets Manager | 1Password | LastPass Enterprise | Предложенное решение |
|--|--|---------------------------------|--|----------------------------------|---|
| Способы аутентификации | LDAP, OAuth, GitHub, Keycloak, MFA | IAM (AWS), MFA | Мастер-пароль, 2FA | Мастер-пароль, MFA | Keycloak, MFA |
| Модель управления доступом | + | + | + | + | + |
| Где хранятся данные | Локально, в облаке | В облаке AWS | В облаке 1Password | В облаке LastPass | Локально |
| Шифрование | AES-256, TLS | AES-256, TLS | AES-256, сквозное шифрование | AES-256, Zero-Knowledge Security | AES-256 |
| Интеграция с внешними сервисами | Kubernetes, AWS, GCP, Azure | AWS Lambda, RDS, DynamoDB | Браузеры | Браузеры | Telegram-бот |
| Мобильное приложение | - | - | + | + | - |
| Автоматическая ротация секретов | Да, для баз данных и облачных сервисов | Да, для AWS-ресурсов | - | - | Да, настройка сроков действия секретов |
| Журналирование и аудит | Подробное ведение логов | CloudTrail | Watchtower (мониторинг утечек паролей) | Dark Web Monitoring, аудит | Логирование всех действий пользователей |
| Поддержка MFA | + | + | + | + | + |
| Доступ через API | Да, REST API [12] | Да, AWS SDK | - | - | Да, REST API |

| | | | | | |
|---|---|---|------------------------------------|---------------------------------|--------------------------------|
| Поддержка мобильных приложений | - | - | + | + | - |
| Стоимость | Open-source, платные корпоративные версии | Платная, зависит от количества секретов | Подписка для частных лиц и бизнеса | Подписка для бизнеса | Бесплатное, Open-source |
| Поддержка SSO | Да, с провайдерами OAuth и LDAP | Да, через IAM и AWS SSO | Да, с корпоративными аккаунтами | Да, с корпоративными аккаунтами | Да, через Keycloak |
| Возможность развёртывания on-premise | + | - | - | - | + |
| Поддержка командной работы | Да, с granular RBAC | Да, через IAM | Да, через общие хранилища | Да, через группы пользователей | Да, через рабочие пространства |
| Наличие техподдержки | Да, в платной версии | + | + | + | - |

Выводы по главе

В данной главе рассматривается предметная область и описываются проблемы, которые решает приложение для хранения корпоративной конфиденциальной информации. Даётся обзор проблемы с точки зрения бизнеса и его сотрудников.

Также производится обзор существующих решений и их функционала, а затем – обзор разрабатываемого решения в виде функциональных требований и сравнительный анализ между ними.

2. Глава 2. Проектирование хранилища

2.1. Пользовательские сценарии

В данном разделе содержатся пользовательские сценарии, которые описывают основные взаимодействия пользователей с системой, позволяя понять, как реализованы функции управления учетными записями, секретами и правами доступа. Основная цель веб-приложения – обеспечить надежное хранение и безопасный обмен конфиденциальными данными внутри корпоративной среды. Для удобства восприятия в раздел добавлена визуализация сценариев в виде диаграмм прецедентов, иллюстрирующих процессы аутентификации, работы с секретами и настройки доступов к ним.

Основой системы является учетная запись пользователя, которая обеспечивает доступ к функционалу приложения. Пользователи регистрируются в системе через внешнюю систему аутентификации Keycloak. Авторизация возможна как по логину и паролю, так и через SSO (Single Sign-On). После входа в систему пользователи могут управлять своими профилями, изменять настройки безопасности и настраивать многофакторную аутентификацию (MFA) для повышения уровня защиты данных.

