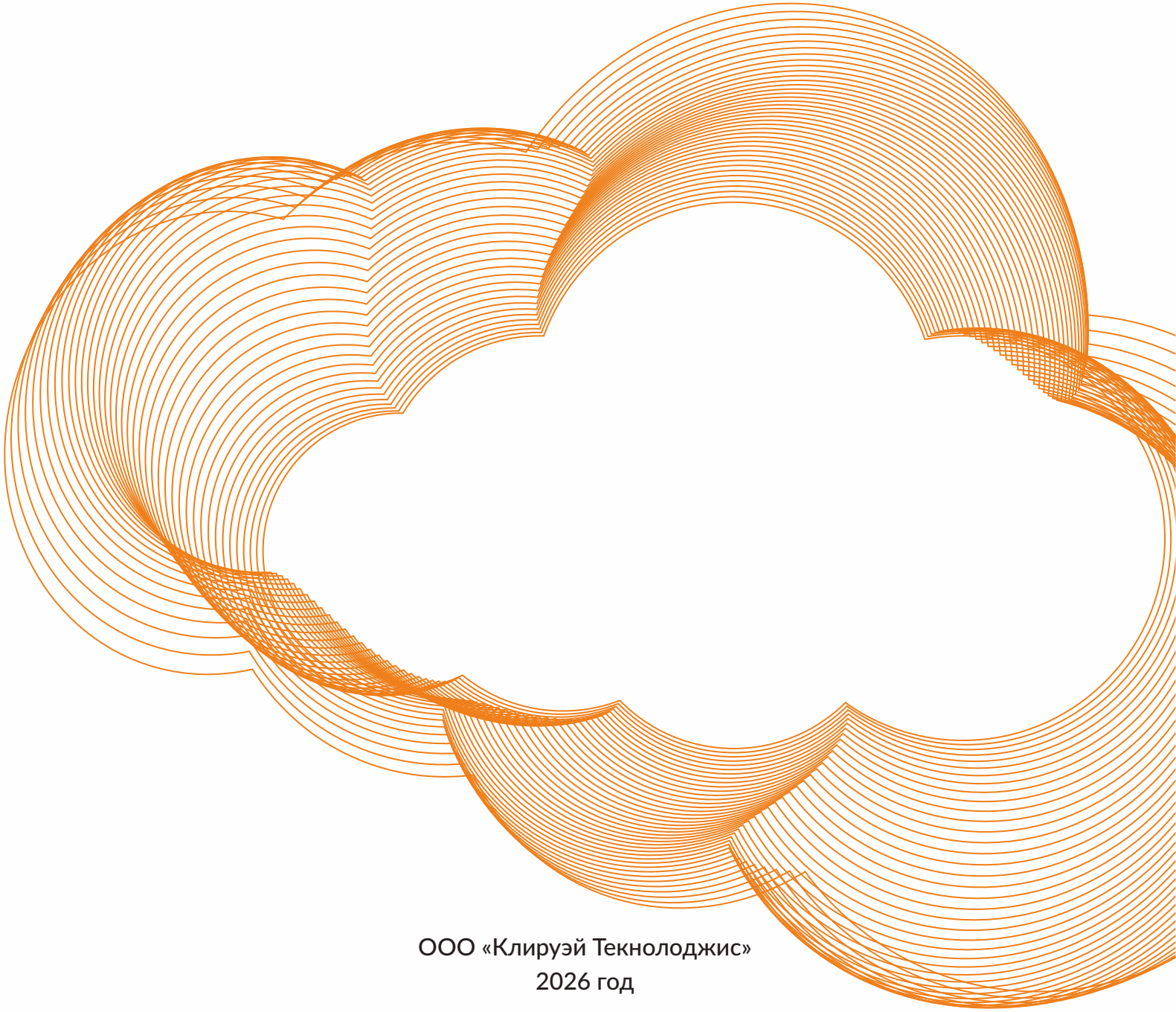
CLEARWAY INTEGRATION

EXC

Единое Хранилище Секретов



ООО «Клируэй Текнолоджис»
2026 год

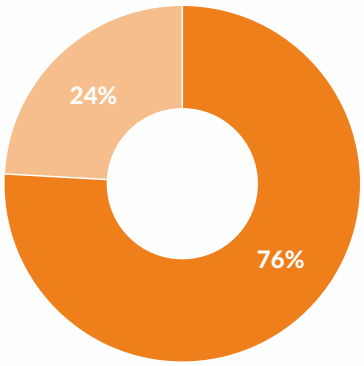
CLEARWAY INTEGRATION

Сегодня любая современная ИТ-инфраструктура держится на секретах: учетных данных, паролях доступа, ключах API, сертификатах и веб-токенах. Именно они обеспечивают непрерывность бизнес-процессов, встраиваясь в корпоративные приложения и сервисы.

