

Контроль доступа к периферийным устройствам в крупной компании

Опыт внедрения

Инсайдерские атаки

- Инфильтрация и Эксфильтрация
- Различные типы устройств
 - Съёмные носители (**Flash, дисководы**)
 - Сетевые устройства (**Wi-fi, Ethernet, Bluetooth**)
 - **Телефоны**
 - **Принтеры**
 - **Композитные** устройства

Масштабы

- **Распределенная** сеть
- **Десятки тысяч** конечных устройств
- **Требования** ИТ и ИБ



Ситуация на момент старта разработки

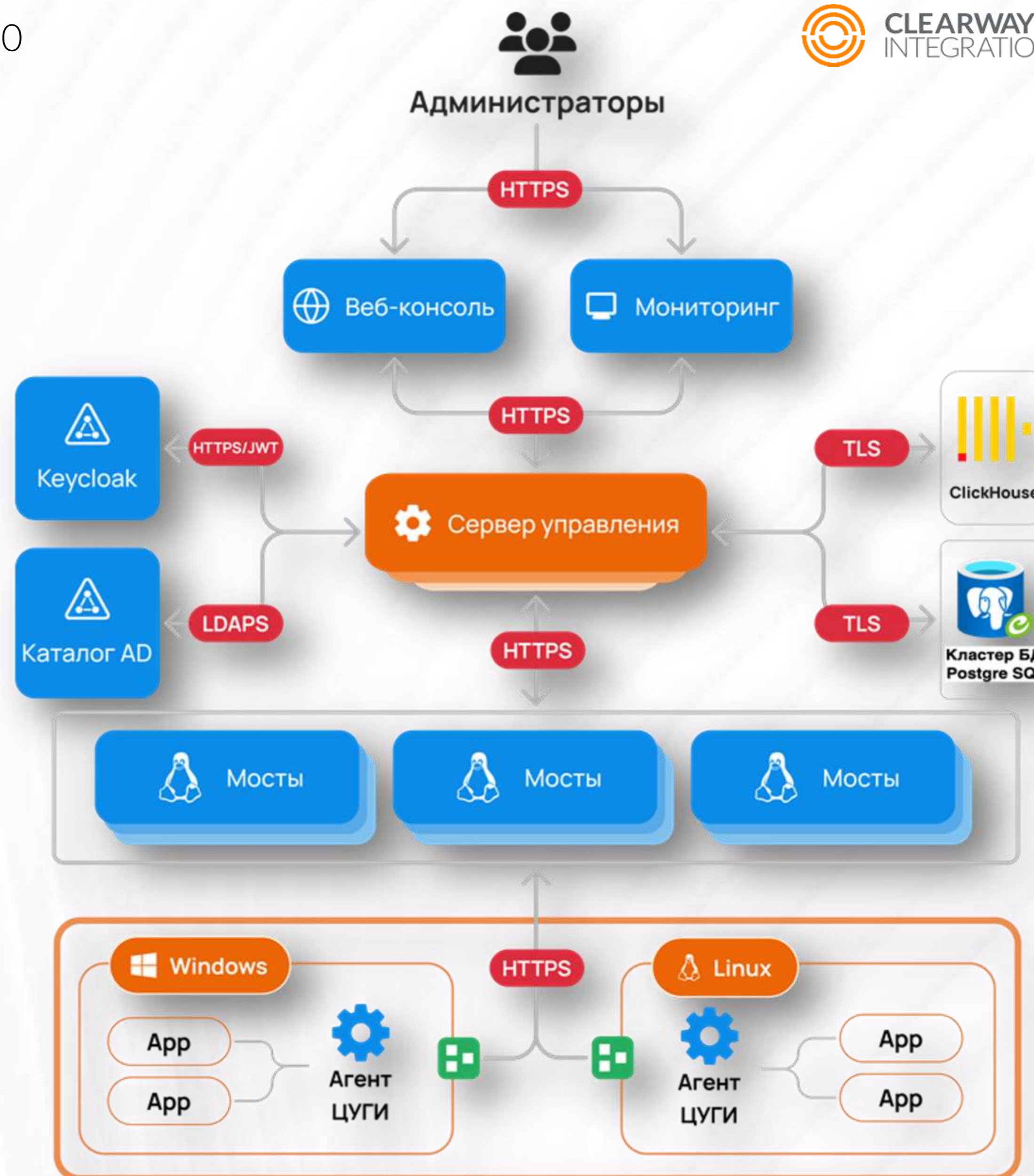
- Собственные средства ОС Windows и Linux
 - Windows – Registry, Group Policies
 - Linux - udev
- Существовавшие решения
 - Windows first
 - Linux и другие ОС – через виртуализацию



