

Как ИБ контролировать установку и обновление миллионов сертификатов?

Мониторинг, самообслуживание и аналитика
технологической ИОК

Секция:
«Интеграция PKI с прикладными системами.
PKI-проекты и продукты»

Проблемы и задачи – ч.1

- Общий справочник всех сертификатов организации
- Поиск и фильтрация по общему справочнику
- Подписка на события с сертификатами:
 - срок действия ключа
 - срок действия сертификата
 - отзыв сертификата
- Мониторинг доступности и корректности AIA/CRL, Delta CRL/CDP
- Мониторинг параметров серверов УЦ и их компонентов
- Мониторинг работоспособности HSM
- Мониторинг синтетической транзакции выпуска сертификата
- Мониторинг шаблонов УЦ и корректности их настроек

Проблемы и задачи – ч.2

- Контроль резервного копирования УЦ
- Доска и трекер задач для администраторов УЦ
- Сводные диаграммы и таблицы мониторинга всех УЦ в организации
- Инвентаризация сертификатов в хранилищах ОС и ИС
- Инвентаризация сертификатов на сетевых портах
- Инвентаризация сертификатов на токенах
- Личный Кабинет Пользователя Сертификатов
 - Личный список сертификатов
 - Переназначение ответственных/владельцев
 - Аналитика обновления и использования
 - Получение сводных данных из систем ЕСАУС, СМИОК, МиУ и Учет СКЗИ
 - Ручной выпуск и перевыпуск сертификатов
 - Мастер подключения ИС к ЕСАУС
 - Интеграция с корпоративной CMDB и реестром ИС

Компоненты решения

- **Платформа ЦУГИ** (№13033 в реестре отечественного ПО)
 - Кроссплатформенный агент (Ready for Astra) – Win/Linux/AIX/MacOS
 - Мосты (Ready for Astra)
 - Сервер Управления Политиками и Агентами
 - Драйвер УЦ для интеграции
- Продукт **СМИОК** – Система Мониторинга ИОК
- Продукт **ЛКПС** – Личный Кабинет Пользователя Сертификатов
- **МиУ** – Мониторинг и Управление АРМ и Серверов
- Интеграция с ЕСАУС
- Интеграция с KeyBox
- Интеграции с прикладными и инфраструктурными ИС > 100
- Встраивание в бизнес-процесс развертывания новых АРМ