С массовым переходом приложений на платформы контейнерной оркестрации, такие как Kubernetes, количество секретов в организациях резко возрастает. А традиционный подход к хранению конфиденциальных данных в конфигурационных файлах и кодовой базе становится чрезмерно трудоёмким и многократно повышает риски информационной безопасности. Все это приводит к ежегодным масштабным утечкам и многомиллионным убыткам. Управлять подобной инфраструктурой вручную уже невозможно — требуется безопасная автоматизация.

Автоматизированное решение для управления секретами впервые предложила компания HashiCorp. Однако из-за санкционных ограничений зарубежные продукты недоступны на российском рынке, а отечественный сегмент подобных решений находится в стадии формирования.

Именно поэтому мы создали **EXC** — Единое Хранилище Секретов, централизованное отечественное решение для управления всеми типами чувствительных данных: учетными записями, паролями доступа, ключами API, сертификатами, веб-токенами и SSH-сертификатами.



Атаки на корпоративную инфраструктуру в 2025 году

Ключевые проблемы: слабые пароли, статические секреты, секреты в репозиториях и CI/CD пайплайнах.

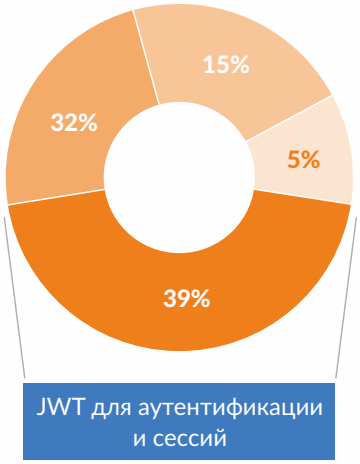
Исследования показали: в среднем свыше 50% статических ключей клиентов не обновлялись более года, а в ряде российских корпораций эта доля достигает 90%.

- Нацелены на базы данных
- Другие типы хранилищ

Утечки секретов

Большинство секретов, обнаруженных сканерами в репозиториях в 2025 году, приходилось на инфраструктуру веб-приложений (39%) и CI/CD (32%). Далее шла облачная инфраструктура (15%) и базы данных (5%). Среди раскрытых секретов инфраструктуры веб-приложений **66% составляли JWT для аутентификации и сессий**.

- CI/CD
- Облачная инфоструктура
- Базы данных
- Инфраструктура веб-приложений



*Источник: отчеты Yandex Cloud & Yandex Infrastructure и Verizon DBIR 2025

EXC превращает бессистемное хранение секретов в централизованную и автоматизированную систему, которая минимизирует риски утечек и потери секретов, сокращает операционные затраты и повышает общую надежность и безопасность инфраструктуры.

Преимущества:

- Интеграция с программно-аппаратным модулем безопасности КриптоПро HSM для хранения мастер-ключа EXC;
- Шифрование базы данных с использованием отечественных алгоритмов ГОСТ Р 34.12-2015 посредством использования библиотеки Astra Linux и интеграции с КриптоПро CSP
- Управление жизненным циклом сертификатов при интеграции с ЦУГИ Clearway CA и ЦУГИ ЕСАУС с поддержкой версионирования:
  - Хранение прошлых версий сертификатов для восстановления данных;
  - Выпуск будущих версий сертификатов для предоставления потребителям при недоступности ЦС.
- Наличие локального кошелька пользовательских секретов (Wallet) для хранения и синхронизации секретов с EXC.

EXC решает все ключевые задачи управления секретами:

Централизованное безопасное хранение секретов
Все секреты хранятся в одном месте и зашифрованы с возможностью использования алгоритмов шифрования ГОСТ

Разграничение доступа к секретам и операциям
В EXC реализована ролевая модель доступа (RBAC) с возможностью применения гибких ACL политик