КСУ: Общая архитектура

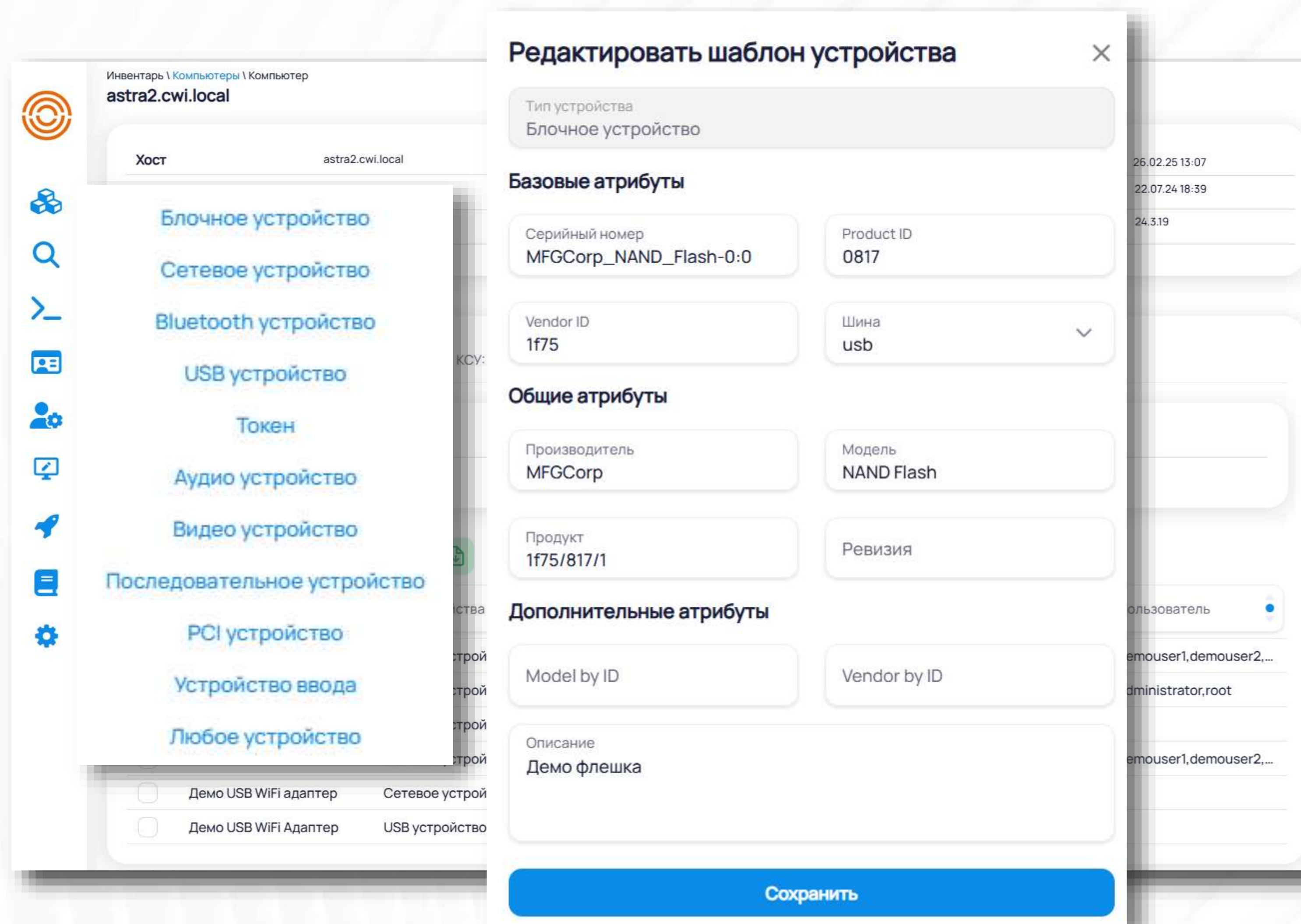
Система **к**онтроля **с**ъёмных **у**стройств

- Кросс-платформенный агент
- Мосты – балансировка
отказоустойчивость
оптимизация трафика
- ClickHouse и/или PostgreSQL
- KeyCloak
- Службы каталога



КСУ: Функции

- События:
 - подключение
 - разрешение/запрет
 - вход пользователей
- Шаблоны устройств
- Правила доступа (ACE/ACL)