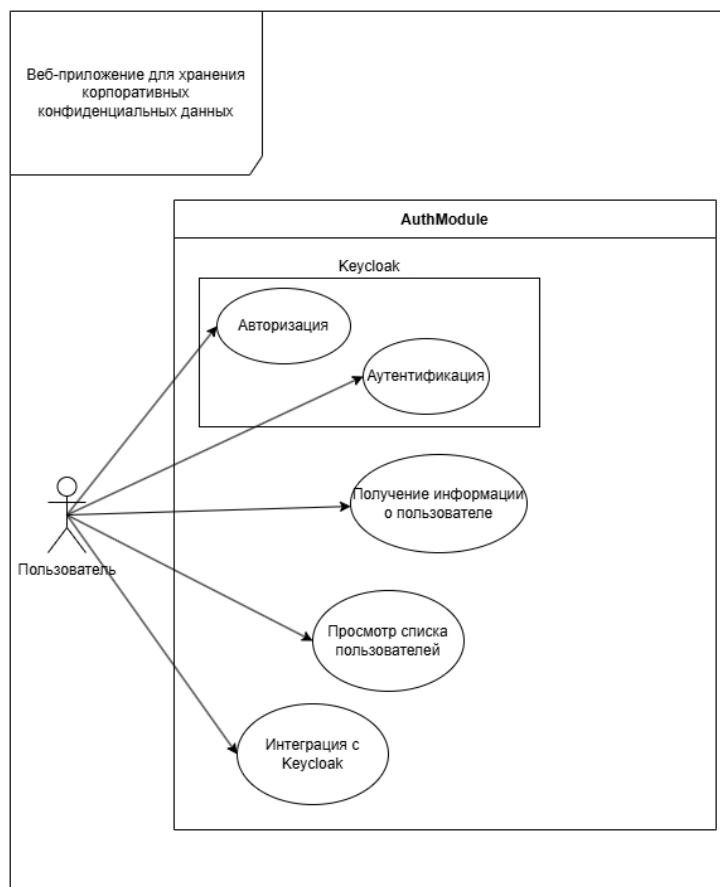


Рисунок 1 – Диаграмма прецедентов AuthModule

Приложение организует взаимодействие между пользователями через рабочие пространства. Его администратор может добавлять участников в пространство, назначая им определенные

роли и права. Например, одни пользователи могут только просматривать секреты, в то время как другие получают возможность их редактировать или удалять. При необходимости участники могут быть удалены из рабочего пространства, что автоматически закрывает им доступ ко всем связанным секретам.

Веб-интерфейс системы позволяет пользователям просматривать список участников рабочих пространств и управлять их правами. Такая гибкая модель доступа гарантирует, что конфиденциальные данные остаются в пределах установленных границ безопасности.

