CLEARWAY
INTEGRATION
Technology. Talent. Results.

Экосистема корпоративной инфраструктуры PKI

О НАС

>200 000 000
выпускается сертификатов в год

>4 000 000
сертификатов под мониторингом

>600 000
сертификатов выпущенных Clearway CA за три месяца

>110 000
установленных агентов

>300
серверов PKI под управлением и мониторингом

Мы создаем передовые решения и технологии, которые делают бизнес-процессы прозрачными и управляемыми, позволяют руководителям сосредоточиться на стратегических задачах, снижают нагрузку на IT-команды и повышают уровень информационной безопасности и устойчивости инфраструктуры.

Преимущества наших решений:

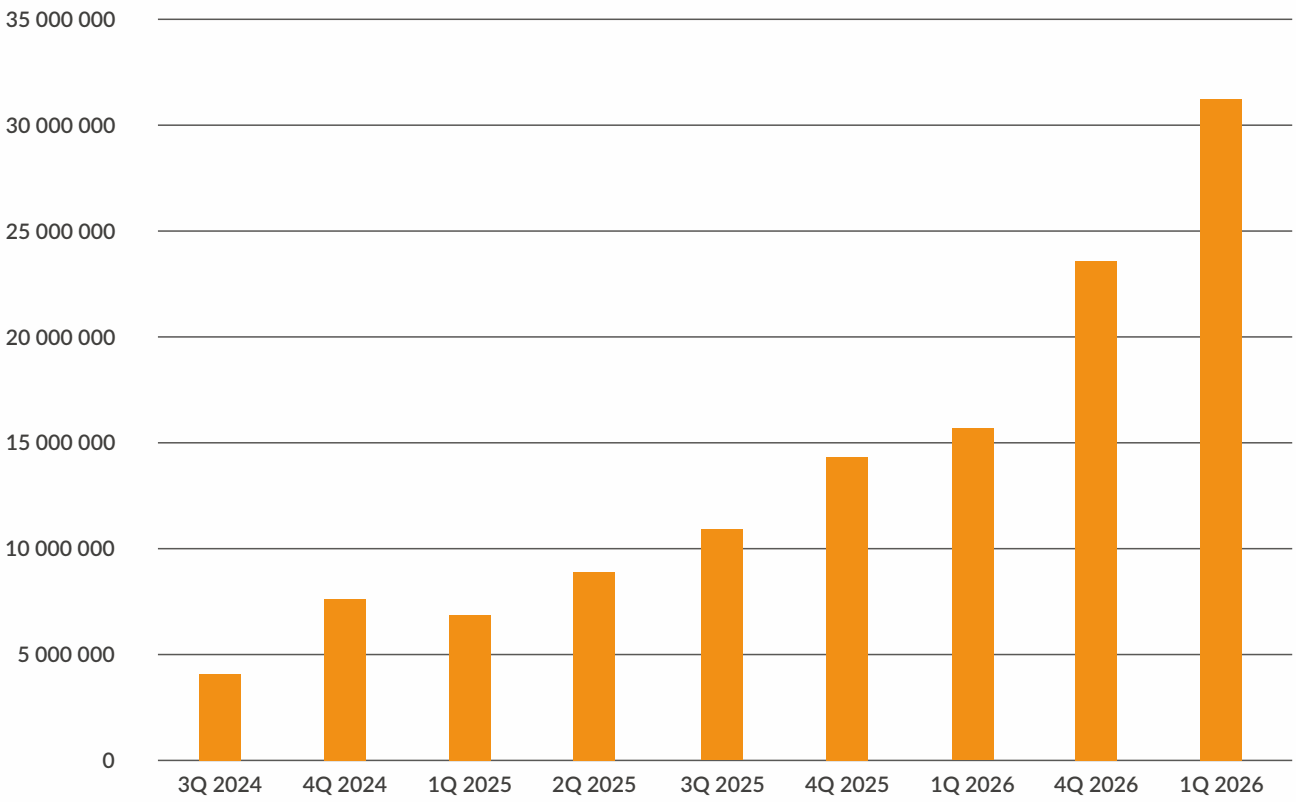
- Автоматизированный подход к управлению жизненным циклом технологических сертификатов SSL/TLS и сопровождении ИОК RSA;
- Комплексный и эффективный мониторинг Инфраструктуры Открытых Ключей и состояния сертификатов RSA и ГОСТ;
- Гибкие инструменты для централизованного управления и контроля выпуска сертификатов;
- Разработка простых и доступных решений для импортозамещения не только УЦ Microsoft CA, но и всего функционала, входящего в Microsoft Enterprise PKI;
- Удобный и многофункциональный личный кабинет для владельцев сертификатов, позволяющий отслеживать статус их сертификатов и контролировать непрерывность бизнес-процессов;
- Централизованное автоматизированное управление жизненным циклом всех типов секретов с возможностью их доставки и применения для информационных систем, серверов и рабочих станций.

Инфраструктура выросла. Управление - нет.

Ещё пять–восемь лет назад корпоративная PKI в среднем насчитывала несколько сотен сертификатов — один администратор с таблицей Excel успешно справлялся с задачей её администрирования. Сегодня компания аналогичного размера оперирует десятками тысяч сертификатов. На каждый микросервис, каждому пользователю и его рабочей станции, каждому API эндпоинту, каждому устройству в сети и даже каждому AI-агенту нужен свой сертификат. Концепция Zero Trust и связанное с ней широкое применение mTLS сделали сертификаты обязательным удостоверением для любого элемента IT-инфраструктуры без исключений.

Параллельно мы наблюдаем массовую тенденцию к существенному и планомерному сокращению сроков действия сертификатов, связанную с развитием квантовых технологий и с рисками компрометации классических асимметричных алгоритмов криптографии. В 2027 году максимальный срок действия публичных TLS-сертификатов составит 100 дней, к 2029-му сократится до 45-47 дней. В итоге организация с привычными сейчас 5 000 сертификатов будет вынуждена обрабатывать свыше 39 000 операций выпуска и продления в год.

Количество сертификатов, выпускаемых для крупной организации (реальная статистика Clearway Integration)



Это подтверждает наш собственный опыт: статистика последних трёх лет работы демонстрирует устойчивый рост количества клиентских запросов на выпуск сертификатов — в среднем в 4–6 раз ежегодно. Причём ещё до вступления в силу новых требований по сокращению сроков их действия.

Один просроченный сертификат. Последствия на месяцы вперёд.

По данным исследований рынка информационной безопасности, 79% компаний сталкивались с незапланированными сбоями из-за истёкших или неверно установленных сертификатов. Финансовые потери при этом лишь часть картины: остановка критичного сервиса даже на несколько часов бьёт по репутации и доходам компании сильнее любого штрафа.

компаний со сбоями

79%

из-за сертификатов

вендоров ушло с рынка

> 3

Entrust, DigiCert, Sectigo и другие

стоимость инцидента на один просроченный сертификат

15 млн. руб

в худшем случае

Российский рынок добавляет собственный контекст. В июне 2026 года GlobalSign и Let's Encrypt внесли изменения в условия обслуживания и начали целенаправленно отказывать в выпуске сертификатов для подсанкционных организаций. Для ряда компаний был начат процесс отзыва действующих сертификатов. Существует риск полного прекращения работы зарубежных ЦС с российскими компаниями. Организации, выстроившие процесс управления сертификатами вокруг инструментов этих ЦС, оказались перед непростым выбором: либо выстраивать всё заново, либо продолжать работу с нарастающими операционными рисками.

Для снижения рисков и защиты инфраструктуры от подобных инцидентов, предприятия переходят от ручного управления сертификатами к автоматизации. Именно запрос на автоматизацию лёг в основу экосистемы Clearway Integration: полный цикл управления PKI-инфраструктурой, разработанный в соответствии с реалиями российского рынка и требованиями регуляторов.