The screenshot displays the 'Edit Device Template' dialog box in the Clearway Integration interface. The background shows a navigation menu on the left and a main content area with a breadcrumb trail: 'Инвентарь \ Компьютеры \ Компьютер astra2.cwi.local'. The main content area lists various device types: 'Блочное устройство', 'Сетевое устройство', 'Bluetooth устройство', 'USB устройство', 'Токен', 'Аудио устройство', 'Видео устройство', 'Последовательное устройство', 'PCI устройство', 'Устройство ввода', and 'Любое устройство'. The 'Edit Device Template' dialog box is open, showing the following fields:

- Тип устройства: Блочное устройство
- Базовые атрибуты:
 - Серийный номер: MFGCorp_NAND_Flash-0:0
 - Product ID: 0817
 - Vendor ID: 1f75
 - Шина: usb
- Общие атрибуты:
 - Производитель: MFGCorp
 - Модель: NAND Flash
 - Продукт: 1f75/817/1
 - Ревизия:
- Дополнительные атрибуты:
 - Model by ID
 - Vendor by ID
- Описание: Демо флешка

A blue 'Сохранить' (Save) button is located at the bottom of the dialog box.

КСУ в цифрах

Всего

≈85 000

Рабочих станций

Из них

54 000

Под управлением
КСУ

Масштабы

35
администраторов

≈65 000
Пользователей на
рабочих станциях

>10млрд
Строк в некоторых таблицах
инвентарей

Нагрузка

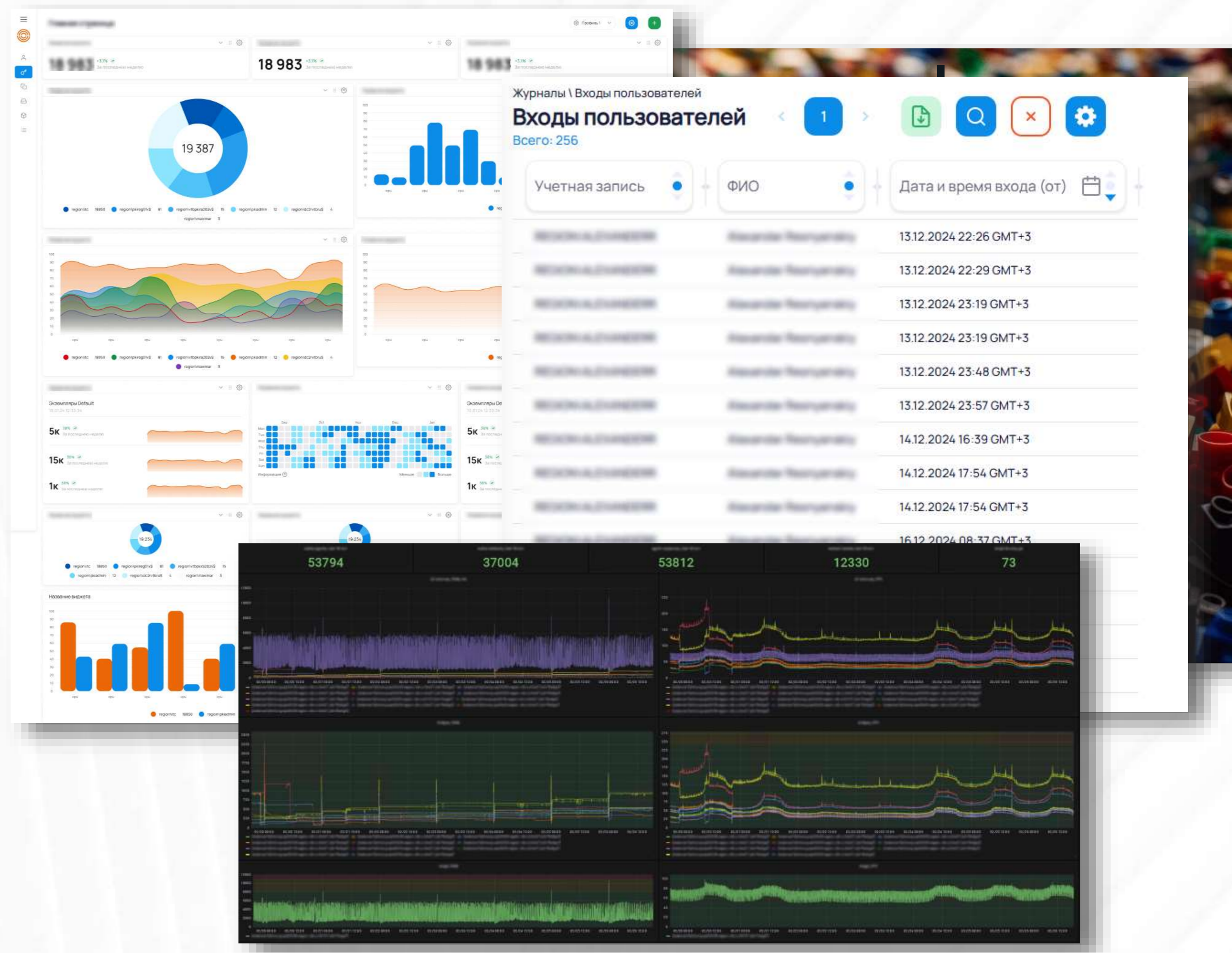
>100млн
Событий контроля доступа с
начала эксплуатации