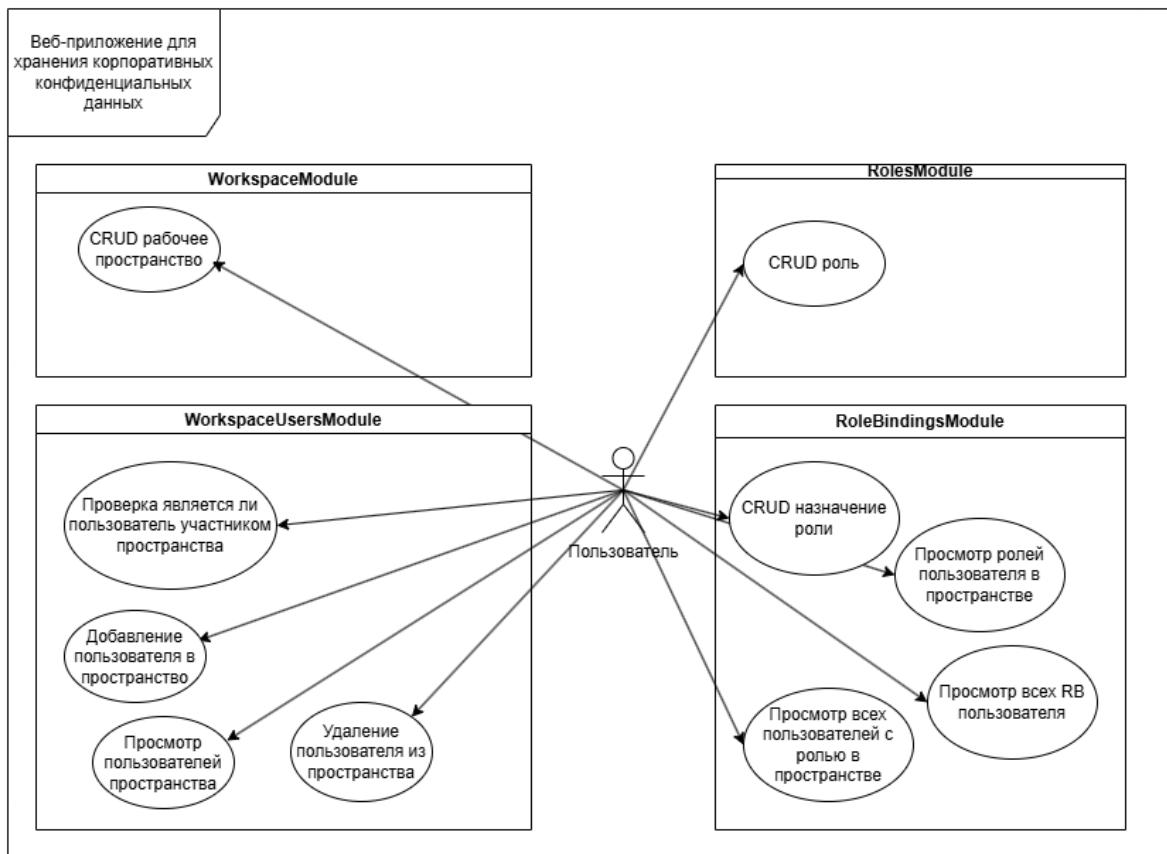


Рисунок 2 – Диаграмма прецедентов WorkspaceModule, WorkspaceUserModule, RolesModule, RoleBindingsModule

Ключевая функциональность системы сосредоточена вокруг управления секретами. Пользователи могут создавать записи с конфиденциальными данными, такими как SSH-ключи, API-токены, сертификаты и пароли. Каждому секрету можно задать уникальные параметры, включая срок действия и уровень доступа.

Редактирование и удаление секретов доступны только тем пользователям, у которых есть соответствующие права. Для удобства администраторы могут настраивать видимость секретов, определяя, кто может их просматривать и изменять. Это позволяет разделить доступ между различными командами внутри компании, предотвращая несанкционированный доступ к критически важным данным.