Каждый продукт в линейке закрывает конкретный участок этого цикла: от выпуска и доставки сертификатов RSA, ГОСТ и ECC до мониторинга и учёта СКЗИ.

Ниже представлена полная линейка продуктов Clearway Integration с детальным описанием каждого решения.

Линейка продуктов Clearway Integration предлагает полную автоматизацию процессов управления сертификатами:

СМИОК

Система Мониторинга Инфраструктуры Открытых Ключей (PKI).
Мониторинг работоспособности Инфраструктуры Открытых Ключей и контроль срока действия сертификатов. Встроенная детальная модель здоровья PKI-системы для глубокого анализа работоспособности PKI.

ЕСАУС

Единая Система Автоматического Управления Сертификатами.
Кроссплатформенный автоматический выпуск, доставка и установка пользовательских и технологических сертификатов на инфраструктуре АРМ, серверов и Kubernetes. Распространение и поддержание в актуальном состоянии списка доверенных сертификатов.

ЛКПС

Личный Кабинет Пользователя Сертификатов.
Личный кабинет для потребителей сертификатов с единым окном для поиска, анализа статистики применения, выпуска и обновления сертификатов.
Назначение и контроль ответственных за использование сертификатов.

СУУ СКЗИ 2.0

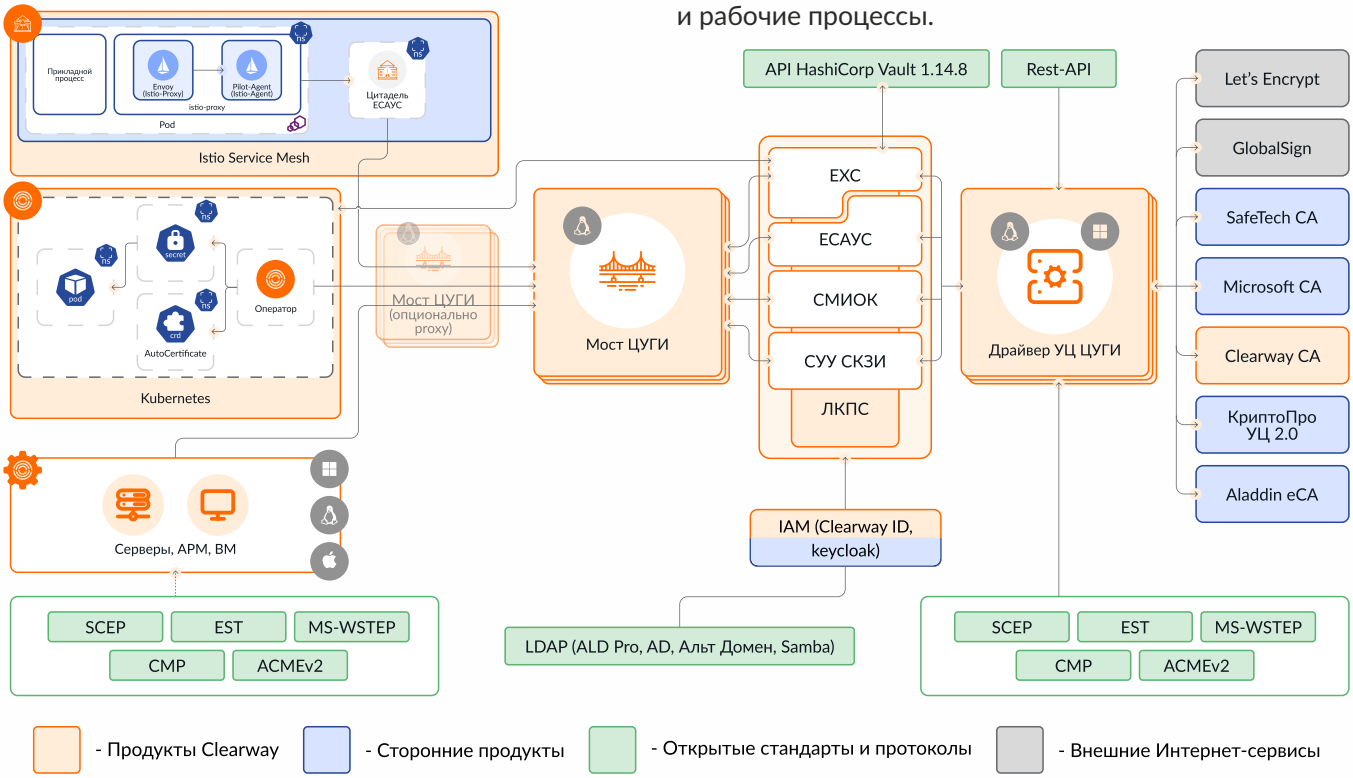
Система Учета и Управления Средствами Криптографической Защиты Информации 2.0.
Контроль жизненного цикла криптографических носителей, программных средств СКЗИ и ключевых документов. Инвентаризация и фиксация фактов их установки и использования.

Clearway CA

Центр сертификации, улучшенный отечественный аналог Microsoft CA на базе криптографического модуля OpenSSL.

EXC

Единое Хранилище Секретов.
Централизованное хранение и управление всеми типами чувствительных данных (секретами) с возможностью их доставки до конечных потребителей и внедрения в приложения и рабочие процессы.



Экосистема корпоративной инфраструктуры PKI и управления секретами Clearway Integration

Clearway CA

Является ядром Инфраструктуры Открытых Ключей (PKI) и обеспечивает поддержку всех необходимых функций по управлению сертификатами на различных типах ОС и контейнерных сред.

Clearway CA построен на микросервисной архитектуре и обеспечивает горизонтальное масштабирование и отказоустойчивую кластеризацию для высоконагруженных сред.

Clearway CA сохраняет высокий уровень производительности при выпуске до десятка миллионов сертификатов.

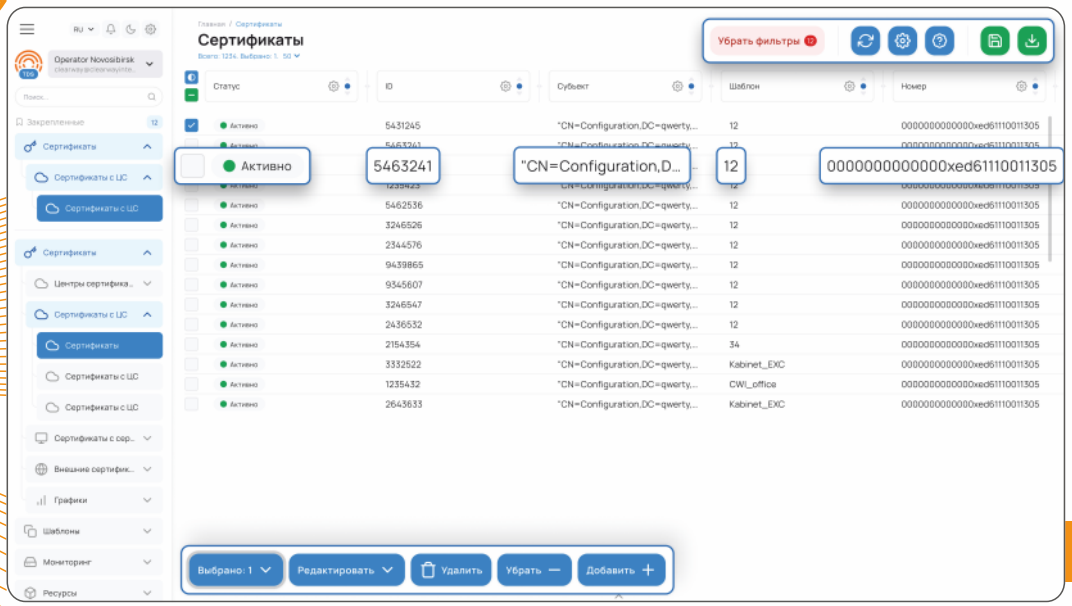
Центр сертификации Clearway CA является улучшенным аналогом Microsoft CA и идеально подходит для импортозамещения зарубежных решений. Clearway CA обеспечивает стабильный выпуск, отзыв и проверку сертификатов, гарантируя непрерывную и безопасную работу сервисов и приложений.

