

Простое решение по предотвращению утечек через периферийные устройства

Александр Суховей
«Клируэй Текнолоджис»

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

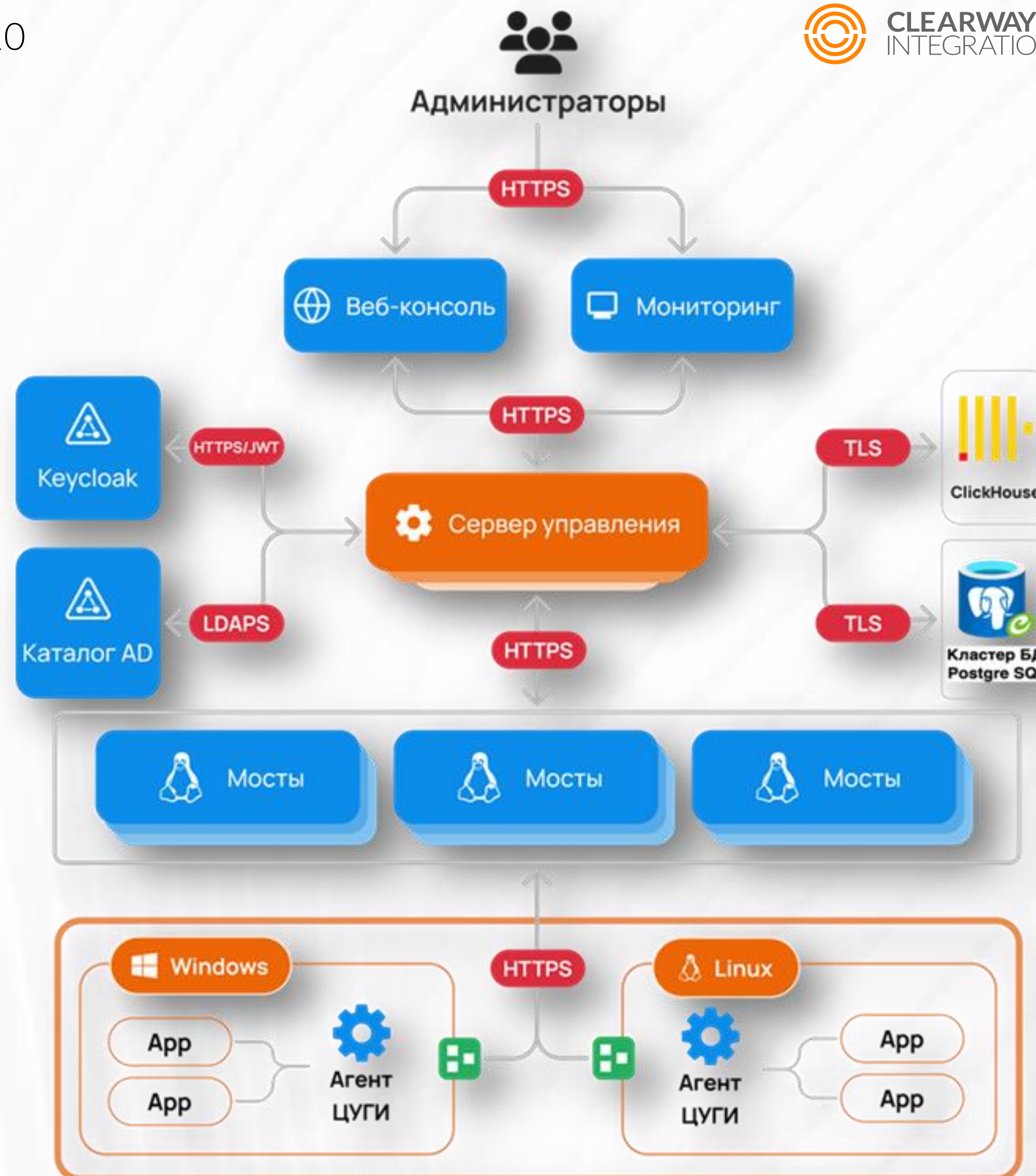
- Собственные средства ОС Windows и Linux
 - Windows – Registry, Group Policies
 - Linux - udev
- Существовавшие решения
 - Windows first
 - Linux и другие ОС – через виртуализацию