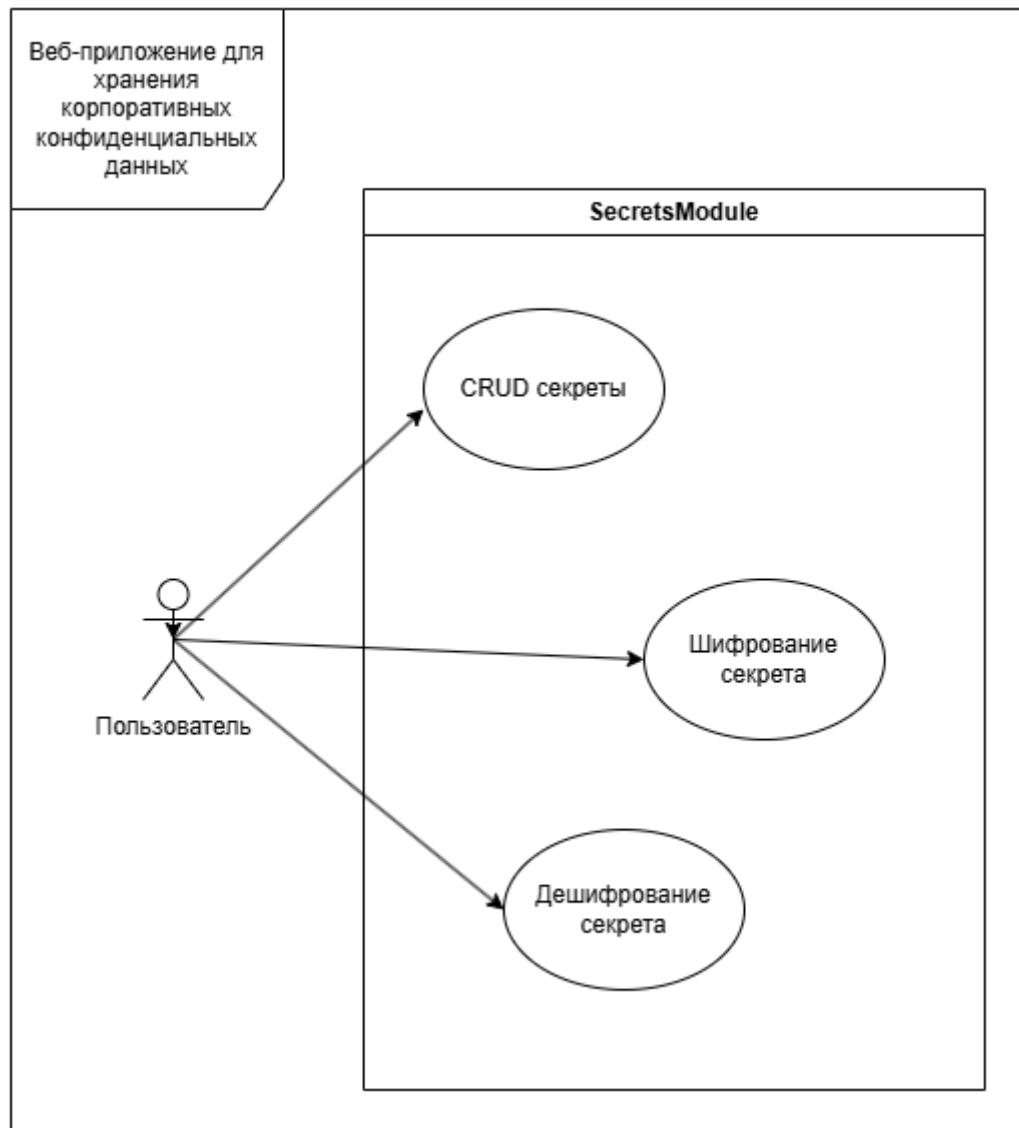


Рисунок 3 – Диаграмма прецедентов SecretsModule

Система также поддерживает интеграцию с внешними ресурсами. Пользователи могут экспортировать логи активности в текстовом формате для анализа, а уведомления о ключевых изменениях в секретах отправляются через Telegram-бот, что делает процесс мониторинга более удобным.

В отличие от платформ для хранения пользовательского контента, приложение не предусматривает публичного доступа к секретам. Однако внутри системы администраторы могут управлять шаблонами политик безопасности и настраивать рекомендации по конфигурациям доступа. Эти рекомендации доступны всем пользователям внутри организации и помогают выстраивать безопасную модель хранения секретов.

Приложение предоставляет автоматизированные инструменты для управления сроками действия секретов. Администраторы могут задавать политики автоматического обновления или удаления устаревших данных, что снижает риски хранения неактуальных учетных данных.

Система также ведет историю всех изменений, что позволяет пользователям отслеживать, кто и когда вносил правки в конфиденциальную информацию. Для неавторизованных пользователей работа с секретами недоступна, так как приложение требует входа для доступа к любым данным.

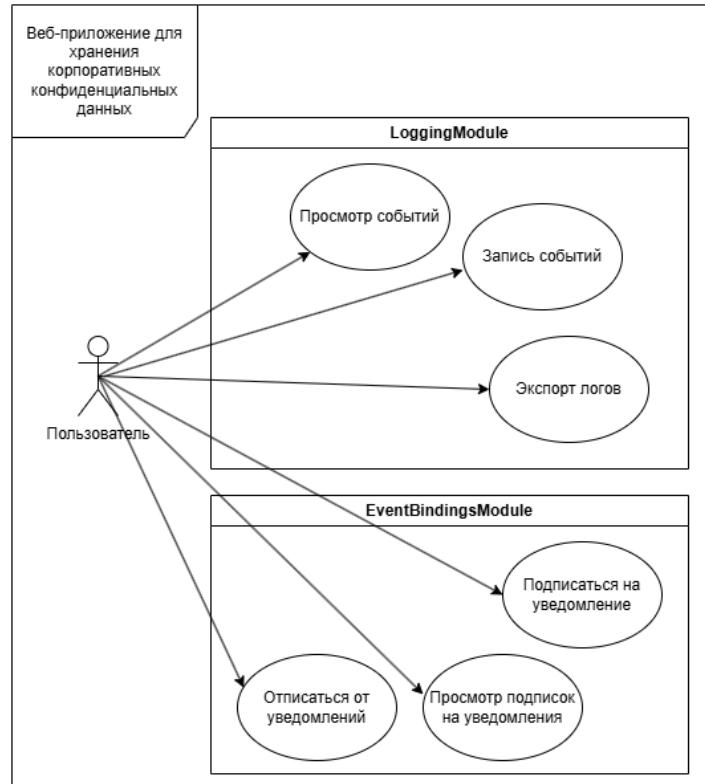


Рисунок 4 – Диаграмма прецедентов LoggingModule и EventBindingsModule

Для информирования пользователей о важных событиях реализована система уведомлений. Она позволяет получать сообщения о запросах на доступ, изменениях в секретах и системных предупреждениях, связанных с безопасностью.