>9 000
Событий КСУ в минуту в
пиковые часы

>2 000 **>1 500**
Шаблонов Правил КСУ

КСУ: Уроки внедрения

- **Совместимость**
 - Совместная работа
 - Производители ОС
- **Безопасность**
 - Least privilege
 - Linux capabilities
- **Enterprise features**
 - Мониторинг
 - Журналирование
 - Роли и аудит
- **Быстродействие**



Всё?



Инвентаризация

- Оборудование
- Windows, Linux, ПО
- Безопасность
- Сеть, службы каталогов

Инвентарь | Коллекции | Выполнить команду | КСУ: События | КСУ: ACL | Процессы

- Linux - Локальные пользователи
- Linux - Операционная система
- Linux - Параметры sysctl
- Linux - Привилегии (sudoers)
- Linux - Процессы
- Linux - Процессы по списку
- Linux - Серверы DNS
- Linux - Сервисы
- Linux - Сетевые интерфейсы
- Linux - События auditd
- Linux - Установленное ПО
- Linux - Файловые системы
- Безопасность - Вход/выход пользователей
- Безопасность - Ограничения безопасности
- Безопасность - Статистика auditd
- КриптоПРО
- Оборудование - BIOS
- Оборудование - CPU
- Оборудование - HDD
- Оборудование - RAM
- Оборудование - Модели APM

Инвентарь | Компьютеры | Компьютер
astra2.cwi.local

Хост	astra2.cwi.local	Авторизован	Авторизован	Последняя активность	26.02.25 13:07
ОС	Linux	Статус	Активен	Создан	22.07.24 18:39
Версия агента	2024.4.1101	Обслуживание	Не на обслуживании	Версия КСУ	24.3.19

Инвентарь | Коллекции | Выполнить команду | КСУ: События | **КСУ: ACL** | Процессы

Статус доставки ACL: Применен

Время обновления: 24.02.25 15:14

Всего: 6. Выбрано: 0.

Описание	Тип устройства	Модель	Производитель	Права	Пользователь
<input type="checkbox"/> Демо флешка	Блочное устройство	NAND Flash	MFGCorp	ENABLE,BLOCK_WRITE	demouser1,demouser2,...
<input type="checkbox"/> Демо флешка	Блочное устройство	NAND Flash	MFGCorp	ENABLE	administrator,root
<input type="checkbox"/> USB Адаптер Ethernet	Сетевое устройство	USB 10/100/1000 LAN	Realtek	ENABLE	*
<input type="checkbox"/>	Блочное устройство	USB Flash Disk	Generic	ENABLE	demouser1,demouser2,...
<input type="checkbox"/> Демо USB WiFi адаптер	Сетевое устройство	USB WLAN	802.11n		*
<input type="checkbox"/> Демо USB WiFi Адаптер	USB устройство	USB WLAN	802.11n		*

Путь до исполняемого файла деинсталляции	C:\Program Files (x86)\Notepad++\uninstall.exe	
Архитектура	32	
Дата установки	01.01.70 03:00	
CVE	CVE ID	Базовый рейтинг
	CVE-2019-16294	9.4
	CVE-2022-31901	3.5
	CVE-2022-32168	7.9
	CVE-2023-40031	7.8
	CVE-2023-40036	5.5
	CVE-2023-40164	5.5
	CVE-2023-40166	5.5