КСУ: Общая архитектура

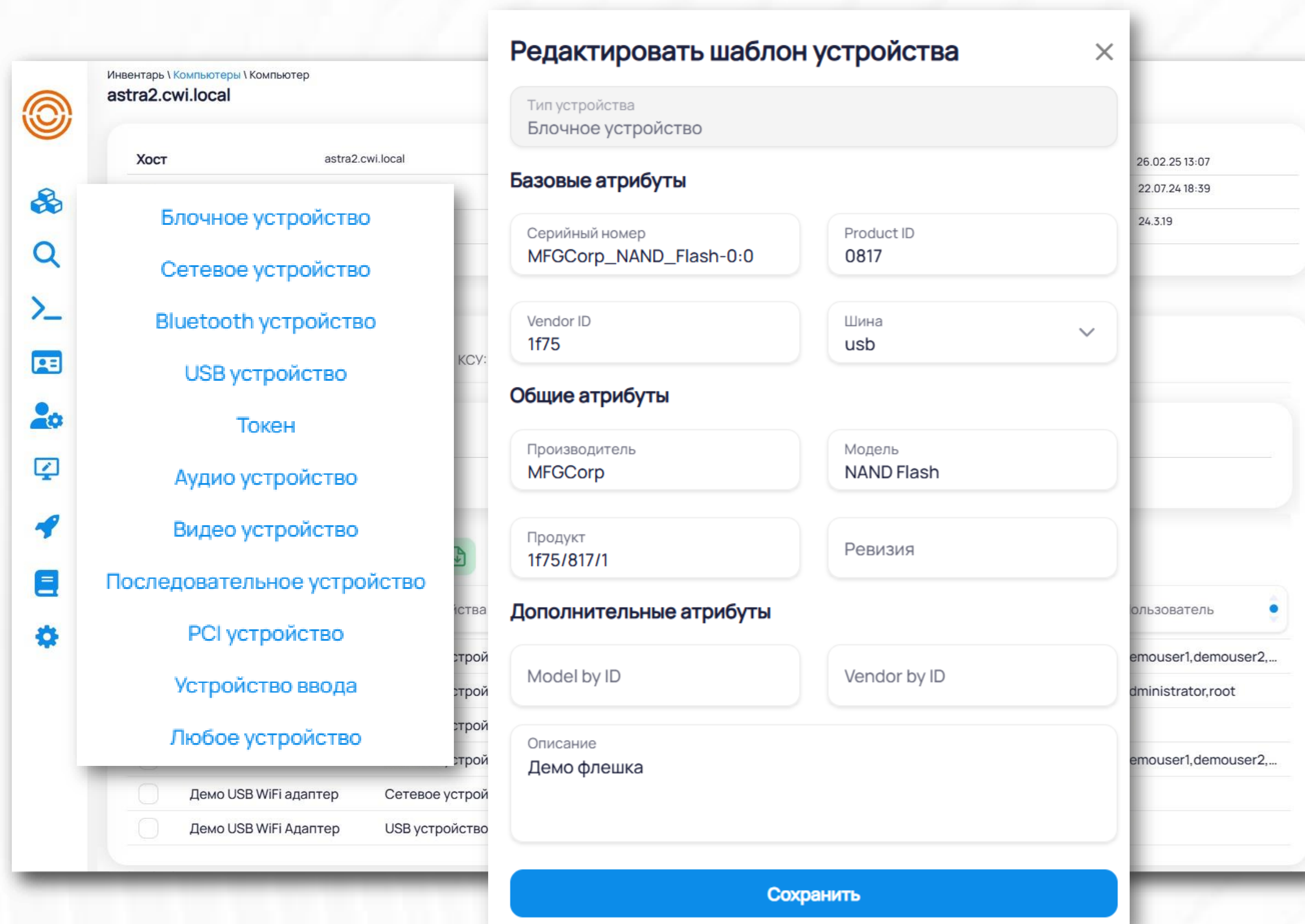
Система **к**онтроля **с**ъёмных **у**стройств

- 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 device inventory page for 'astra2.cwi.local' with a list of devices and a sidebar with navigation icons.