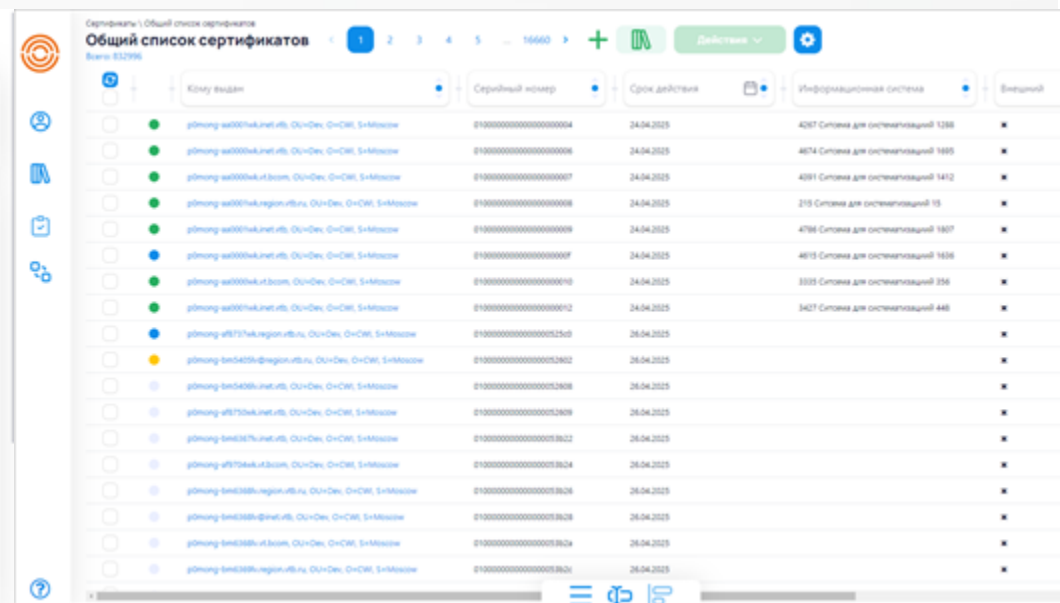
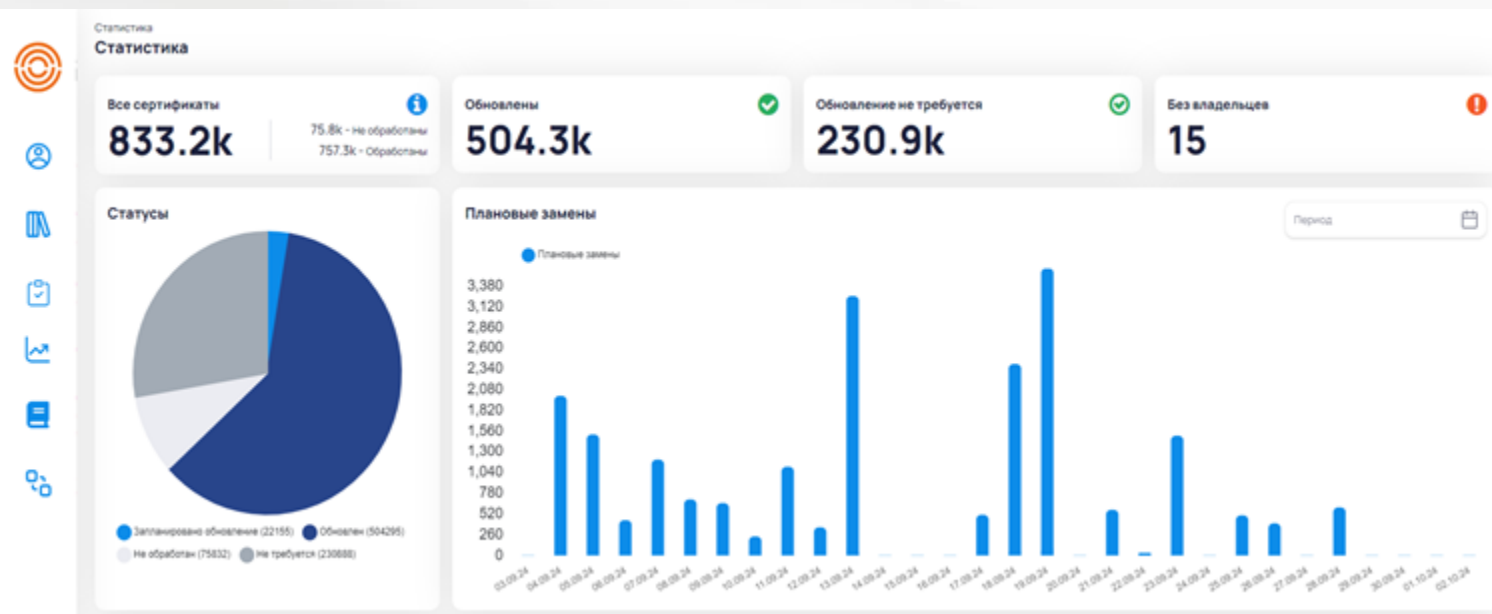
ЕСАУС: Доставка и установка сертификатов



- Формирование/сбор запросов
- Проверка запросов на соответствие политикам
- Доставка запросов на УЦ
- Обратная доставка сертификатов потребителю
- Установка сертификатов в Информационных Системах (ИС)

Функции Личного Кабинета

- Единое окно для пользователей
- Поиск по всем сертификатам
- Сбор данных из всех систем ЦУГИ и других ИС
- Определение владельца и передача сертификатов
- Места установки и использования
- Отчеты для руководства
- Уведомления пользователям
- Статистика и аналитика
- API для прикладных задач
- Выпуск и обновление сертификатов



Общий список сертификатов

Всего: 132996

Кому выдан	Серийный номер	Срок действия	Информационная система	Внешний
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000004	24.04.2025	4267 Система для системной 1288	*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000006	24.04.2025	4674 Система для системной 1685	*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000007	24.04.2025	4381 Система для системной 1412	*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000008	24.04.2025	219 Система для системной 15	*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000009	24.04.2025	4766 Система для системной 1807	*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	0100000000000000000000000000000F	24.04.2025	4615 Система для системной 1636	*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000010	24.04.2025	3335 Система для системной 356	*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000012	24.04.2025	3427 Система для системной 448	*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000015	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000016	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000017	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000018	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000019	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000020	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000021	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000022	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000023	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000024	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000025	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000026	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000027	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000028	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000029	26.04.2025		*
plmimg-ws0000uknet.ru, O=C=Dev, O=C=WS, S= Moscow	01000000000000000000000000000030	26.04.2025		*