Clearway CA решает задачи управления большим количеством сертификатов. Построен на базе криптографического модуля OpenSSL, который входит в состав всех популярных дистрибутивов Linux, включая российские сертифицированные ОС.

Обеспечивает повышенный уровень безопасности инфраструктуры открытых ключей благодаря поддержке HSM, безопасным коммуникациям, подписи запросов сертификатов и ролевой модели разграничения доступа;

Обеспечивает широкую поддержку протоколов, стандартов безопасности и основных видов криптографии для инфраструктуры PKI;

Легко интегрируется с системами мониторинга и SIEM.



Clearway CA предоставляет следующие возможности:

1. Выпуск и управление сертификатами
Clearway CA обеспечивает автоматизированный выпуск, отзыв и проверку статуса большого количества сертификатов, обеспечивая непрерывную и безопасную работу сервисов и приложений.

2. Шаблоны сертификатов
Настройка шаблонов сертификатов осуществляется оператором ЦС через графический интерфейс.

3. Поддержка протоколов
Clearway CA поддерживает основные протоколы выпуска сертификатов: SCEP, EST, CMP, ACMEv2, MS-WSTEP. Работа по данным протоколам позволяет выпускать сертификаты для широкого спектра устройств и сетевого оборудования на разных операционных системах (Windows, Linux, MacOS, *nix-системы).

4. Адаптивность
Clearway CA использует криптографические модули OpenSSL или CryptoPro CSP. Это обеспечивает свободу выбора алгоритмов криптографии (RSA, ECDSA, ГОСТ) и форматов сертификатов (например, PEM, DER), позволяя адаптировать Clearway CA к решению различных задач безопасности.

5. Возможности интеграции
Clearway CA совместим с любым корпоративным PKI и легко интегрируется с другими продуктами на платформе ЦУГИ.

около 600 000
сертификатов за 3 месяца в проде

более 4 000 000
сертификатов за сутки в тесте

Ключевые преимущества:

- Признанный и популярный крипто-провайдер (OpenSSL в составе Astra и других версий Linux);
- Улучшенный и интуитивно понятный пользовательский интерфейс;
- Удобный интерфейс для работы из командной строки;
- Высокая производительность работы с миллионами сертификатов;
- Контекстный полнотекстовый поиск по сертификатам и их отдельным полям;
- Ролевая модель, журналирование, интеграция с системами мониторинга и SIEM;
- Гибкая система лицензирования по модулям и функциям системы;
- Поддержка шаблонов, открытый API и экспорт данных в xlsx. и csv.

СМИОК

Мониторинг, анализ и управление всеми ЦС и другими компонентами PKI из единого окна.

Предотвращение сбоев PKI за счет выявления предшествующих событий на основе «модели здоровья»

Предотвращение сбоев различных компонентов зависимой информационной инфраструктуры за счет мониторинга статуса всех сертификатов.

Система Мониторинга ИОК (СМИОК) разработана для автоматизации контроля и управления Инфраструктурой Открытых Ключей (PKI). Она позволяет не только отслеживать состояние ИОК, но и анализировать её использование в прикладных системах, обеспечивая прозрачность и эффективность применения PKI и сертификатов в организации.

Основные функции:

- Поддержка множества иерархий ЦС от разных производителей;
- Мониторинг устройств HSM;
- Отображение результатов мониторинга в виде диаграмм и таблиц, просмотр данных через статистику, графики и виджеты;
- Синтетический выпуск сертификатов для комплексной проверки работы всех компонентов;
- Автоматизация и трекинг рабочих задач администраторов и дежурной смены ЦС/PKI;
- Выпуск сертификатов по заявкам с одобрением и автоматически;
- Общий список сертификатов и шаблонов с различных ЦС с функцией контекстного поиска;
- Назначение ответственных за сертификаты для уведомлений, привязка другой дополнительной информации к сертификатам;
- Мониторинг как внутренних, так и внешних сертификатов с возможностью контроля отзыва всех сертификатов;
- Оценка рисков истечения срока действия выпущенных сертификатов и рисков некорректных настроек шаблонов сертификатов;
- Инвентаризация фактически установленных сертификатов на серверах;
- Карточки серверов для просмотра всех установленных сертификатов;
- Отправка уведомлений о проблемах и сбоях в PKI на почту, в Telegram и по SMS;
- Отправка событий во внешние системы мониторинга и системы сбора логов.

Функционал структурированного мониторинга:

- Возможность объединения объектов мониторинга в логические группы для более удобного контроля;
- Отдельный виртуальный объект, состояние которого зависит от всех входящих в него реальных объектов;
- Виртуальные объекты имеют полный функционал, включающий возможность добавления на визуальные диаграммы и подписку на оповещения об изменении состояния.

Лучшее решение для группы сопровождения PKI

СМИОК обеспечивает своевременное реагирование на события мониторинга и позволяют упростить эксплуатацию корпоративного PKI любого масштаба.

Модель здоровья, отточенная годами практического опыта

Готовая модель здоровья снизит затраты на настройку и запуск мониторинга вашей PKI;
Отправка уведомлений и событий во внешние системы мониторинга и системы сбора логов;
Настройка подписок на оповещения о состоянии объектов мониторинга, с поддержкой различных каналов доставки (электронная почта, СМС, Telegram).

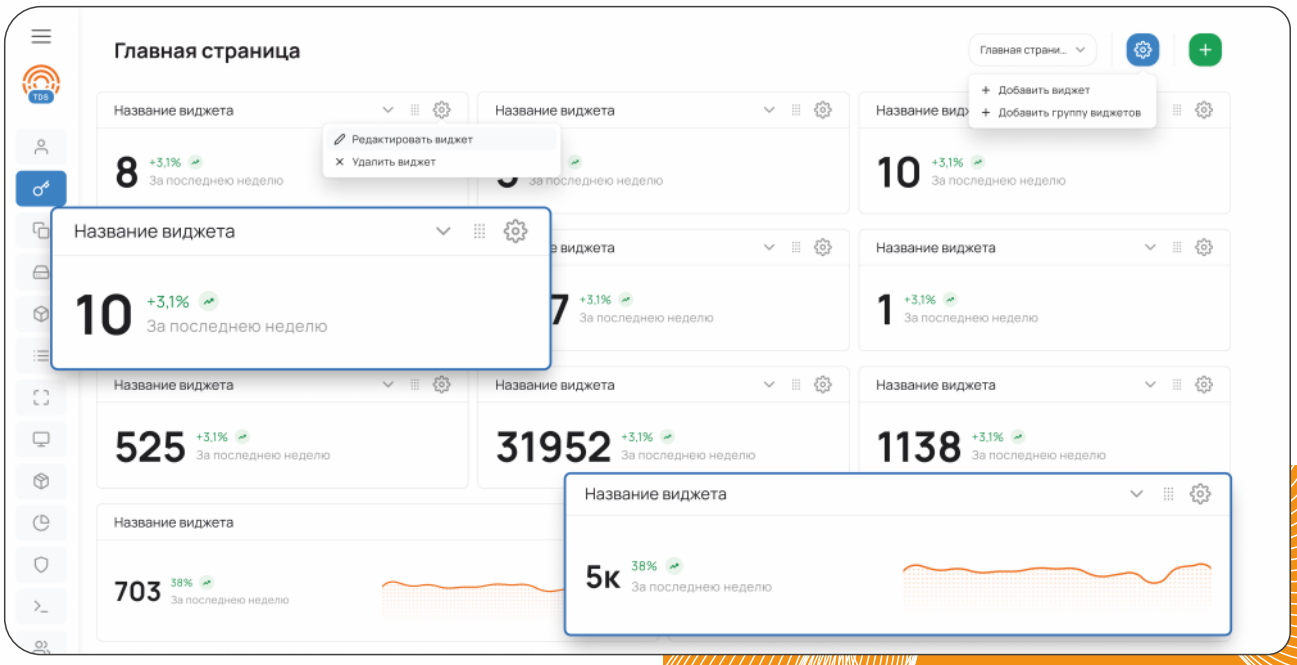
Возможности масштабирования решения

Эффективная работа с большим количеством сертификатов в едином справочнике;
Поддержка множества независимых иерархий PKI в рамках одной организации: технологические иерархии RSA, сертифицированные иерархии ГОСТ во всех сетевых сегментах;
Подробные отчеты и статистика по сертификатам и истории их выпуска.