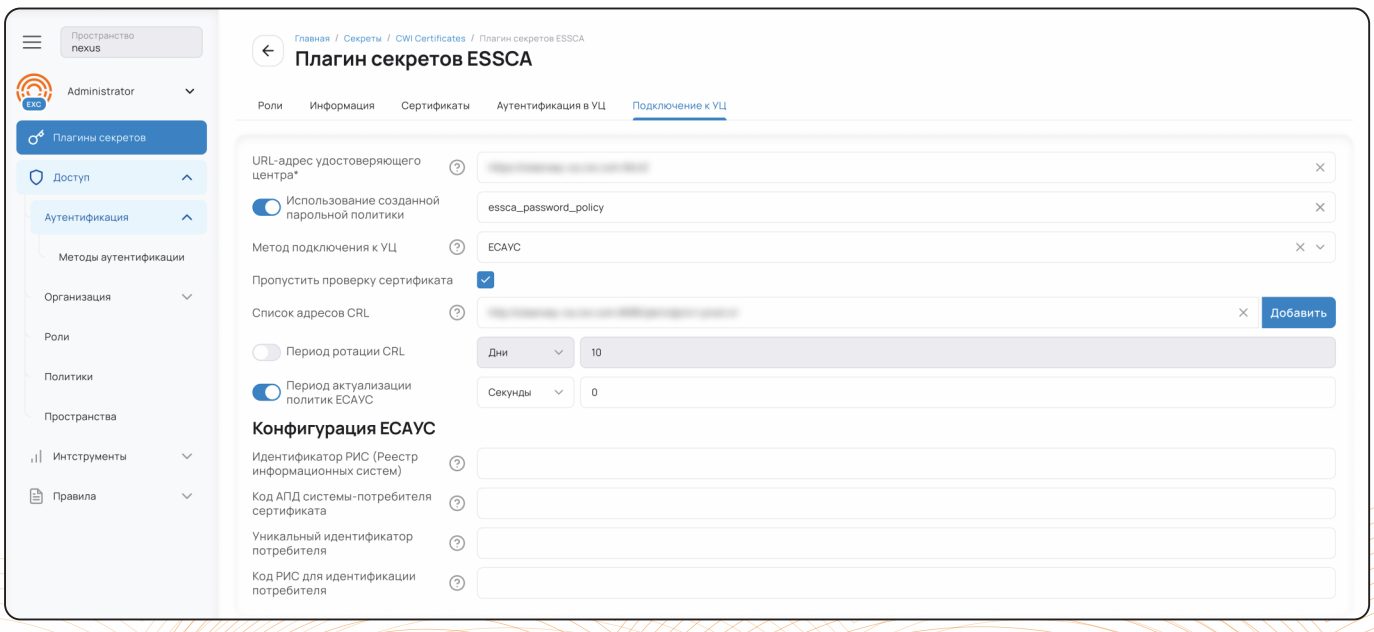
Автоматизация управления жизненным циклом секретов
Автоматическая ротация статических секретов, динамическая генерация и отзыв временных секретов

Доставка секретов до потребителей
EXC обеспечивает доставку секретов на аппаратные и виртуальные сервера, а также в среды контейнерной оркестрации Kubernetes. Для доставки секретов на АРМ пользователей реализован пользовательский кошелек Wallet с возможностью локального кеширования секретов.

Логирование и аудит всех операций
Полное логирование всех событий жизненного цикла секретов и действий пользователей

Получите консультацию по продукту

+7 495 142 13 15
info@clearwayintegration.com
clearway.ru



EXC Wallet
Локальное приложение для безопасной доставки и хранения секретов, предоставленных сотрудникам компании на АРМ, с возможностью автоподставновки в Web-формы и в pipeline Bash команд. Локальный кэш секретов позволяет предоставить временный доступ к секретам в случае отсутствия связи с EXC.

Сценарии использования

Импортозамещение HashiCorp Vault отечественным решением

С 2022 года компании, работающие с Vault от HashiCorp, утратили возможность обновлять и лицензировать данное решение. Дополнительное ограничение — несоответствие зарубежных продуктов HashiCorp требованиям регуляторов в сфере информационной безопасности. Перед отечественными компаниями встаёт задача импортозамещения, оперативной трансформации программной инфраструктуры и внедрения адаптивных средств защиты информации.

EXC обеспечивает бесшовный переход на отечественное решение: полная совместимость с API HashiCorp Vault вплоть до версии 1.14.8 и встроенный модуль миграции позволяют перенести данные из действующих инсталляций Vault без прерывания бизнес-процессов.

Автоматизированное управление большим объёмом секретов

Масштабирование корпоративной инфраструктуры — рост числа приложений, контейнеризация, мультиоблачные среды – заставляют формировать индивидуальный подход к управлению различными типами секретов.
Ручное управление большим количеством секретов в таких условиях неизбежно порождает человеческие ошибки и нарушения регуляторных требований.

EXC автоматизирует управление любым типом секретов и обеспечивает их своевременную актуализацию.
Это исключает риски неактуальных секретов минимизирует вероятность простоя сервисов.

