

СМИОК

Система Мониторинга Инфраструктуры
Открытых Ключей

Преимущества:

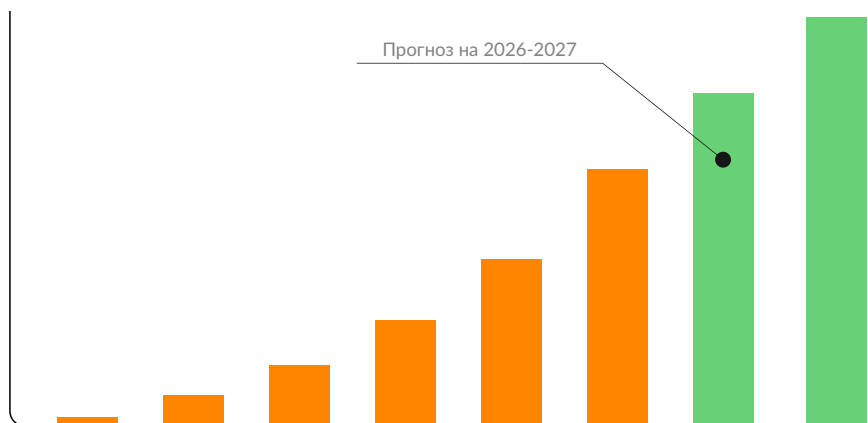
Внедрение СМНОК значительно повышает доступность PKI и способствует сокращению затрат на ее поддержку за счет следующих факторов:

- **Мониторинг**, анализ и управление всеми УЦ и другими компонентами PKI из единого окна;
- **Своевременное оповещение** о сбоях компонентов PKI;
- **Оповещения о событиях** жизненного цикла сертификатов (например, отзыв или окончание срока действия);
- **Предотвращение сбоев PKI** за счет выявления предшествующих событий на основе «модели здоровья»;
- **Предотвращение сбоев** различных компонентов зависимой информационной инфраструктуры за счет централизованного мониторинга срока действия всех сертификатов.

Увеличение количества веб-компонентов и веб-приложений (в том числе, контейнерных и облачных платформ Kubernetes и Service Mesh) ведет к наращиванию нагрузки на центр сертификации и экспоненциальному росту количества выпускаемых сертификатов.

Ранее IT-специалисты использовали стандартные средства администрирования PKI, входящие в состав операционных систем. Но с ростом числа сертификатов эти методы стали неэффективными: человеческий фактор, несистемное управление Центров сертификации и нарушение стандартов безопасности – все эти проблемы с эксплуатацией PKI резко снижают уровень защищенности организации, поскольку PKI является ядром информационной безопасности.

В современном мире для эффективного управления PKI и растущими объемами выпускаемых сертификатов требуется автоматизированный инструмент мониторинга, контроля и управления.



Система Мониторинга ИОК (СМНОК) 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.

Лучшее решение для группы сопровождения PKI

СМНОК обеспечит своевременное реагирование на события мониторинга и позволит осуществлять эксплуатацию корпоративного PKI любого масштаба.

Предотвращение сбоев и автоматизация управления сертификатами:

- ◆ Автоматизация и треккинг рабочих задач администраторов и дежурной смены УЦ/PKI;
- ◆ Возможность выпуска сертификатов по запросам с подтверждением и автоматически;
- ◆ Мониторинг функциональности и доступности HSM;
- ◆ Выпуск тестовых сертификатов для контроля работы всех компонентов;
- ◆ Загрузка в единый справочник внутренних и внешних сертификатов и мониторинг их состояния, включая незапланированный отзыв;
- ◆ Оценка качества: мониторинг рисков, ошибок, нарушений для выпущенных сертификатов и настроек шаблонов сертификатов.

**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).

Контроль внешних сертификатов:

- СМНОК позволяет добавлять внешние сертификаты (выпущенные за пределами организации) в единый справочник и вести их анализ и мониторинг;
- Инвентаризация фактически установленных сертификатов на серверах;
- Карточки серверов для просмотра всех установленных в них сертификатов.

В СМНОК предусмотрена «модель здоровья», которая включает в себя:

- ◆ Проверку состояния процессов УЦ в ОС сервера;
- ◆ Снятие счётчиков производительности УЦ;
- ◆ Анализ журналов событий УЦ;
- ◆ Проверку доступности и содержимого точек распространения CDP/AIA;
- ◆ 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 MiniCA;
- ◆ Анализ выпущенных сертификатов на типовые риски и требования безопасности.