Модель здоровья включает:

- Проверку состояния процессов ЦС в ОС сервера;
- Снятие счётчиков производительности ЦС;
- Анализ журналов событий ЦС;
- Проверку доступности и содержимого точек распространения CDP/AIA;
- Анализ ответов OCSP;
- Постоянный пробный выпуск тестового сертификата;
- Проверку совпадения сертификатов на разных путях CDP/AIA;
- Анализ состояния и работоспособности HSM (при наличии);
- Анализ шаблонов сертификатов в Microsoft Active Directory и в Clearway CA;
- Анализ выпущенных сертификатов на типовые риски и требования безопасности.

Механизмы сбора данных в СМИОК позволяют гибко настраивать и расширять процесс контроля состояния компонентов ИОК



ЕСАУС

Единая система автоматического управления сертификатами (ЕСАУС) – решение для комплексного управления жизненным циклом сертификатов и SSH-ключей. Оно обеспечивает надежную доставку, установку и своевременное обновление сертификатов в гетерогенной инфраструктуре . ЕСАУС построена на платформе ЦУГИ (№13033 в реестре отечественного ПО) из модульных компонентов.

>700
типов систем, подключенных к ЕСАУС

>40 000 000
сертификатов обрабатывается в год

до 10 000
сертификатов в минуту - пиковая производительность

ЕСАУС – это многоуровневая архитектура, разработанная специально для комфортной работы со сложными и сегментированными сетями:

- Принцип Zero Trust: специализированные агенты передают не только запрос на сертификат (CSR), но и сведения об окружении, в котором он был сформирован. Эта информация сверяется с утвержденными ИБ политиками выпуска сертификатов.
- Централизованный аудит: система ведёт полный журнал всех операций, включая сертификаты, которые УЦ обычно не регистрируют в своей базе.
- Архитектурные паттерны: постоянная взаимная проверка доступности компонентов; автоматическое восстановление подключения к компоненту после устранения сбоя; механизмы коммуникации между компонентами для управления пропускной способностью системы и др.

Автоматизация рутинных операций с сертификатами и SSH-ключами позволяет:

- Повысить уровень информационной безопасности;
- Уменьшить операционные и репутационные риски, связанные с компрометацией данных и простоями из-за неактуальных или неправильно установленных сертификатов;
- Сократить затраты благодаря экономии времени высококвалифицированных специалистов;
- Минимизировать влияние человеческого фактора.

Поддержка широкого спектра УЦ и миграция между ними:

Отечественные Clearway CA, КриптоПро УЦ 2.0 (в том числе, через КриптоПро PKI-кластер), SafeTech CA, Aladdin eCA. Зарубежный Microsoft CA. Запланирована поддержка Validata, VipNet, Notary-Pro, DigiSert, GlobalSign и Let`s Encrypt.

Преимущества

Балансировка нагрузки и легкая миграция между УЦ разных производителей с сохранением непрерывности работы и показателей надежности бизнес-процессов.

Проверка любого запроса сертификата (CSR) и окружения, где он был сформирован, на соответствие ряду требований ИБ. Требования задаются с помощью политик ЕСАУС.

Поддержка различных протоколов (DCOM, MS-WSTEP, ACMEv2, CMP, EST и др.), что обеспечивает совместимость с широким спектром устройств и упрощает интеграцию в разнородные ИТ-среды.

Вынос логики УЦ за пределы микросервисных платформ, возврат контроля за выпуском сертификатов службе информационной безопасности, разделение функций ИБ и администраторов Kubernetes/Istio.

Автоматическая настройка информационных систем для использования обновленных сертификатов:

Поддержка сложных сценариев, в том числе координированного обновления сертификатов в кластерах и в распределённых информационных системах

Возможность расширения сценариев выпуска и установки сертификатов за счёт поддержки скриптовых языков: Bash, Python, PowerShell

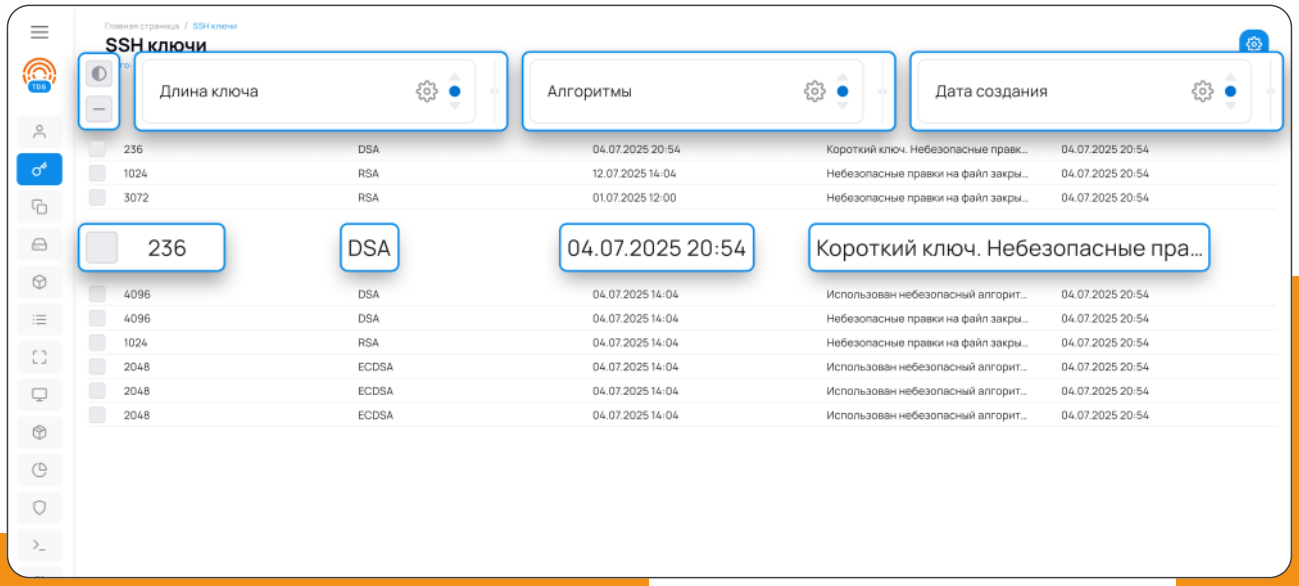
Актуализация и распространение списков доверенных корневых и промежуточных УЦ в рамках всей организации

Интеграция с корпоративными хранилищами секретов

Учёт технологических окон при обновлении сертификатов и SSH-ключей

Политики управления SSH-ключами:

- Инвентаризация: централизованный контроль SSH-ключей на хостах для выявления несоответствий требованиям ИБ (отсутствие passphrase, недостаточная длина ключа и другие параметры);
- Автоматизация: выпуск и ротация SSH-ключей по заданным политикам для исключения слабых параметров и обеспечения единых криптографических стандартов.