ЛКПС в цифрах

Всего 550 тыс. сертификатов для 1979 ИС

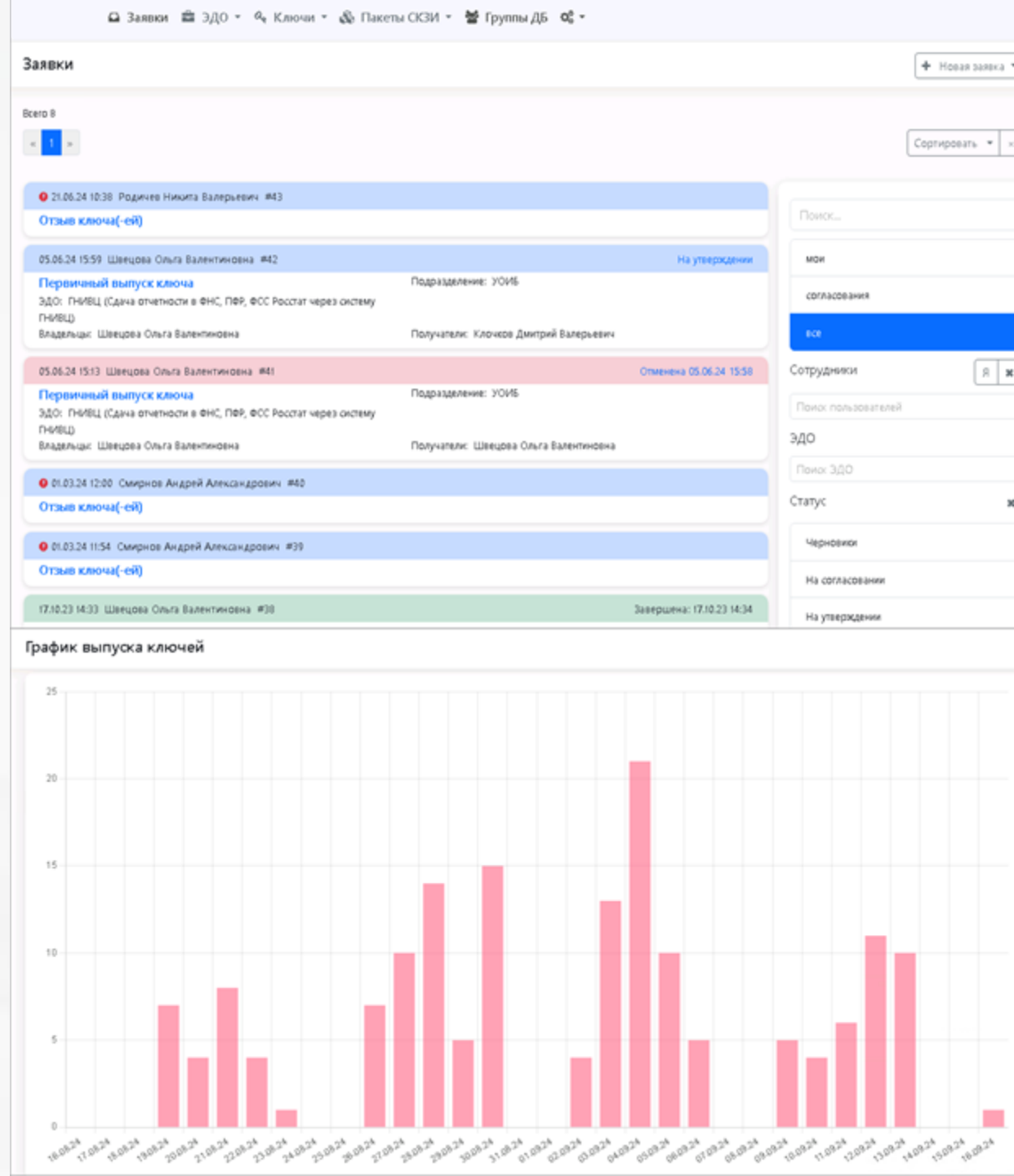
Пользователи ЛКПС:

- 250-300 администраторов
- В будущем около 90 тыс. пользователей

Сертификаты:

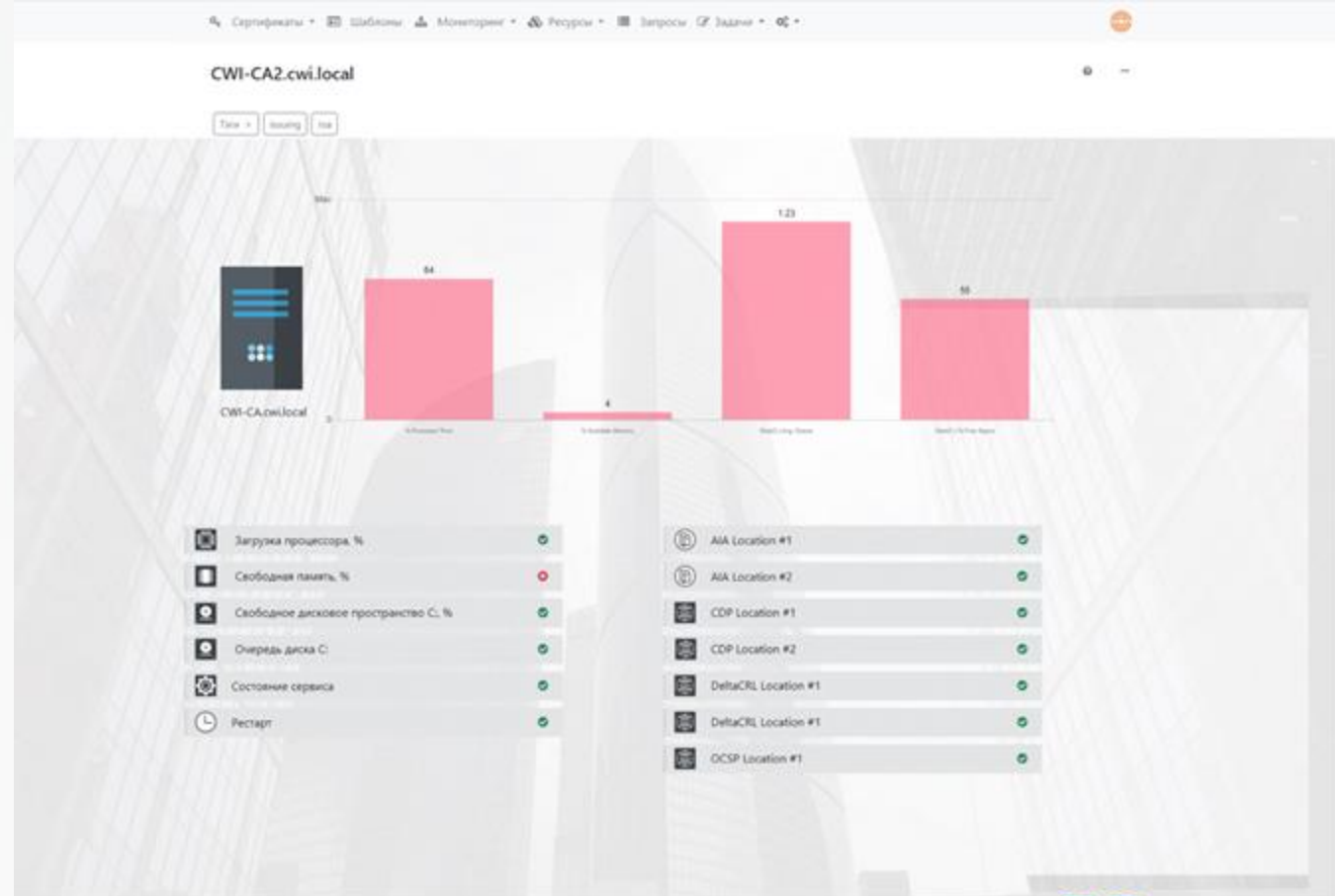
- Квалифицированных ключей – 780
- Неквалифицированных ключей – 1507
- Сертификатов для технических нужд (VPN и т.п.) – 90 тысяч.

Уведомлений для пользователей за 2 года – 87 тыс.