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

**Возможности масштабирования
решения**

- Эффективная работа с миллионами 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.

Мониторинг \ Объекты мониторинга

Объекты мониторинга < 1 >

Всего: 37. Выбрано: 0

ID	Наименование	Статус	Активность	Класс	Группа
<input type="checkbox"/>	146 CWI Root CA. CDP Location #1	Success	Активные	CWIMonitoring.CWI Root CA.CDP Location #1	CWI Root CA
<input type="checkbox"/>	145 CWI Root CA. AIA Location #1	Success	Активные	CWIMonitoring.CWI Root CA.AIA Location #1	CWI Root CA
<input type="checkbox"/>	144 CWI-CA2. OCSP Location #1	Success	Активные	CWIMonitoring.CWI-CA2.OCSP Location #1	cwi-ca2
<input type="checkbox"/>	143 CWI-CA2. DeltaCRL Location #1	Success	Активные	CWIMonitoring.CWI-CA2.DeltaCRL Location ...	cwi-ca2
<input type="checkbox"/>	142 CWI-CA2. AIA Location #2	Success	Активные	CWIMonitoring.CWI-CA2.AIA Location #2	cwi-ca2
<input type="checkbox"/>	141 CWI-CA2. AIA Location #1	Success	Активные	CWIMonitoring.CWI-CA2.AIA Location #1	cwi-ca2
<input type="checkbox"/>	139 CWI-CA. CDP Location #2	Success	Активные	CWIMonitoring.CWI-CA.CDP Location #2	cwi-ca
<input type="checkbox"/>	138 CWI-CA. DeltaCRL Location #2	Error	Активные	CWIMonitoring.CWI-CA.DeltaCRL Location #2	cwi-ca
<input type="checkbox"/>	137 CWI-CA. DeltaCRL Location #1	Error	Активные	CWIMonitoring.CWI-CA.DeltaCRL Location #1	cwi-ca
<input type="checkbox"/>	136 CWI-CA. AIA Location #2	Success	Активные	CWIMonitoring.CWI-CA.AIA Location #2	cwi-ca
<input type="checkbox"/>	135 CWI-CA. AIA Location #1	Success	Активные	CWIMonitoring.CWI-CA.AIA Location #1	cwi-ca
<input type="checkbox"/>	134 CWI-CA. CDP Location #1	Success	Активные	CWIMonitoring.CWI-CA.CDP Location #1	cwi-ca
<input type="checkbox"/>	132 CWI-CA2. CDP Location #1	Success	Активные	CWIMonitoring.CWI-CA2.CDP Location #1	cwi-ca2
<input type="checkbox"/>	130 CRL availability: http://cwi-ca.cwi.local/CertE...	Error	Активные	CWIMonitoring.CWI-CA.AIA Location #1	cwi-ca2
<input type="checkbox"/>	97 http://pki.cwi.local/CertEnroll/CWI_MiniCA_1...	Success	Активные	CWIMonitoring. http://pki.cwi.local/CertEnrol...	cwi-de-camn
<input type="checkbox"/>	96 cwi-de-camn.cwi.local. Server status	Success	Неактивные	CWIMonitoring. Virtual Server Status	cwi-de-camn
<input type="checkbox"/>	95 http://pki.cwi.local/CertEnroll/CWI_MiniCA_1...	Success	Активные	CWIMonitoring. http://pki.cwi.local/CertEnrol...	cwi-de-camn
<input type="checkbox"/>	94 http://pki.cwi.local/CertEnroll/CWI_MiniCA_1...	Success	Активные	CWIMonitoring. http://pki.cwi.local/CertEnrol...	cwi-de-camn
<input type="checkbox"/>	93 cwi-ca.cwi.local. Server status	Success	Неактивные	CWIMonitoring. Virtual Server Status	cwi-ca
<input type="checkbox"/>	92 cwi root ca.cwi.local. Server status	Success	Неактивные	CWIMonitoring. Virtual Server Status	cwi root ca
<input type="checkbox"/>	91 cwi-ca2.cwi.local. Server status	Success	Неактивные	CWIMonitoring. Virtual Server Status	cwi-ca2
<input type="checkbox"/>	77 cwi-ca.cwi.local. Service CertSvc - Running	Success	Активные	CWIMonitoring.Service CertSvc	cwi-ca
<input type="checkbox"/>	76 cwi-ca2.cwi.local. Service CertSvc - Running	Success	Активные	CWIMonitoring.Service CertSvc	cwi-ca2
<input type="checkbox"/>	75 cwi-ca.cwi.local. RDP Sessions Count = 1	Success	Ак...	DP Sessions Count	cwi-ca

Текст

Подписчики

Обслуживание В работе x v

Найти

Очистить фильтры

Компоненты:

Сервер мониторинга

реализует модель здоровья, производит обработку данных.