EXC

Единое Хранилище Секретов (EXC) предназначен для комплексного управления жизненным циклом секретов, обеспечивая централизованное безопасное хранение с возможностью доставки секретов до потребителей.

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. Продукт автоматизирует процесс доставки и применения секретов, как для информационных систем, так и для серверов и рабочих станций.

EXC решает все ключевые задачи управления секретами:

- Централизованное безопасное хранение секретов:
  - Все секреты хранятся в одном месте и надежно зашифрованы;
  - Возможен выбор алгоритма шифрования – AES или ГОСТ.
- Разграничение доступа к секретам и их управлению:
  - Права доступа основаны на базе гибких ACL политик (Policy-Based Access Control - PBAC);
  - Поддержка ролевой модели доступа (Role-Based Access Control - RBAC);
  - Поддержка мультитенантности для изоляции групп секретов с возможностью выделения теннантов в отдельные БД.
- Автоматизация управления жизненным циклом секретов:
  - Автоматический контроль срока жизни секретов;
  - Автоматическая ротация статических секретов;
  - Динамическая генерация секретов;
  - Удаление и отзыв секретов.
- Доставка секретов до потребителей:
  - На аппаратные и виртуальные сервера;
  - В среду контейнерной оркестрации Kubernetes (в shared Volume и переменные окружения подов);
  - На рабочие станции пользователей с помощью Wallet – кошелька пользовательских секретов.

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;
- Выделение изолированной области хранилища EXC в пространство имён (namespace) с возможностью хранения в отдельной базе данных;
- Наличие графического веб-интерфейса и утилиты командной строки для удобного администрирования EXC и работы с секретами без необходимости специфичных знаний продукта;
- 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;
- Наличие графического инсталлятора для быстрой установки продукта без специальных технических знаний.

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

С помощью EXC Wallet вы можете:

Локально хранить и управлять разрешёнными секретами EXC с использованием графического интерфейса Wallet

Синхронизация секретов между EXC и локальным кошельком пользователя (Wallet) позволяет локально хранить и управлять разрешёнными секретами без необходимости обращения к EXC.

Графический интерфейс Wallet обеспечивает понятное интуитивное управление секретами без необходимости технических знаний.

Автоматизировать использование секретов на рабочем месте

Wallet предоставляет возможность автозаполнения секретов в веб-формы за счёт специализированных плагинов для браузеров. Утилита командной строки (Wallet CLI) позволяет получать секреты EXC напрямую из кошелька и автоматически подставлять их в конвейеры Bash и PowerShell команд без необходимости обращения к EXC.

Локально аутентифицироваться в EXC

Для локального доступа к секретам EXC необходимо пройти аутентификацию в Wallet с помощью одного из доступных методов: доменной учётной записи, TLS сертификата или персонального сертификата, расположенного на съемном устройстве (Токен, Смарт-карта). Также поддерживается двухфакторная аутентификация с использованием TOTP в качестве второго фактора.

Локально кэшировать секреты EXC

Пользователь кошелька может использовать кэшированные секреты даже при отсутствии связи между кошельком и EXC. Пользователь может локально кэшировать доступные секреты EXC на определённый срок, если это разрешено администратором. Все кэшированные секреты хранятся в локальном хранилище Wallet в зашифрованном виде с использованием алгоритмов AES или ГОСТ.

Централизованно управлять кошельками и коллекциями кошельков

С помощью веб-интерфейса EXC администратор может настраивать параметры работы как отдельных кошельков, так и коллекций кошельков на разных хостах:

- устанавливать двухфакторную аутентификацию для кошелька или доступа к отдельным секретам;
- включать возможность локального кэширования отдельных секретов и ограничивать срок их хранения;
- включать проверку соответствия окружения (compliance) при открытии кошельков.

ЛКПС

ЛКПС - Личный Кабинет Пользователя Сертификатов, предназначен для комфортной работы со всеми сертификатами в организации через современный интерфейс. Содержит встроенную базу хранения всех сертификатов организации. Предусматривает возможность дополнить информацию о сертификатах данными из внешних систем и из других продуктов на платформе ЦУГИ.

ЛКПС хранит все сертификаты организации и позволяет осуществлять:

- Автоматический импорт сертификатов из УЦ;
- Ручной импорт сертификатов из веб-интерфейса;
- Просматривать сертификаты в веб-интерфейсе единым списком;
- Полнотекстовый поиск, фильтрацию, агрегацию и экспорт по всем полям разобранных сертификатов;
- API для автоматического импорта сертификатов с любого УЦ;
- Возможность назначать себя или своих коллег ответственными за сертификаты вручную или автоматически с помощью коллекций сертификатов.

Справочник ответственных позволяет указывать кадровый статус сотрудника (в отпуске, уволен и т.д.), и его руководителей и учитывать эту информацию при отправке уведомлений.

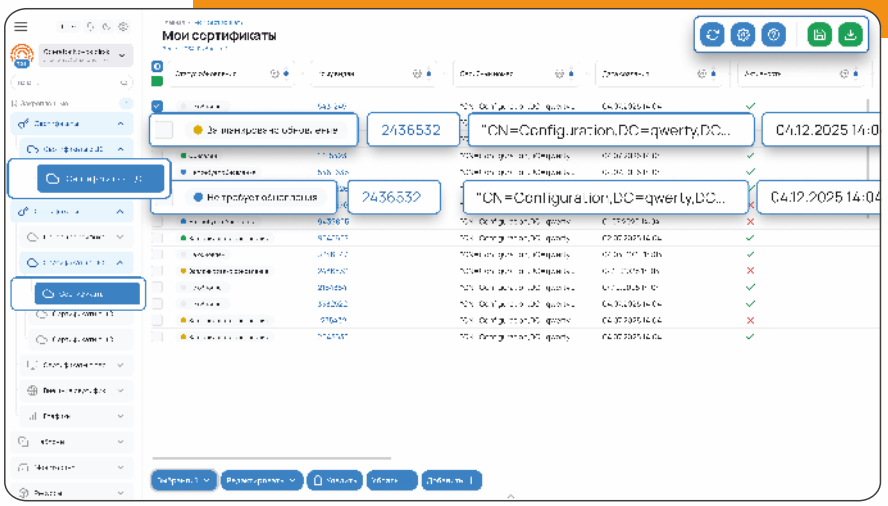
Справочник информационных систем и организационных единиц позволяет:

- Привязывать сертификаты к информационным системам (ИС) и организационным единицам (ОЕ);
- Получать статистику по сертификатам в разрезе ИС и ОЕ;
- Автоматически назначать ответственных за сертификаты, через привязку к ИС и ОК.

Классификаторы позволяют выполнять анализ загруженных в систему сертификатов и группировать в ячейки сертификаты для одного потребителя (например, сервера). На основе этого можно автоматически или вручную проставлять статусы обновления сертификатов и назначать ответственных.