Управление

- Настройка ПО и обновлений
- Групповые политики и Workflow
- Сети и подсети

Управление | База данных | Управление | Сценарий управления

Сценарий управления

Имя: Установка и регистрация СурфПро CSP 3.0

Описание: Установка СурфПро CSP 3.0 и установка общего шаблона

Шаги сценария

Шаг 1

Имя: Установка СурфПро CSP 3.0

Сценарий: Командный файл

Пользователь: administrator,root

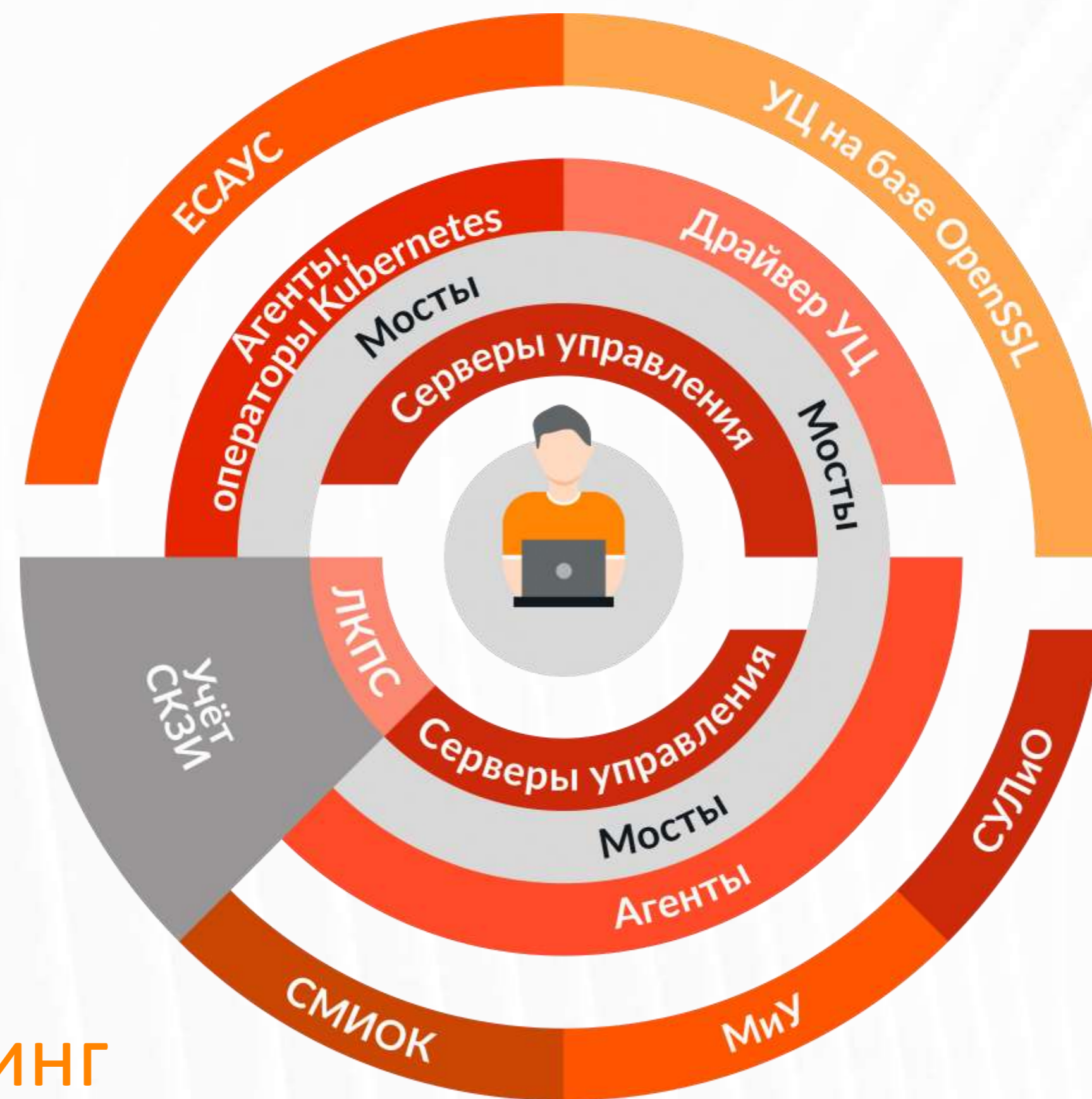
Параметры: `cmd /c ...`

ЦУГИ

Автоматическое управление сертификатами

Личный кабинет пользователя сертификатов

Мониторинг инфраструктуры открытых ключей



Интеграция и замещение удостоверяющих центров

Учет лицензий ПО

Развертывание ПО и обновлений

Мониторинг и Управление АРМ

Получите готовое решение



- 📍 Москва, улица Магистральная 4-я, д. 11
- ✉ info@clearwayintegration.com
- ☎ +7 495 142 13 15
- 🌐 clearwayit.ru