Редктировать шаблон устройства

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

Сохранить

КСУ в цифрах

Всего

>100 000

Рабочих станций

Из них

≈60 000

Под управлением
КСУ

Масштабы

35
Операторов КСУ

≈65 000
Пользователей на
рабочих станциях

>2 300 **>1 700**
Шаблонов Правил КСУ

Нагрузка

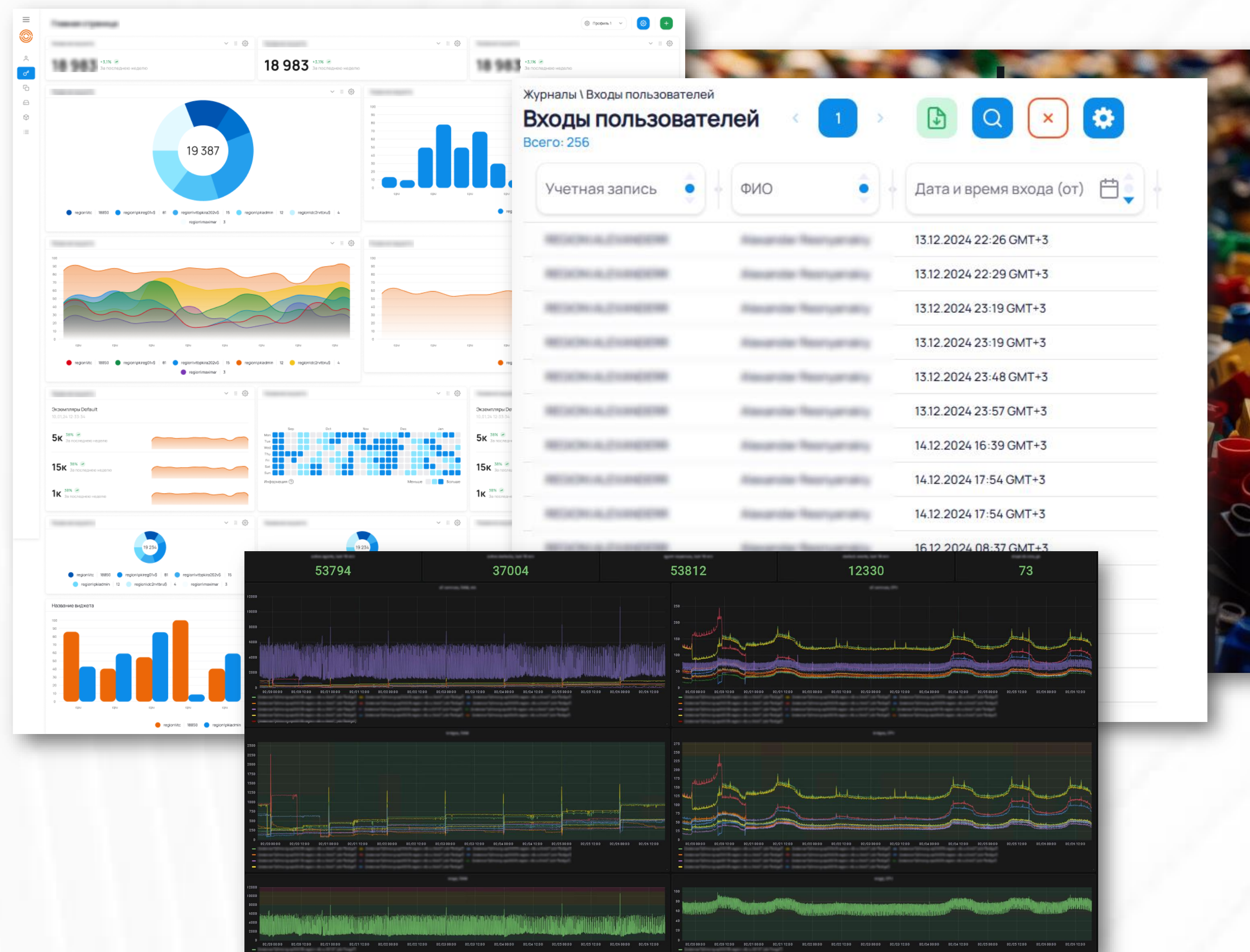
>100млн
Событий контроля доступа с
начала эксплуатации

>9 000
Событий КСУ в минуту в
пиковые часы

>10млрд
Строк в некоторых таблицах
инвентарей

КСУ: Уроки внедрения

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



BCĚ?



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
Демо флешка	Блочное устройство	NAND Flash	MFGCorp	ENABLE,BLOCK_WRITE	demouser1,demouser2,...
Демо флешка	Блочное устройство	NAND Flash	MFGCorp	ENABLE	administrator,root
USB Адаптер Ethernet	Сетевое устройство	USB 10/100/1000 LAN	Realtek	ENABLE	*
	Блочное устройство	USB Flash Disk	Generic	ENABLE	demouser1,demouser2,...
Демо USB WiFi адаптер	Сетевое устройство	USB WLAN	802.11n		*
Демо USB WiFi Адаптер	USB устройство	USB WLAN	802.11n		*