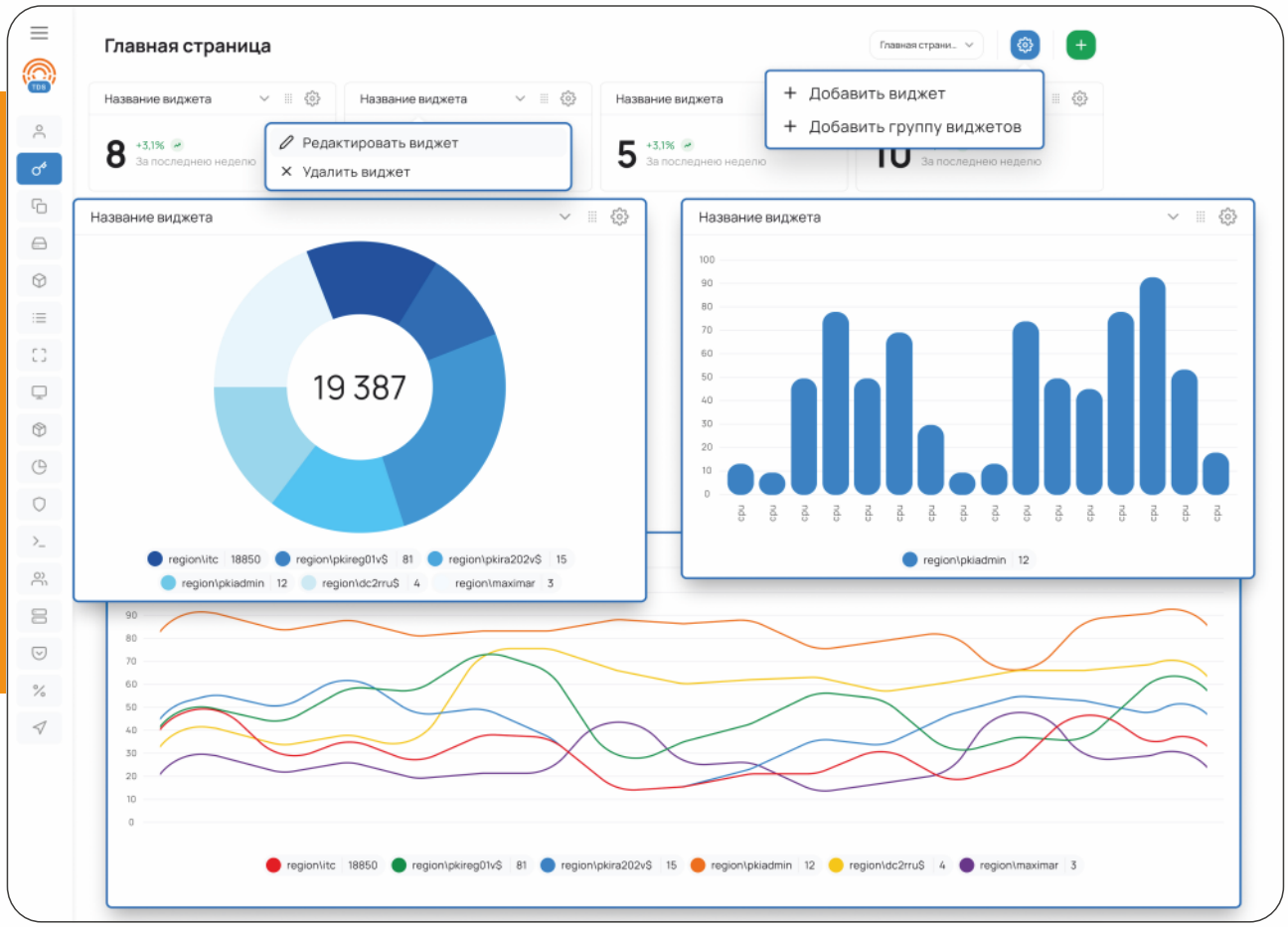
Вся информация собрана в одном месте: ЛКПС предоставляет возможность автоматически (через API) или вручную привязывать к сертификатам дополнительную информацию: места установки, владелец (ФИО, телефон, электронная почта), политика ЕСАУС, по которой был выпущен сертификат, и тип выпуска, плановая дата замены, статус обновления («заменен» или «не требуется»), статус отзыва (проверка crl).

Повышение надёжности:



ЛКПС заранее предупреждает о плановой дате замены или необходимости обновления сертификата и исключает ситуации, когда сертификат истекает неожиданно. Также позволяет оперативно выпустить новый сертификат через csr-запрос или обновить существующую ключевую пару из интерфейса системы.

Наличие статистики позволяет просматривать актуальную информацию о состоянии всех сертификатов на дашбордах и выгружать ее в формате таблиц.



Наличие интеграции с другими системами ЦУГИ (ЕСАУС, МИУ, СКЗИ) позволяет получить данные об инвентаризации сертификатов на токенах, серверах, АРМ и сетевых портах из ЦУГИ МиУ. ЛКПС предоставляет API для интеграции с различными инфраструктурными сервисами (например, в случае необходимости связывания сертификатов с данными корпоративной CMDB и добавления из нее информации к сертификатам).

СУУ СКЗИ 2.0

Портал для пользователей с возможностью создавать заявки на допуск, выдачу СКЗИ и установку дистрибутива.

Автоматическое формирование всех необходимых журналов и ведомостей.

Инвентаризация, установка и обновление Программных СКЗИ.

Автоматическая инвентаризация и регистрация всех объектов учета СКЗИ.

СУУ СКЗИ 2.0 предназначена для ИТ-специалистов и администраторов систем информационной безопасности для целей автоматизации и контроля ключевых процессов при работе с СКЗИ.

СУУ СКЗИ 2.0 позволяет максимально автоматизировать учёт и управление криптографическими средствами защиты информации и существенно снизить количество ручных операций и ошибок при заполнении карточек СКЗИ, журналов и актов.

При разработке системы был тщательным образом проанализирован опыт фактического учета СКЗИ в крупных организациях, приказы ФАПСИ 152, 313 приказ ФСБ и ПКЗ 2005. Мы стремились создать продукт, который будет максимально соответствовать требования законодательства.

Портал пользователя:

- Система помогает подобрать необходимый пользователю тип СКЗИ, исходя из ответов на уточняющие вопросы. Это экономит время ответственным за СКЗИ и позволяет пользователям самостоятельно формировать заявки на допуск к нужному типу СКЗИ;
- Портал помогает получить допуск к нужному типу СКЗИ. Пользователю предоставляются обучающие материалы в форме карточек, после изучения которых можно пройти тестирование на умение работать с выбранным СКЗИ. При успешном прохождении теста результат автоматически прикрепляется к формируемой заявке, а сама заявка направляется ответственному лицу для проверки и подписания. Все сведения об обучении и допуске фиксируются в журнале инструктажа по информационной безопасности и в журнале учета допусков к средствам криптографической защиты;
- Портал пользователя помогает сформировать заявку на получение СКЗИ и установку дистрибутива. После отправки заявка поступает ответственному за СКЗИ для принятия решения о предоставлении доступа. При этом пользователь может через систему запросить установку ПО. По результатам рассмотрения заявки ответственный за СКЗИ выполняет установку на АРМ без необходимости выхода пользователя из системы.

С помощью СУУ СКЗИ 2.0 вы сможете:

Обеспечить прозрачность процедур допуска пользователей к работе с СКЗИ

Для удобства пользователей разработан портал, на котором предусмотрена подача заявок с возможностью обучения и обязательного тестирования знаний по корректному применению СКЗИ. Портал позволяет пользователям подавать заявки на получение СКЗИ и на установку дистрибутивов, что значительно экономит время ответственных.

Эффективно собирать информацию для расследования инцидентов

Система информирует ответственных за СКЗИ при обнаружении инцидентов безопасности. СУУ СКЗИ 2.0 дает возможность выгружать сырые данные и историю эксплуатации о любом объекте учета для последующего анализа и расследования.

Гибко выстроить работу организационной структуры в компании

Двухуровневая организационная структура департаментов с возможностью настраивать права конкретных ролей в каждом из департаментов для качественной организации работы ОКЗ.

Сбор информации о программно-аппаратной конфигурации (ПАК) устройства и ведение карточки АРМ

Агенты сами собирают информацию о программно-аппаратной конфигурации устройства и хранят эту информацию в специальных карточках АРМ. Ответственный за СКЗИ имеет полную информацию не только об устройстве, но и о подключенных к нему ключевых носителях и пользовательских сертификатах.