Сервер отображения (web)

интерфейс системы.

Осуществляет отображение состояния наблюдаемой системы, производит оповещения, предоставляет инструменты управления, взаимодействует с внешними системами.

Сервер БД

хранит собираемые данные и предоставляет их по запросам других компонентов.

Мост

предоставляет интерфейс управления агентами на наблюдаемых серверах.

Агент

системный сервис, управляемый с сервера моста и осуществляющий сбор данных по сценариям.

СМИОК производит сбор общесистемных метрик и параметров, специфичных для ИОК для проведения оценки состояния компонентов. В типовой набор метрик для Центра Сертификации входит:

- Загрузка ЦПУ;
- Доступная оперативная память;
- Доступное дисковое пространство по каждому диску;
- Очереди к дискам;
- Состояние сервиса ЦС;
- Состояние резервного копирования;
- События перезагрузки (Uptime);
- Доступность HSM.

Агенты присылают метрики на сервер мониторинга, где они обрабатываются и отображаются согласно правилам.

Безагентский мониторинг

Кроме внутренних метрик на серверах ИОК, необходимо также контролировать доступность различных интерфейсов, которые предоставляют компоненты ИОК. Такие проверки осуществляются без применения агентов и выполняются с сервера мониторинга или сервера Моста. Предусмотрены проверки доступности и состояния следующих сущностей:

- Точек распространения CRL;
- Сертификатов на точках AIA;
- Отклика OCSP;
- Интерфейсов NDES/SCEP и MS-WSTEP/MS-XSCEP, а также доступность интерфейса запроса сертификатов на ЦС.

Функционал структурированного мониторинга:

- ◆ Возможность объединять объекты 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, включая возможность добавления на визуальные диаграммы и подписку на оповещения об изменении состояния.

Поддержка и сопровождение

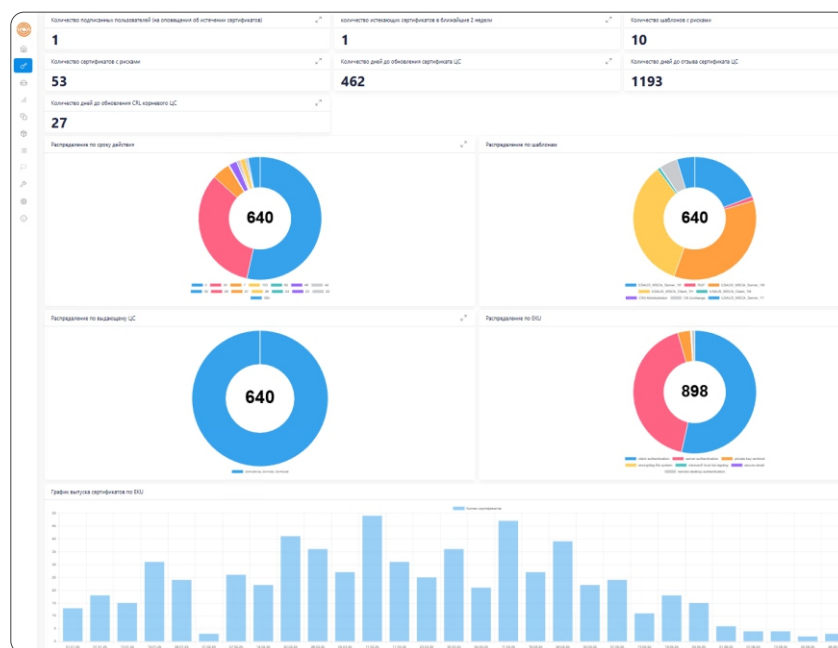
После внедрения вы не останетесь один на один с системой. Мы предлагаем:

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



Получите
консультацию
по продукту

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



СМИОК содержит центр регистрации, где любой пользователь, имеющий необходимые разрешения, может запросить сертификат. Такой способ запроса сертификата обладает рядом преимуществ перед стандартными способами:

- ◆ Максимально простой интерфейс;
- ◆ Дополнительные данные по сертификату заносятся в БД: кто запросил, для каких целей и т.п.;
- ◆ Пользователь автоматически подписывается на оповещения об истечении сертификата;
- ◆ Можно настроить выпуск автоматически или с одобрением администратора;
- ◆ Имеется конструктор запросов CSR.