Локальный менеджер секретов Wallet

Сотрудники компании ежедневно используют большое количество секретов для доступа к цифровым сервисам: CRM, внутренние порталы, различные базы данных. Отсутствие единой системы хранения приводит к записи паролей в заметках на телефоне, в текстовых файлах на рабочем столе или на стикерах, приклеенных к монитору.
Процесс онбординга новых сотрудников и отзыва доступов при увольнении становится хаотичным, уволенные сотрудники нередко сохраняют доступ к корпоративным ресурсам, что создаёт прямую угрозу утечки данных.

Wallet EXC полностью решает эти проблемы, предоставляя единое зашифрованное хранилище секретов доступных сотруднику компании, устраняет парольный хаос и предотвращает утечки данных, включая риски, связанные с «мёртвыми душами» и фишинговыми атаками.

Инструменты по доставке секретов EXC

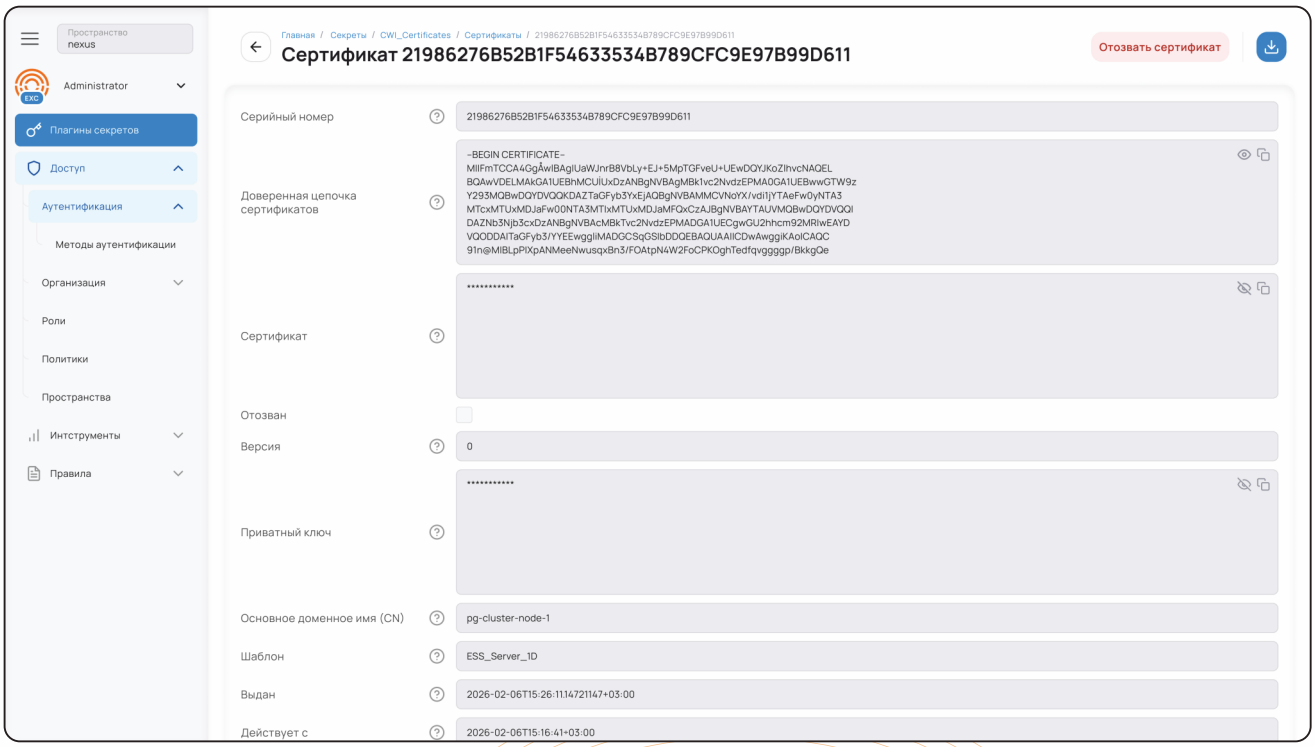
EXC предоставляет обширный набор инструментов для доставки секретов до конечных потребителей как на аппаратные, виртуальные сервера и АРМ пользователей так и в среду Kubernetes:

- **API**
  Полностью совместимое с API HashiCorp Vault версии 1.14.8 и ниже
- **SDK**
  Клиентские библиотеки для ключевых языков программирования: Go, C#, Java, Python и Node.js, позволяющие легко и безопасно внедрять управление секретами напрямую в код приложений
- **Легковесный Агент EXC**
  Приложение, реализующее доставку секретов в файлы конфигурации и переменные окружения приложений. Агент EXC также обеспечивает доставку секретов до legacy-систем и позволяет передавать секреты в параметры запуска приложений. Помимо доставки секретов Агент реализует graceful-ротацию, что позволяет пользовательским приложениям считывать обновлённые секреты без простоя сервисов
- **EXC Инжектор + Sidecar Агент EXC**
  Доставка секретов EXC в Kubernetes Pods пользовательских приложений с помощью инжектирования Sidecar-контейнера Агента EXC. Поддержка Init-контейнера для доставки нулевого секрета
- **EXC Оператор**
  Специализированный оператор для синхронизации секретов EXC и секретов Kubernetes
- **EXC Wallet**
  Приложение, реализующее доставку секретов на АРМ пользователей с возможностью локального кеширования секретов.

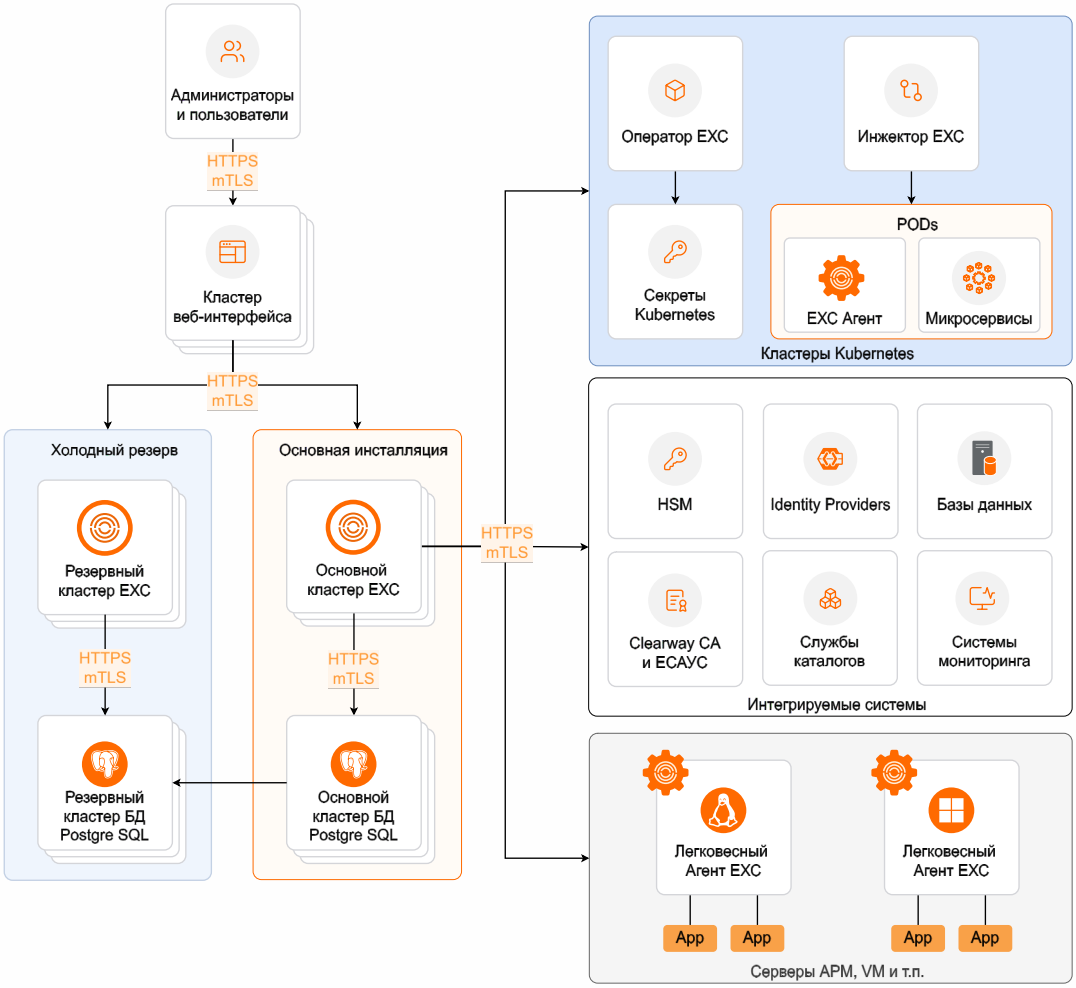
Архитектура системы

EXC реализован по модульной архитектуре: это позволяет адаптировать существующие компонент под меняющиеся требования и оперативно развёртывать новые функциональные блоки:

- **Ядро системы EXC**
  Основной компонент, который выполняет задачи шифрования, расшифровки данных и записи в хранилище;
- **Хранилище данных**
  База данных для хранения всей информации EXC. Поддерживаются PostgreSQL и Raft;
- **Веб-интерфейс**
  Реализует графический веб-интерфейс для управления EXC. Упрощает настройку методов аутентификации и управления жизненным циклом секретов;
- **Модули аутентификации**
  Поддержка различных типов аутентификации: Token, AppRole, Username&Password, JWT/OIDC, Kubernetes, LDAP/AD, Kerberos, RADIUS, SSL/TLS сертификаты. Поддержка двухфакторной аутентификации;
- **Модуль авторизации**
  Реализация ролевой модели доступа (RBAC), а также поддержка назначения гибких ACL политик доступа к секретам и действиям в системе;
- **Модули управления секретами**
  Управление жизненным циклом различных типов секретов: секреты в формате ключ-значение, учётные записи LDAP/AD и баз данных, SSL/TLS и SSH сертификаты, токены, сервисные аккаунты и роли Kubernetes, учётные записи RabbitMQ, одноразовые пароли TOTP;
- **Модуль журналирования и аудита**
  Логирование всех действий пользователей и системы с возможностью отправки событий по протоколу Syslog во внешние системы, включая отечественные решения класса SIEM;
- **Модуль мониторинга**
  Сбор метрик о состоянии системы EXC. Интеграция с различными системами мониторинга, например, Prometheus, Loki.



Интерфейс получения сертификата в EXC



Надёжность и масштабирование EXC:

Горячий резерв. Система представляет из себя кластер, состоящий из единственной master node и множества replica node. В случае отказа master node одна из replica node автоматически становится master;

Консистентность. Внесение изменений в хранилище секретов осуществляется только на master node, после чего, эти изменения автоматически реплицируются на replica node;

Горизонтальное масштабирование. Узлы replica node могут быть переведены в режим performance, за счет чего распределяют нагрузку интенсивного чтения базы EXC. В случае роста нагрузки новые replica node могут быть добавлены без прерывания работы кластера;

Холодный резерв. Еще один кластер в режиме ожидания, готовый быстро заменить основной при сбое или аварии.

Безопасность EXC:

Защищённые соединения. Передача данных защищена протоколом TLS 1.3 с поддержкой mTLS между всеми компонентами EXC и потребителями секретов:

- EXC и Легковесным EXC Агентом;
- Узлами кластера EXC;
- EXC и базой данных;
- EXC и потребителями секретов (если поддерживается потребителями).

Безопасное хранение секретов. Все данные EXC хранятся в зашифрованном виде;

Поддержка HSM. EXC поддерживает интеграцию с программно-аппаратными модулями безопасности КриптоПро HSM для хранения мастер-ключа в сертифицированном защищённом окружении;

Шифрование ГОСТ. EXC реализует шифрование базы данных с использованием отечественных алгоритмов ГОСТ Р 34.12-2015 посредством использования библиотеки Astra Linux и интеграции с КриптоПро CSP, что существенно повышает соответствие требованиям ФСТЭК, ФСБ и 152-ФЗ.

Интеграция с другими продуктами ЦУГИ

EXC является частью платформы **ЦУГИ** и предоставляет дополнительные возможности при интеграции с другими продуктами Clearway Integration.

При интеграции с Единой Системой Автоматического Управления Сертификатами (ЕСАУС) и Clearway CA реализует управление жизненным циклом сертификатов с поддержкой версионирования:

- Хранение прошлых версий сертификатов и создание будущих версий сертификатов обеспечивает отказоустойчивость Kubernetes Pods при выходе из строя Центра Сертификации;
- Проверка статуса сертификата может выполняться как на основании CRL, так и по протоколу OCSP.

Clearway CA
Интеграция с Clearway CA позволяет выпускать сертификаты с использованием внешнего центра сертификации Clearway CA и посредством взаимодействия с Драйвером УЦ обеспечивает поддержку других ЦС, таких как Microsoft CA, КриптоПро УЦ, SafeTech CA и Aladdin Enterprise CA.