- **Контроль выдачи, передачи и уничтожения СКЗИ.**
  Каждое действие с объектом учета фиксируется в системе и в соответствующих актах и журналах. Это позволяет отследить жизненный цикл СКЗИ от его ввода в систему до уничтожения.
- **Учет ключей и неключевых СКЗИ.**
  СУУ СКЗИ 2.0 позволяет учитывать не только СКЗИ, но и другие значимые объекты учета. Для каждой сущности предусмотрена возможность назначать дату уведомления, что обеспечивает эффективный контроль за большим количеством объектов учета.
- **Поддержка НЭП и сканов документов.**
  Система поддерживает разные виды подписей, утверждения заявок, актов и заполнения журналов. Допускается использование отсканированных документов, а также неквалифицированной электронной подписи организации.

Мы систематизировали многолетний опыт внедрения и интеграции сложных ИТ-продуктов в единую, полностью прозрачную процедуру. Для обеспечения управляемости и предсказуемости проекта мы используем типовые методики развертывания, которые включают детализированные инсталляционные карты, единый план внедрения и заранее согласованный перечень документов для подписания.

Для кого этот продукт:	Для администраторов УЦ	Для администраторов всех УЦ и их руководителя	Для пользователя сертификатов	Для Потребителя сертификатов (администраторы ИБ, пользователи ИС)	Для Органа Криптозащиты и его сотрудников	Для администраторов IT и ИБ служб, всех потребителей секретов
Для чего этот продукт:	Импортозамещение Microsoft CA	Для мониторинга и повышения надежности всех УЦ	Для самообслуживания и учета сертификатов потребителями	Для автоматизации выпуска сертификатов и замены Microsoft Enterprise PKI	Для инвентаризации, учета и управления всеми типами СКЗИ	Для централизованного управления всеми типами секретов

Функция	Clearway CA	СМИОК	ЛКПС	ЕСАУС	СКЗИ 2.0	EXC
Выпуск сертификатов						
Работа с различными УЦ через Драйвер УЦ	✗	✓	✓	✓	✓ (2026)	✓
Наличие встроенного ЦС	✓	✗	✗	✗	✗	✓
Передача закрытого ключа поверх TLS	✗	✗	✗	✗	✗	✓
Поддержка защищенных закрытых ключей на Токенах	✓	✗	✗	✓ (2026)	✓ (2026)	✗
Графический интерфейс выпуска одиночных сертификатов	✓	✓	✓	✗	✓ (2026)	✓
Командная строка для выпуска сертификатов	✓	✗	✗	✓	✗	✓
Выбор шаблона сертификата перед выпуском	✓	✓	✓	✓	✓ (2026)	✓
Механизм утверждения индивидуальных запросов на выпуск	✓	✓	✓	✓ (2026)	✓ (2026)	✗
Механизм утверждения политик автоматического выпуска сертификата	✗	✗	✗	✓	✗	✗
Гибкий графический конструктор индивидуальных запросов	✓	✓	✗	✗	✓ (2026)	✗
Гибкий графический конструктор политик автовыпуска сертификатов	✗	✗	✗	✓	✗	✗
Хранение предыдущих версий сертификатов с возможностью предоставления	✗	✗	✗	✗	✗	✓
Проактивный выпуск будущих версий сертификатов с возможностью предоставления	✗	✗	✗	✗	✗	✓
Автоматическое заполнение полей и расширений в запросе сертификата	✓	✗	✓ (польз.)	✓ (серв.)	✓ (2026)	✗
Индивидуальный выпуск нового сертификата для существующей ключевой пары	✓	✓	✓	✗	✓ (2026)	✗

Функция	Clearway CA	СМИОК	ЛКПС	ЕСАУС	СКЗИ 2.0	ЕХС
Автоматический выпуск нового сертификата для существующей ключевой пары	✗	✗	✗	✓	✓	✗
Обнаружение, анализ и аналитика сертификатов						
Парсинг и отображение сертификатов RSA	✓	✓	✓	✗	✓	✓
Парсинг и отображение сертификатов ГОСТ	✓ (2026)	✓	✓	✗	✓	✗
Общий список сертификатов со всех УЦ организации	✗	✓	✓	✗	✗	✗
Импорт внешних сертификатов	✗	✓	✓	✗	✓	✓ (2027)
Инвентаризация сертификатов на серверах агентом	✗	✓	✓ (МиУ, СМИОК)	✓ (2027)	✗	✓ (2027)
Инвентаризация сертификатов на АРМ агентом	✗	✓	✓ (МиУ, СКЗИ)	✓ (2027)	✓	✓ (2027)
Сетевая инвентаризация сертификатов (сканирование)	✗	✓ (2026)	✓ (МиУ)	✗	✗	✗
Инвентаризация сертификатов на Токенах	✗	✗	✓ (МиУ, СКЗИ)	✓ (2026)	✓	✗
Инвентаризация сертификатов в LDAP-каталогах	✗	✓	✓ (МиУ, СМИОК)	✗	✓	✗
Инвентаризация шаблонов сертификатов на УЦ	✗	✓	✗	✓ (2026)	✗	✗
Выявление рисков в сертификатах	✗	✓	✗	✗	✗	✗
Связывание сертификатов с шаблонами выпуска в едином списке	✓	✓	✓	✓	✓	✗
Связывание сертификатов с местами установки и/или обнаружения	✗	✓	✓	✓	✓ (Token)	✗
Связывание сертификатов с организационными единицами (информационные системы, отделы и пр.)+ ведение справочника орг. единиц	✗	✗	✓	✓	✓ (2026)	✗
Постановка внешнего сертификата на мониторинг (сервис certRkMon)	✗	✓	✓	✗	✗	✗
Аналитика состояния PKI-инфраструктуры (AIA, CDP. OCSP, SCEP, УЦ, HSM и др.)	✗	✓	✗	✗	✗	✗
Аналитика статистики выпуска сертификатов	✓	✓	✓	✓	✗	✗
Аналитика распределения ответственности за сертификаты	✗	✗	✓	✗	✓	✗

Функция	Clearway CA	СМИОК	ЛКПС	ЕСАУС	СКЗИ 2.0	ЕХС
Ведение каталога ключей (Токенов) и связывание их с сертификатами	✗	✗	✓ (СКЗИ 2026)	✓ (2026)	✓	✗
Функции поиска и индексации в едином списке						
Аналитика распределения ответственности за сертификаты	✗	✓	✓	✗	✓	✗
Ведение каталога ключей (Токенов) и связывание их с сертификатами	✗	✗	✓	✗	✗	✗
Персонализация и уведомления						
Ролевая модель: админ, аудитор, пользователь	✓	✓	✓	✓	✓	✓
Личный кабинет – мои сертификаты, мои подписки, мои настройки уведомлений, список моих уведомлений	✓	✓	✓	✓ (2027)	✗	✗
Автоматизация и интеграция с другими ИС						
Автоматическое распространение списка доверенных сертификатов УЦ	✗	✗	✗	✓	✗	✗
В состав системы входит Агент ЦУГИ и соответствующие модули	✗	✓	✗	✓	✓	✓ (2026)
API-вызовы для интеграции с внешними системами	✓	✓	✓	✓	✓	✓
Поддержка HSM и CSP от КриптоПро	✓	✓ (2026)	✗	✓ (2026)	✓	✓
Поддержка RuToken	✗	✗	✓ (СКЗИ)	✓ (2026)	✓ (2026)	✗
Поддержка Clearway CA	n/a	✓	✓	✓	✓	✓
Поддержка Microsoft CA	✗	✓	✓	✓	✗	✓
Поддержка УЦ КриптоПро	✗	✓ (2026)	✓	✓	✓	✓
Поддержка SafeTech CA	✗	✗	✓	✓	✓	✓
Поддержка Aladdin eCA	✗	✗	✓	✓	✓	✓
Поддержка УЦ Валидата	✗	✗	✓ (2026)	✓ (2027)	✓	✓ (2027)
Поддержка УЦ GlobalSign	✗	✗	✓ (2027)	✓ (2026)	✗	✓ (2027)
Поддержка УЦ Let's Encrypt	✗	✗	✓ (2027)	✓ (2026)	✗	✓ (2027)
Автоматическая регистрация токенов пользователей и сертификатов в системе учета	✗	✗	✓ (СКЗИ)	✗	✓	✗
Загрузка метаданных о сертификатах из внешних систем	✗	✗	✓	✗	✗	✗
Логика рассылки уведомлений с учетом кадрового статуса	✗	✗	✓	✓ (2026)	✓	✓ (2026)
Автоматическая доставка и установка сертификатов в ИС-потребители	✗	✗	✗	✓	✗	✓