Функции СМИОК

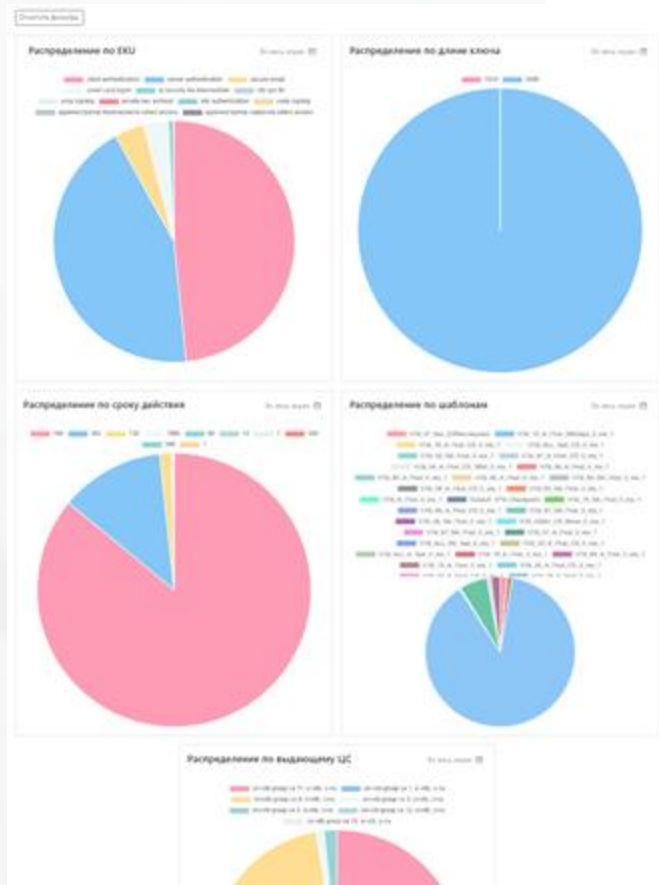
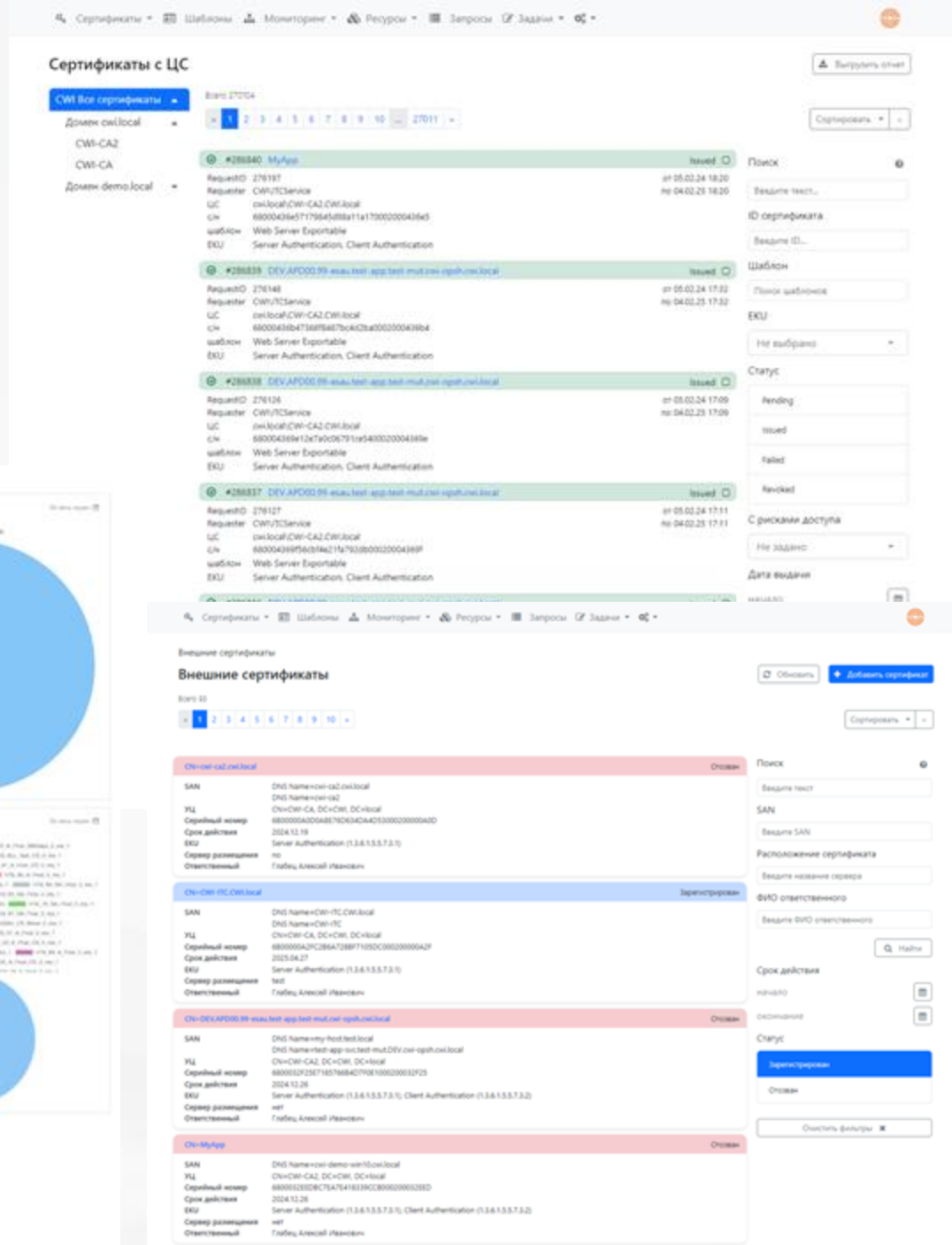
- Мониторинг:
 - оборудования УЦ;
 - серверной ОС УЦ;
 - службы и процессы УЦ;
 - точки распространения AIA/CRL;
 - протоколы OCSP/SCER;
 - выпуск сертификатов;
 - настройки шаблонов;
 - настройки безопасности;
 - резервное копирование;
 - производительность;
 - журналы аудита;



Резервное копирование						
CWI-CA						
20200218	OK	тип: Full	дата: 20.02.20 13:20	расположение	размер (КБайт): 25	Сделать резервную копию
20200219	OK	тип: Full	дата: 20.02.20 13:20	расположение	размер (КБайт): 25	
20240204	OK	тип: Full	дата: 05.02.24 20:49	расположение	размер (КБайт): 22532	
20240205	OK	тип: Full	дата: 05.02.24 20:52	расположение	размер (КБайт): 23556	
Today	OK	тип: Full	дата: 06.02.24 16:41	расположение	размер (КБайт): 24580	
CWI-CA2						
20200217	Running	тип: Full	дата: 14.01.20 18:53	расположение	размер (КБайт): 0	Сделать резервную копию
20200218	Running	тип: Full	дата: 20.02.20 13:20	расположение	размер (КБайт): 0	
20200219	Running	тип: Full	дата: 20.02.20 13:20	расположение	размер (КБайт): 0	
Today	OK	тип: Full	дата: 20.02.20 13:20	расположение	размер (КБайт): 25	