ЕСАУС
При обращении EXC напрямую к встроенному или внешнему ЦС производится валидация следующих параметров запроса на получение сертификата:

- Common Name
- Subject
- Subject Alternative Names

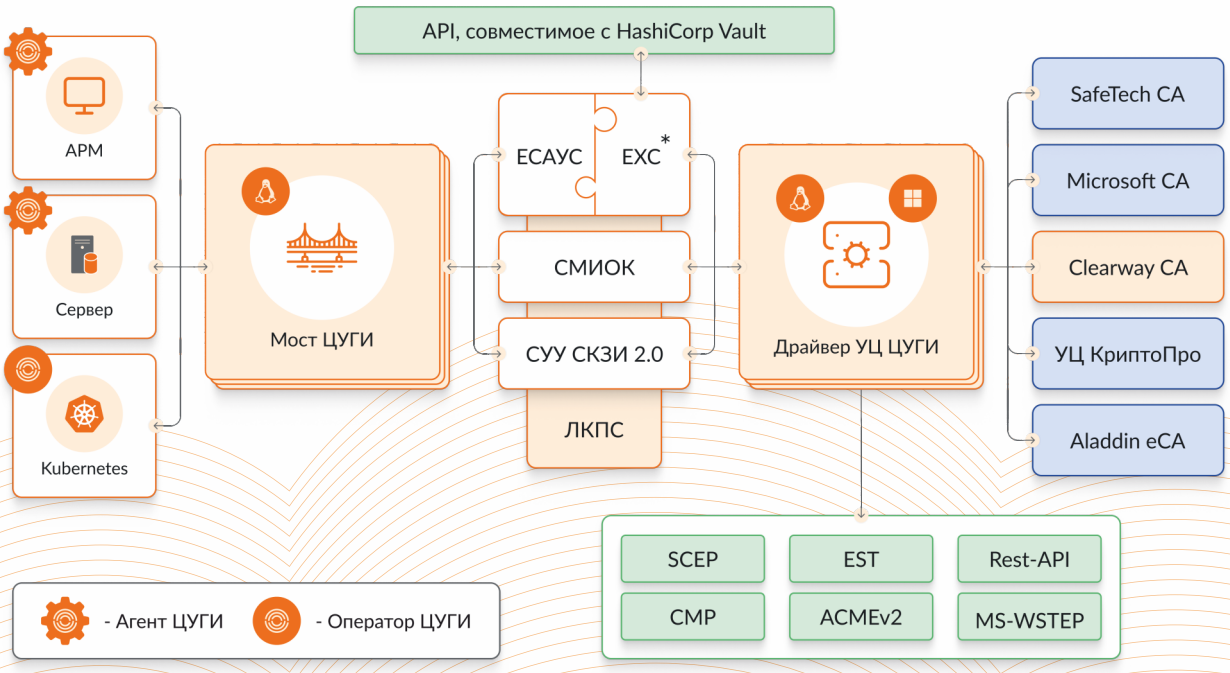
При интеграции с ЕСАУС запросы от EXC к Clearway CA отправляются через ЕСАУС, обеспечивая проверку не только параметров запроса, но и дополнительной информации, полученной от EXC:

- учетной записи EXC для аутентификации в ЕСАУС
- политики выпуска сертификата
- ключевой пары поставщика сертификатов

ЛКПС
Благодаря интеграции EXC с Личным Кабинетом Пользователя Сертификатов (ЛКПС) каждый пользователь секретов может отследить фактическое размещение всех своих секретов в ЛКПС, а также назначить ответственного для каждого секрета.

Продукты ЦУГИ дополняют друг друга, обеспечивая синергетический эффект всей платформы, минимизируя риски при управлении секретами и улучшая пользовательский опыт в гетерогенных средах.

Экосистема корпоративной инфраструктуры PKI Clearway Integration



*Единое хранилище секретов, российский аналог Hashicorp Vault от Clearway Integration

Функция	EXC	ECAУС
Управление SSL/TLS сертификатами		
Работа с различными ЦС через Драйвер ЦС	✓	✓
Генерация ключевой пары и CSR на стороне клиента	✗	✓
Генерация ключевой пары и CSR на стороне системы	✓	✗
Поддержка клиентов с неизвлекаемым приватным ключом	✗	✓
Доставка сертификатов в Kubernetes Secrets	✓	✓
Доставка сертификатов в Kubernetes Pods	✓	✗
Сбор информации о сертификатах в Kubernetes Secrets в формате Prometheus с возможностью отправки во внешние системы	✗	✓
Выпуск сертификатов через ECAУС	✓	n/a
Графический интерфейс выпуска сертификатов	✓	✗
Хранение предыдущих версий сертификатов для предоставления	✓	✗
Выпуск будущих версий сертификатов для предоставления при выходе из строя ЦС	✓	✗
Механизм ручного утверждения индивидуальных запросов на выпуск сертификата	✗	✓ (2026)
Механизм утверждения политик автоматического выпуска сертификата	✗	✓
Предоставление списка сертификатов с указанием шаблонов выпуска	✗	✓
Инвентаризация шаблонов сертификатов на ЦС	✗	✓ (2026)
Актуализация и распространение списков сертификатов доверенных корневых и промежуточных ЦС	✗	✓
Управление SSH ключами		
Инвентаризация и анализ SSH-ключей для выявления несоответствия требованиям ИБ	✗	✓
Автоматизированный выпуск и ротация SSH-ключей по заданным политикам	✗	✓
Управление другими типами секретов		
Управление секретами типа ключ-значение	✓	✗
Управление учетными записями служб каталогов LDAP/AD	✓	✗
Управление учетными записями баз данных	✓	✗
Управление учетными записями RabbitMQ	✓	✗
Управление одноразовыми паролями TOTP	✓	✗
Управление сервисными аккаунтами и ролями Kubernetes	✓	✗
Управление SSH сертификатами	✓	✓ (2026)