Запрос через CSR

Если у пользователя имеется файл запроса CSR, он может вставить текст в форму или указать путь к файлу. Запрос будет автоматически распознан и выведены его параметры. После отправки запроса, в зависимости от прав пользователя, будет выпущен сертификат или запрос будет ожидать одобрения администратора.

Учет задач эксплуатации

Функционал постановки и отслеживания задач эксплуатации в СМИОК обеспечивает следующее:

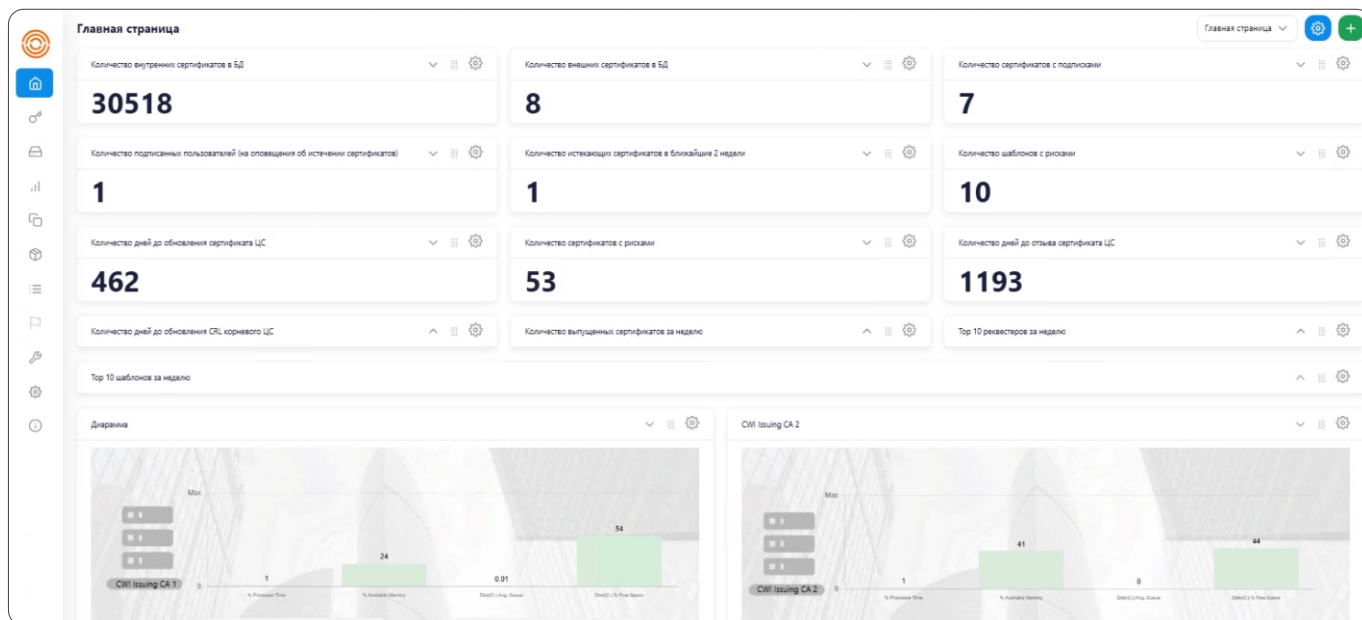
- ◆ Позволяет учитывать время, потраченное на регламентные работы и работы по инцидентам;
- ◆ При изменении определенных параметров задачи производится оповещение участвующих пользователей;
- ◆ Для общей оценки трудоемкости обслуживания ИОК существуют графики продвижения задач, которые показывают степень выполнения и количество потраченного времени за определенный период. Графики позволяют оценить загруженность сотрудников и их эффективность.

В СМИОК предусмотрена система периодических отчетов:

- Периодичность и состав отчетов настраиваются администратором;
- Администратор может выбрать способ отправки оповещений: по электронной почте, СМС или в группу Telegram.

Подписки на оповещения

Объекты мониторинга предоставляют возможность подписываться на оповещения об изменении их состояния. Возможна подписка на любые объекты, как реальные, так и виртуальные. Оповещения могут отправляться по различным каналам, таким как электронная почта, СМС и Telegram.



clearwayintegration.com

info@clearwayintegration.com

Clearway Integration - системный интегратор и 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