Функции СМИОК

- Анализ сертификатов:
 - срок действия сертификатов
 - срок действия ключей
 - со всех УЦ организации
 - мониторинг внешней ИОК
 - внешних сертификатов
 - отзыв внутренних
 - отзыв внешних
 - риски свойств
- Ролевая модель
- Ручной выпуск
- Управление УЦ

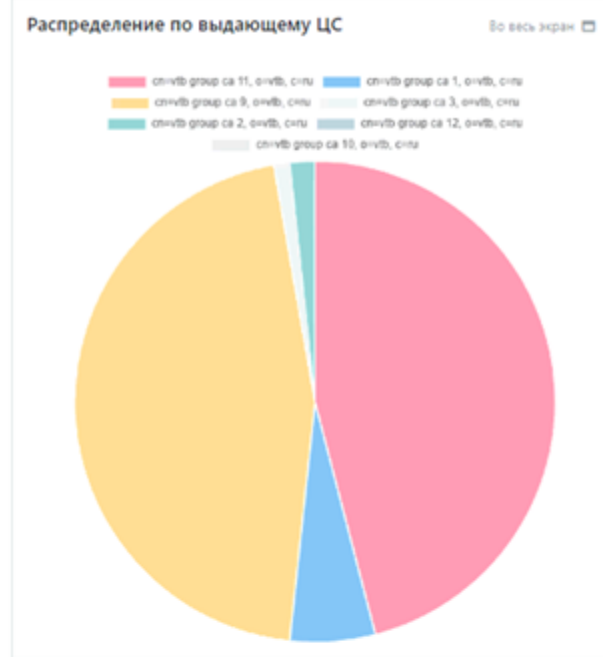



The screenshot displays the Clearway Integration web interface, which includes a navigation bar at the top with tabs for Сертификаты, Шаблоны, Мониторинг, Ресурсы, Запросы, and Задачи. The main content area is divided into two sections:

- Сертификаты с ЦС:** A section for viewing certificates from the Certificate Service (ЦС). It includes a list of certificates with details such as RequestID, Requester, UC, CN, and EKU. The interface also features a search bar, a list of templates, and a status filter.
- Внешние сертификаты:** A section for viewing external certificates. It includes a list of certificates with details such as SAN, DNS Name, and EKU. The interface also features a search bar, a list of templates, and a status filter.

СМИОК в цифрах

- 7 контуров инсталляции СМИОК с общим числом 40 серверов
- Под мониторингом более 100 серверов PKI
- Более 1 миллиона сертификатов на контроле:
 - Внешних сертификатов – 841
 - Сертификатов скоро истекает – 19 тыс.
 - Выявлены риски – 27 штук
 - Выпущенных за неделю – 61 тыс.