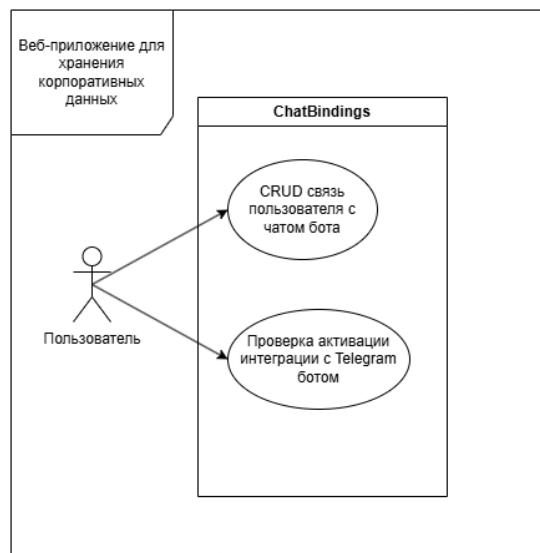


Рисунок 5 – Диаграмма прецедентов ChatBindingsModule

Уведомления отправляются в режиме реального времени через Telegram-бота. Пользователь может настроить типы событий, о которых он хочет получать оповещения, что делает систему более удобной и гибкой.

2.2. Архитектура приложения

Архитектура веб-приложения для хранения корпоративных конфиденциальных данных основана на современных принципах разработки, обеспечивающих безопасность, масштабируемость и гибкость системы. Для описания архитектурных решений используются визуальные инструменты, такие как UML [13] и C4-модели [14], которые помогают представить структуру компонентов, их взаимодействие и потоки данных. Основная цель этого раздела – объяснить устройство системы, ее логику и ключевые механизмы работы.

Приложение построено по трехслойной клиент-серверной архитектуре, включающей клиентскую часть, серверный слой с бизнес-логикой и базу данных. Клиентская часть представляет собой веб-приложение, разработанное на React с использованием TypeScript. Оно обеспечивает удобный интерфейс для управления секретами, рабочими пространствами и правами доступа. Серверная часть реализована на Node.js с использованием TypeScript и представляет собой REST API, отвечающее за обработку запросов клиентов, аутентификацию пользователей и управление данными. Вся информация хранится в реляционной базе данных PostgreSQL [15], где секреты, пользователи и рабочие пространства организованы в виде отдельных таблиц с четко определенными связями.

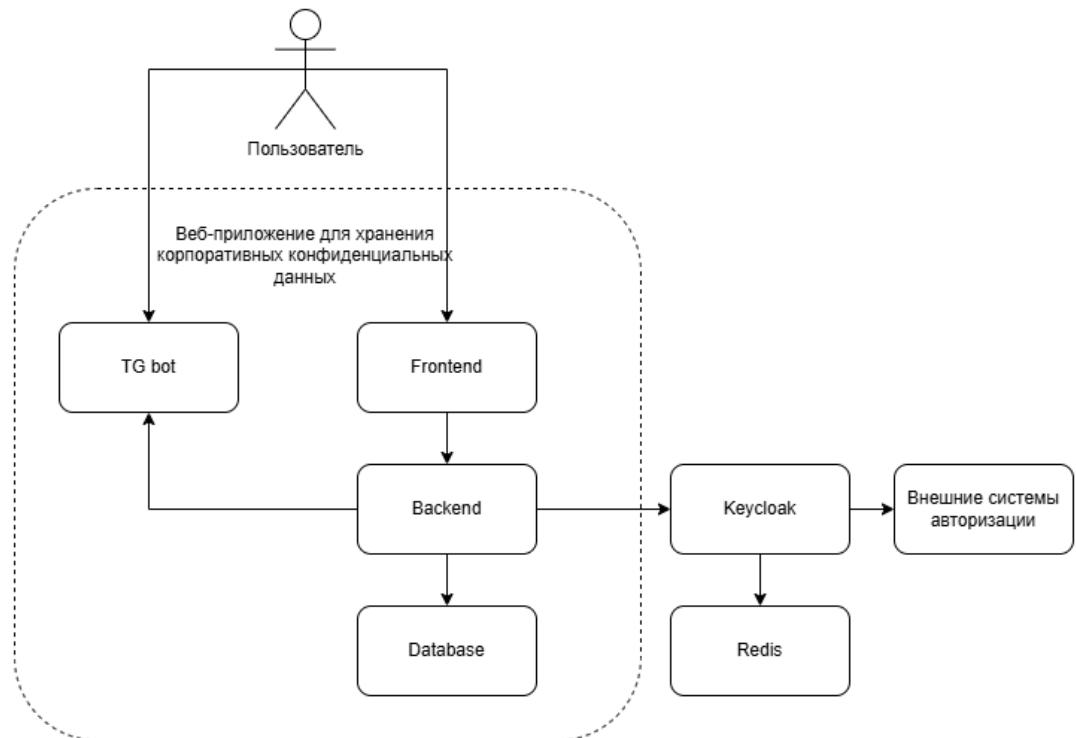


Рисунок 6 – Диаграмма С4 архитектуры приложения