Функция	Clearway CA	СМИОК	ЛКПС	ЕСАУС	СКЗИ 2.0	ЕХС
Автоматическая доставка сертификатов в Kubernetes Secrets	✗	✗	✗	✓	✗	✓
Автоматическая доставка сертификатов в Kubernetes Pods	✗	✗	✗	✓ (2027)	✗	✓
Поддержка пользовательских сценариев выпуска и установки сертификатов	✗	✗	✗	✓	✗	✗
Реализация скоординированного обновления сертификатов на кластерах	✗	✗	✗	✓	✗	✗
Автоматический выпуск сертификатов для Kubernetes и Istio Service Mesh	✗	✗	✗	✓	✗	✓
Установка и обновление доверенных корневых сертификатов на сервера	✗	✗	✗	✓	✗	✗
Установка и обновление доверенных корневых сертификатов на АРМ	✗	✗	✗	✓	✓	✗
Автоматизация резервного копирования УЦ	✓ (2026)	✗	✗	✗	✗	✗
Инструменты диагностики и администрирования всей PKI	✗	✓	✗	✗	✗	✗
Инвентаризация версий установленных криптопровайдеров и крипто библиотек на АРМ	✗	✓	✗	✓ (2027)	✓	✗
Индивидуальные и массовые задания на установку/обновление/удаление ПО криптопровайдеров	✗	✗	✗	✗	✓	✗
Индивидуальные и массовые задания на установку/обновление/удаление лицензий для крипто провайдеров	✗	✗	✗	✗	✓	✗
Ведение журналов и логирование						
Полный цикл функций и комплект журналов для учета СКЗИ по ФАПСИ 152	✗	✗	✗	✗	✓	✗
Журналирование и логирование действий пользователя в системе	✓	✓	✓	✓	✓	✓
Отправка журналов действий пользователей по протоколу Syslog	✗	✗	✗	✓	✗	✓
Отправка журналов действий пользователей в отдельную БД	✗	✗	✓	✓	✗	✓

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА И СОПРОВОЖДЕНИЕ

После внедрения вы не останетесь один на один с системой.
Мы предлагаем:

- **Техническую поддержку 8x5 и 24x7**. Решение любых вопросов в кратчайшие сроки;
- **Обновления**. Регулярные улучшения системы;
- **Консультации** по использованию функциональных возможностей продукта.

Профессиональная экспертиза

Всесторонняя экспертиза инженеров команды поддержки позволит минимизировать риски простоя систем и обеспечить их бесперебойную работу

Круглосуточная поддержка

Эксперты по поддержке продуктов всегда на связи, чтобы ответить на вопросы, помочь решить проблему и обеспечить эффективную работоспособность систем, разработанных Clearway Integration

Индивидуальные рекомендации

Команда Clearway Integration разработает индивидуальное предложение по обеспечению технической поддержки наших продуктов с учетом конкретных задач и потребностей вашего бизнеса

Получите консультацию по продукту

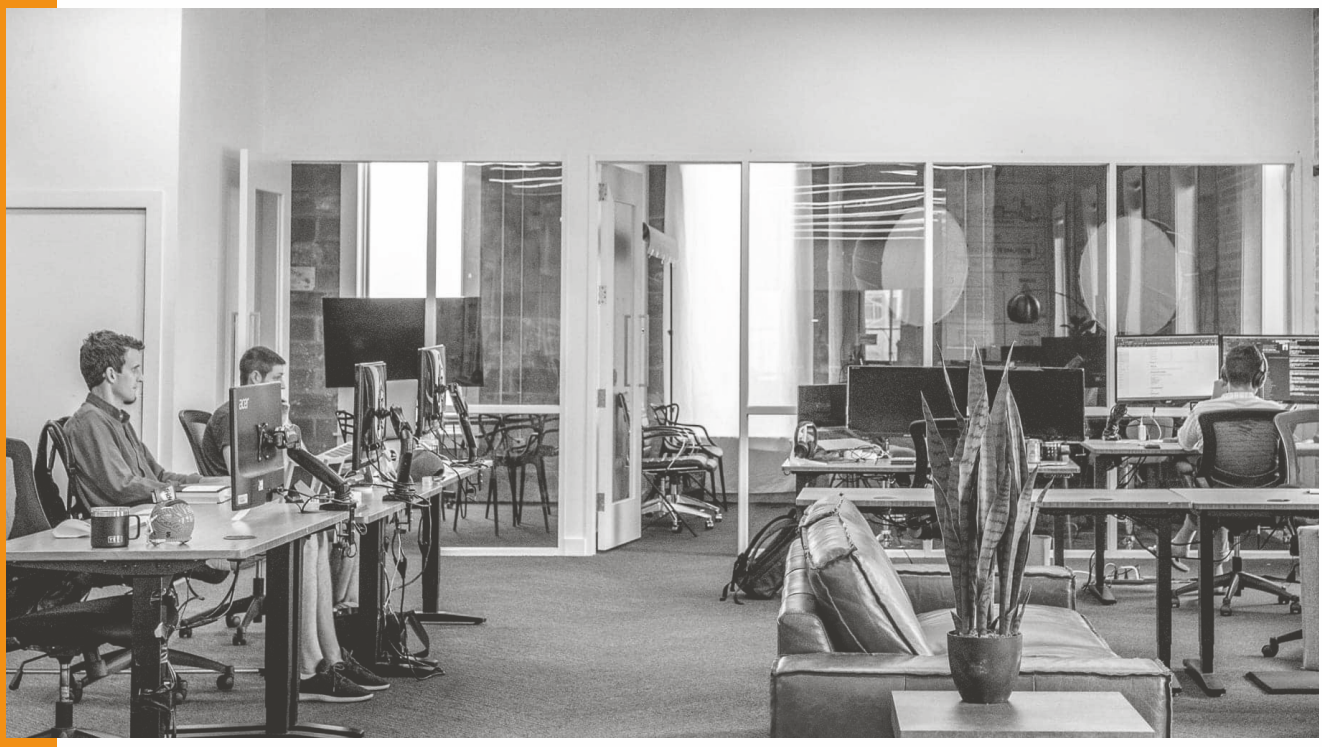
+7 495 142 13 15
info@clearwayintegration.com
clearway.ru

Clearway Integration - разработчик ПО для централизованного и автоматизированного управления ИТ-инфраструктурой бизнеса, обеспечения оптимизации ресурсов и высокого уровня безопасности данных.

Clearway Integration предлагает надёжные и эффективные решения по импортозамещению продуктов линейки Microsoft — Microsoft Enterprise PKI и Microsoft System Center. Продукты разрабатываются на базе единой платформы Централизованного Управления Гетерогенными Инфраструктурами (включена в Реестр Отечественного ПО с 2022 года).

CLEARWAY
INTEGRATION

- Полностью российская разработка
- Импортозамещение линейки продуктов Microsoft Enterprise PKI
- Соответствие требованиям регуляторов
- Гибкая система лицензирования по модулям и функциям системы
- 15+ лет опыта
- Услуги по внедрению и сопровождению
- Круглосуточная техническая поддержка



CLEARWAY
INTEGRATION

Офис в Москве

4-я Магистральная ул., д. 11, стр. 2.
+7 (495) 142-13-15

clearway.ru
info@clearwayintegration.com