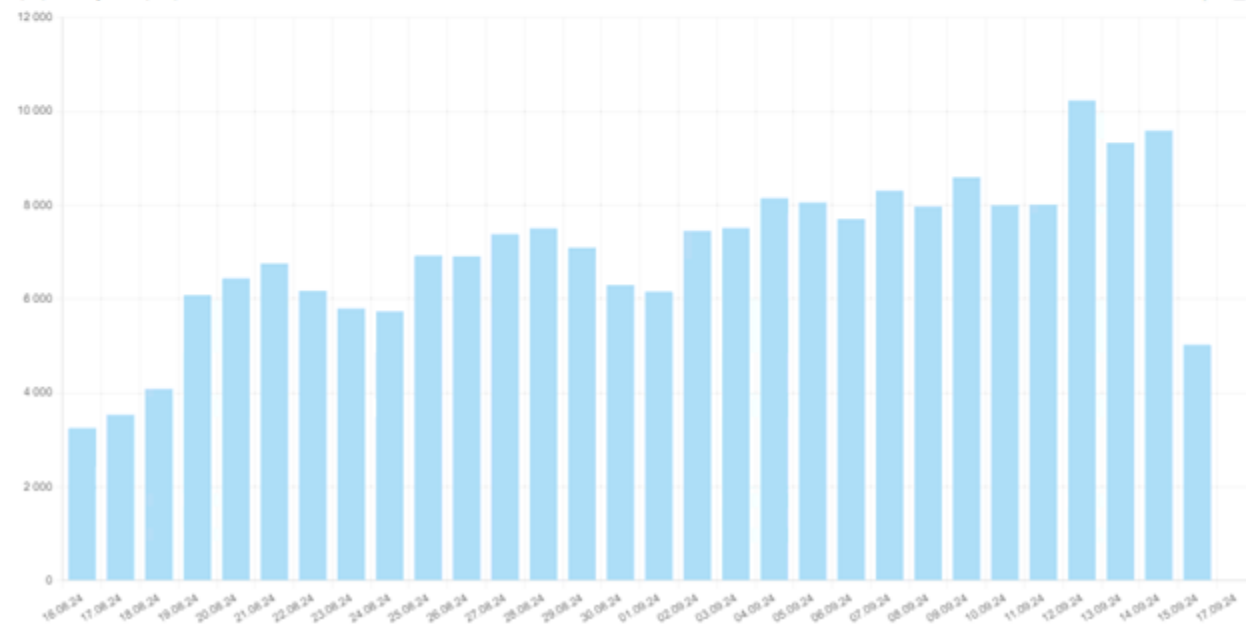


Выпущенные сертификаты

[Посмотреть сертификаты](#)

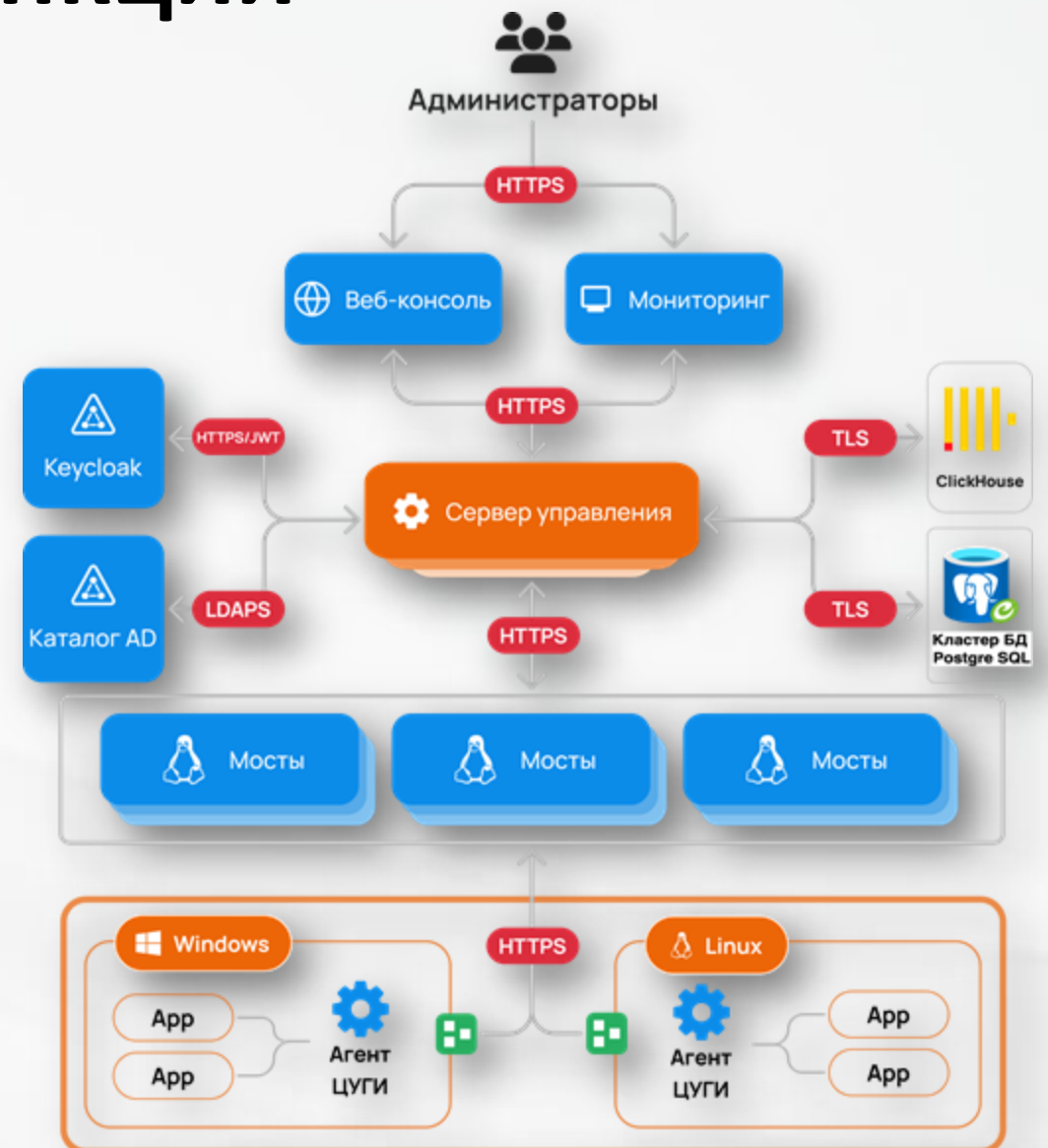
График выпуска сертификатов по EKU:

[Во весь экран](#)



Архитектура МиУ и ее функции

- Инвентаризация сертификатов на сетевых портах путем сетевого сканирования
- Инвентаризация факта установки сертификатов в ОС и приложениях локальным Агентом
- Встроенный модуль Контроля Съемных Устройств, который позволяет выявлять токены и инвентаризировать доступные на них сертификаты
- Проверка и мониторинг работоспособности ИОК и контроль выпуска сертификатов с выбранных АРМ серверов
- Инвентаризация, установка и обновление программных компонентов крипто-провайдеров, крипто-библиотек и их лицензий



МиУ и КСУ в цифрах

- Более 28 000 АРМ под управлением
 - Более 15 тыс. – Windows
 - Более 13 тыс. – Astra Linux
- Всего 30 серверов **МиУ** включая 24 моста
- Инвентаризация 25 классов инвентарей 750Гб данных
- Более 10 миллионов операций **КСУ** (около 80 тыс. в день).

Инвентарь / Установленное ПО по пакетному менеджеру (Linux)

Установленное ПО по пакетному менеджеру (Linux)

Всего 5



Скачать отчёт

Хост	Дата факта	Название	Версия	CVE
alse	10.04.2024 09:31	firefox	84.0.2+build1-0ubuntu0.18.04.1astra1	n/a (465)
mars-4	02.05.2024 13:11	aptdaemon	1.1.1+bzr982-0ubuntu39	3.8 (2)
mars-4	02.05.2024 13:11	postgresql	14+238	8 (1)
mars-4	02.05.2024 13:11	snapt	2.58+22.04.1	7.8 (1)
vtb-bridge-test	03.06.2024 06:00	postgresql	15+248	8 (1)

Установленное ПО по пакетному менеджеру (Linux)

Хост: vtb-bridge-test
Дата факта: 03.06.2024 06:00
Название: postgresql
Версия: 15+248
Отпечаток времени инвентаризации: 1717383629
CVE: [CVE-2024-0985](#)

Базовый рейтинг: 8

Уязвимости по CVE / Сведения об уязвимости

Уязвимость CVE-2024-0985

Название	PUBUSHED
Статус	PUBUSHED
CVE ID	CVE-2024-0985
Дата публикации	08.02.2024
Дата обновления	08.02.2024
Производитель	PostgreSQL
Продукт	PostgreSQL
Версия	13, 14, 15, < 12.18, < 13.14, < 14.11, < 15.6
Базовый рейтинг	8
Описание	Late privilege drop in REFRESH MATERIALIZED VIEW CONCURRENTLY in PostgreSQL allows an object creator to execute arbitrary SQL functions as the command issuer. The command intends to run SQL functions as the owner of the materialized view, enabling safe refresh of untrusted materialized views. The victim is a supervisor or member of one of the attacker's roles. The attack requires luring the victim into running REFRESH MATERIALIZED VIEW CONCURRENTLY on the attacker's materialized view. As part of exploiting this vulnerability, the attacker creates functions that use CREATE RULE to convert the internally-built temporary table to a view. Versions before PostgreSQL 15.6, 14.11, 13.14, and 12.18 are affected. The only known exploit does not work in PostgreSQL 16 and later. For defense in depth, PostgreSQL 16.2 adds the protections that older branches are using to fix their vulnerability.

Экосистема решений платформы ЦУГИ

- **ЕСАУС** – предназначена для комплексного и удобного контроля и управления TLS-сертификатами
- **УЦ на базе OpenSSL** – альтернатива Microsoft Standalone CA
- **Драйвер УЦ** – позволяет работать с УЦ разных производителей.
- **Учет СКЗИ** – система осуществляет сопровождение всего жизненного цикла ключей в организации.
- **СМИОК** – обеспечивает мониторинг как самой ИОК так и внешних/внутренних сертификатов, тестирование CRL.
- **ЕСС** - объединяет сертификаты из разных источников в единую базу
- **ЛКПС** – вместе с ЕСС позволяет работать в одном окне со любыми сертификатами и СКЗИ всей организации.
- **МиУ** – система управления конфигурацией в гетерогенных ИТ-инфраструктурах, предоставляющая ИТ-службам и подразделениям ИБ инструментарий для контроля и управления различными аспектами жизненного цикла и конфигурации рабочих станций и серверов на базе ОС Linux и Windows в едином, наглядном и универсальном интерфейсе.



Получите готовое решение

📍 Москва, улица Магистральная 4-я, д. 11

🌐 clearwayit.com

✉ info@clearwayintegration.com

☎ +7(495)142-13-15