Управление

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

Управление | Библиотека управления | Сценарий управления

Сценарий управления

Имя: Установка и регистрация SurotoPro CSP 5.0

Описание: Установка SurotoPro CSP 5.0 и установка общей лицензии

Шаги сценария

Шаг 1: Параметры шага

Имя: Установка SurotoPro CSP 5.0

Сценарий: * (выбрано)

Рабочий каталог: [поле]

Параметры: [поле]

Добавить переменную окружения: [поле]

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

Файл результатов: install_csp_success

Файл ошибок: install_csp_error

Файл завершения: install_csp_completed

Имя файла: [поле]

Имя типа: [поле]

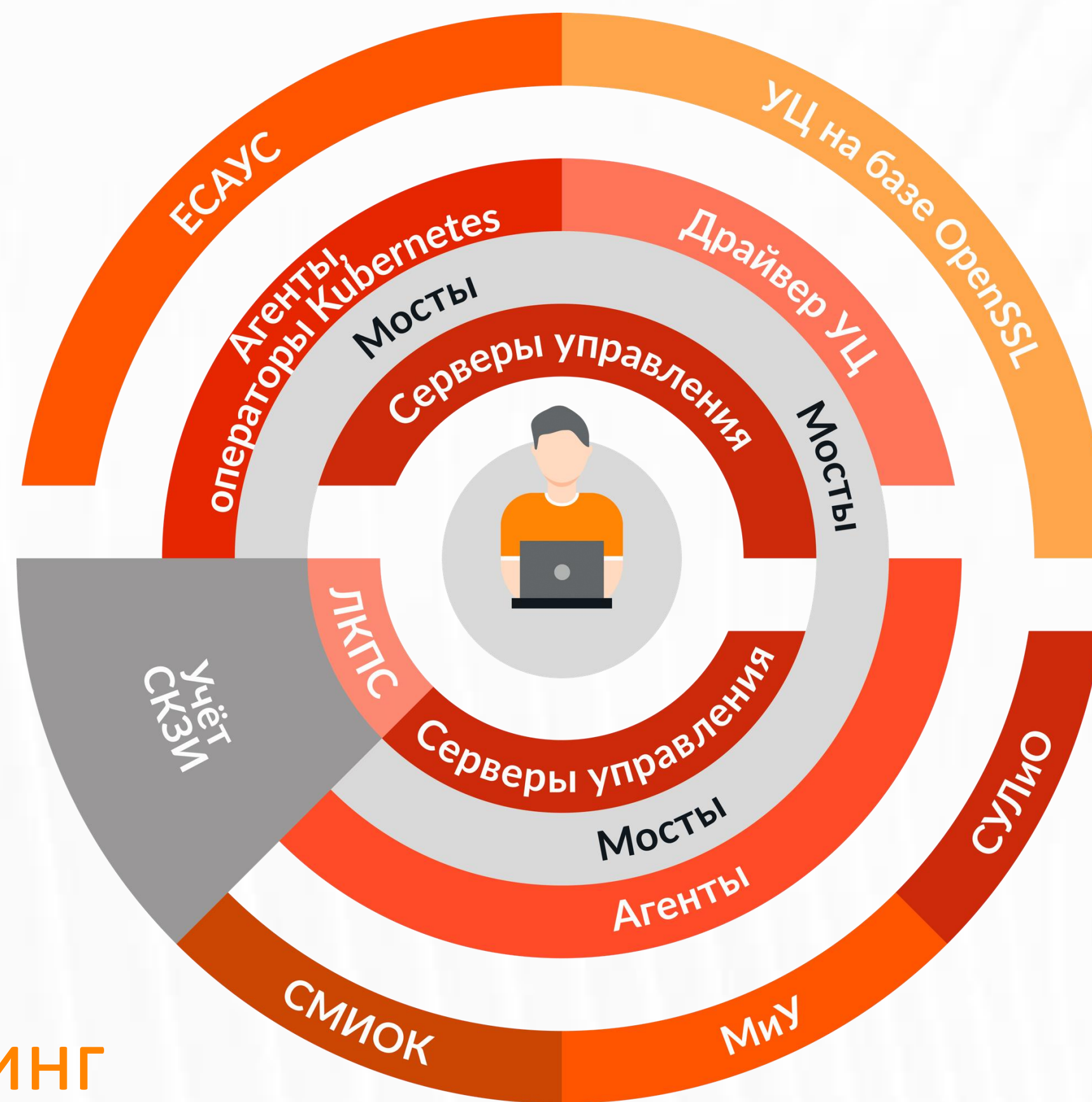
Отмена | Сохранить

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