clearway.ru

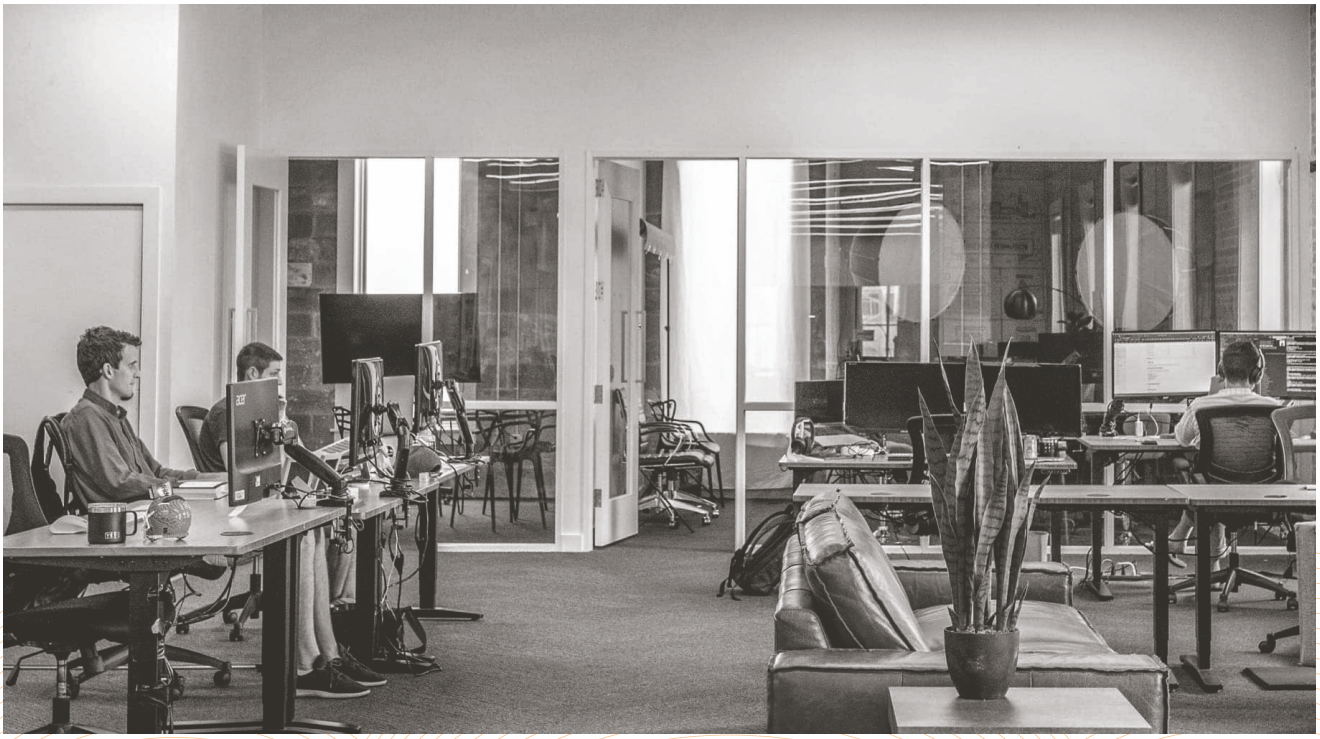
info@clearwayintegration.com

Clearway Integration - разработчик ПО для централизованного и автоматизированного управления ИТ-инфраструктурой бизнеса.

Наша линейка продуктов разрабатывается на базе единой платформы Централизованного Управления Гетерогенными Инфраструктурами (включена в Реестр Отечественного ПО с 21 марта 2022 года, №13033).

CLEARWAY
INTEGRATION

- Полностью российская разработка
- Импортозамещение линейки продуктов Microsoft Enterprise PKI
- Соответствие требованиям регуляторов
- 15+ лет опыта
- Круглосуточная техническая поддержка



CLEARWAY
INTEGRATION