CLEARWAY INTEGRATION

Простое решение по предотвращению утечек через периферийные устройства

Александр Суховей
«Клируэй Текнолоджис»

CLEARWAY INTEGRATION

Инсайдерские атаки

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

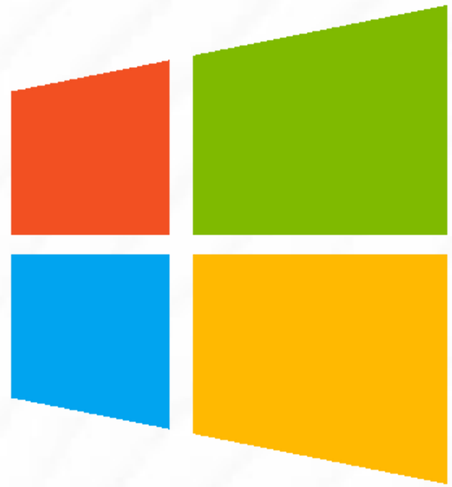
Масштабы

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

CLEARWAY INTEGRATION

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

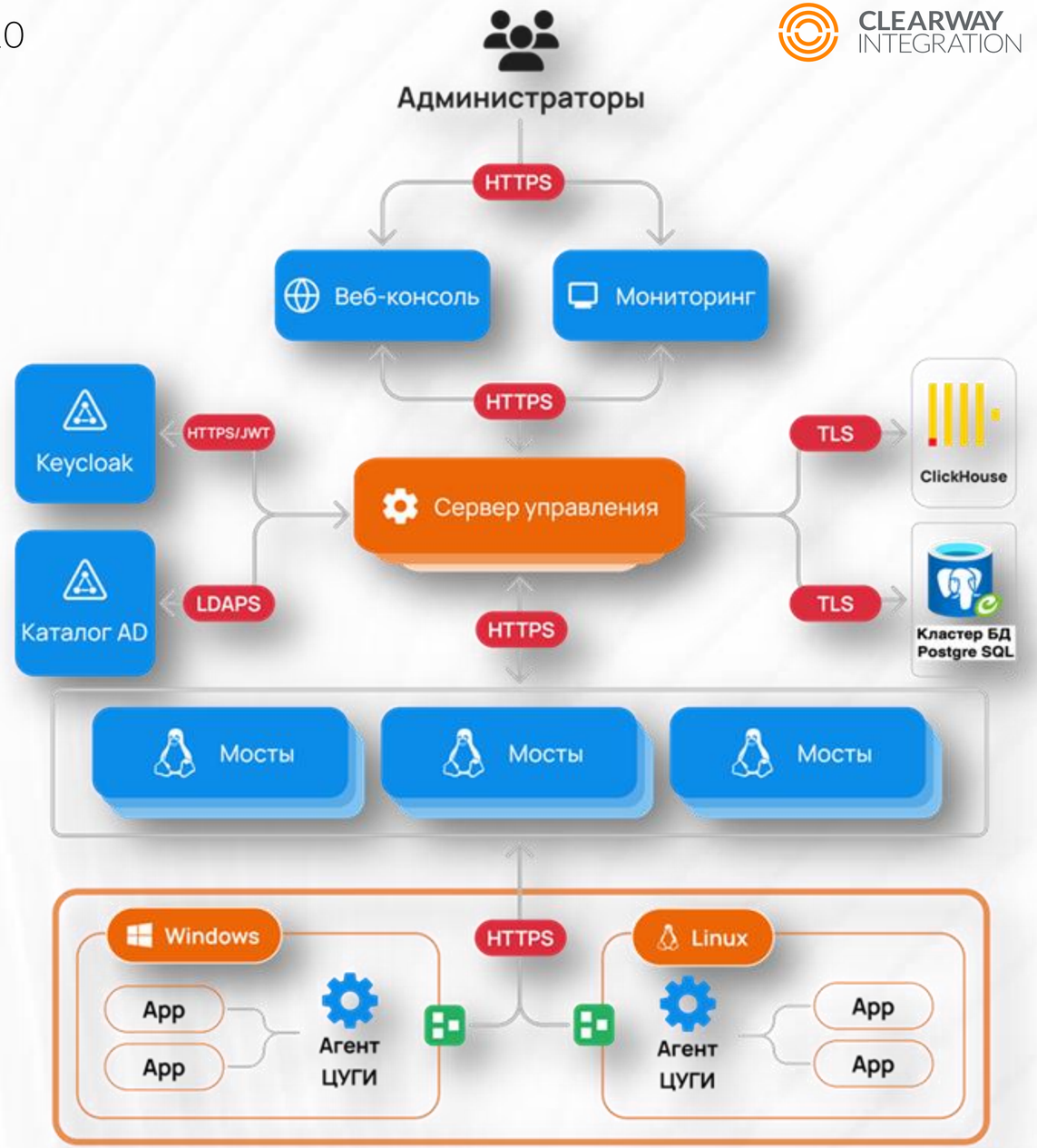


CLEARWAY INTEGRATION

КСУ: Общая архитектура

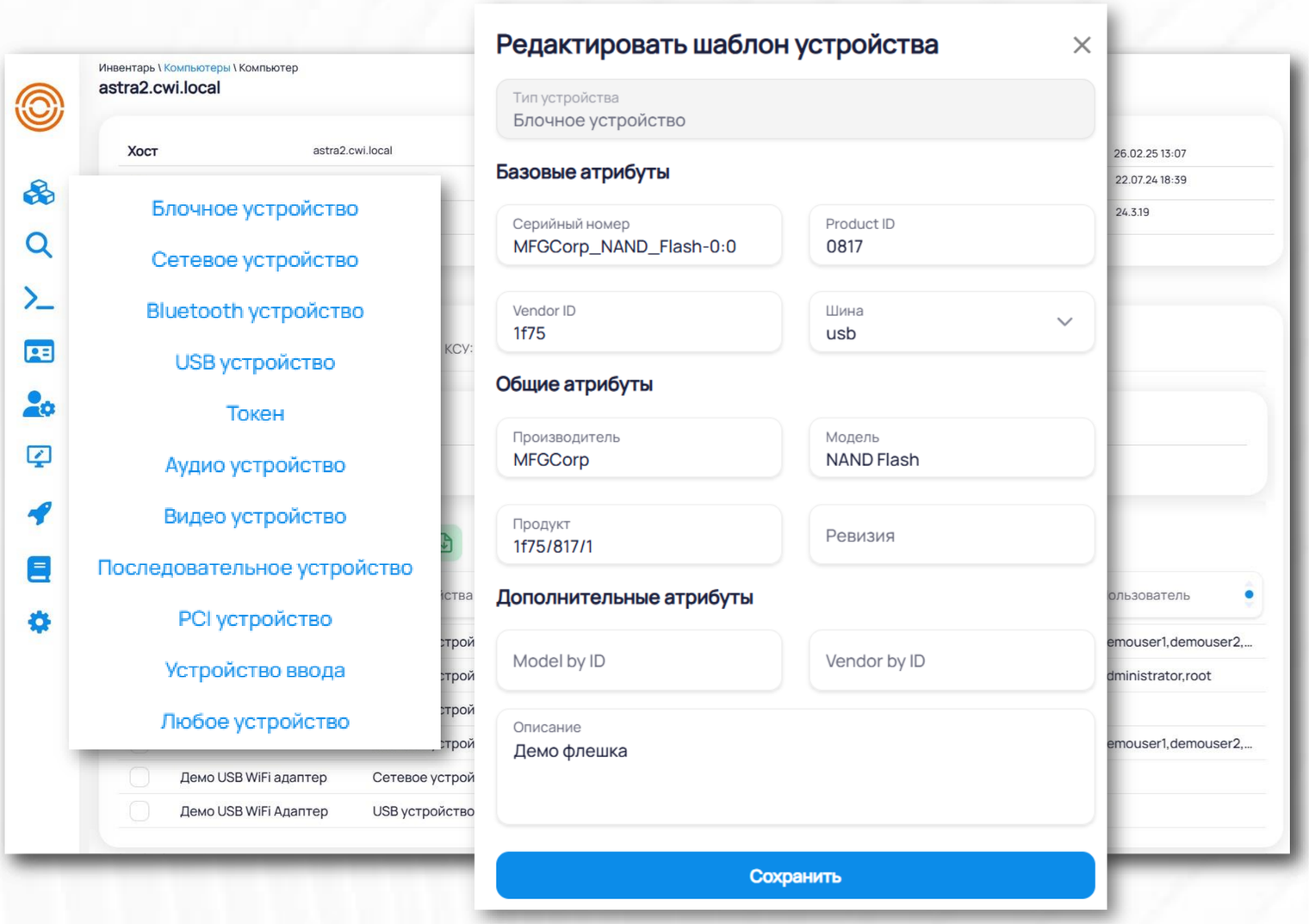
Система контроля съёмных устройств

- 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)



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 Шаблонов

>1 700 Правил КСУ

Нагрузка

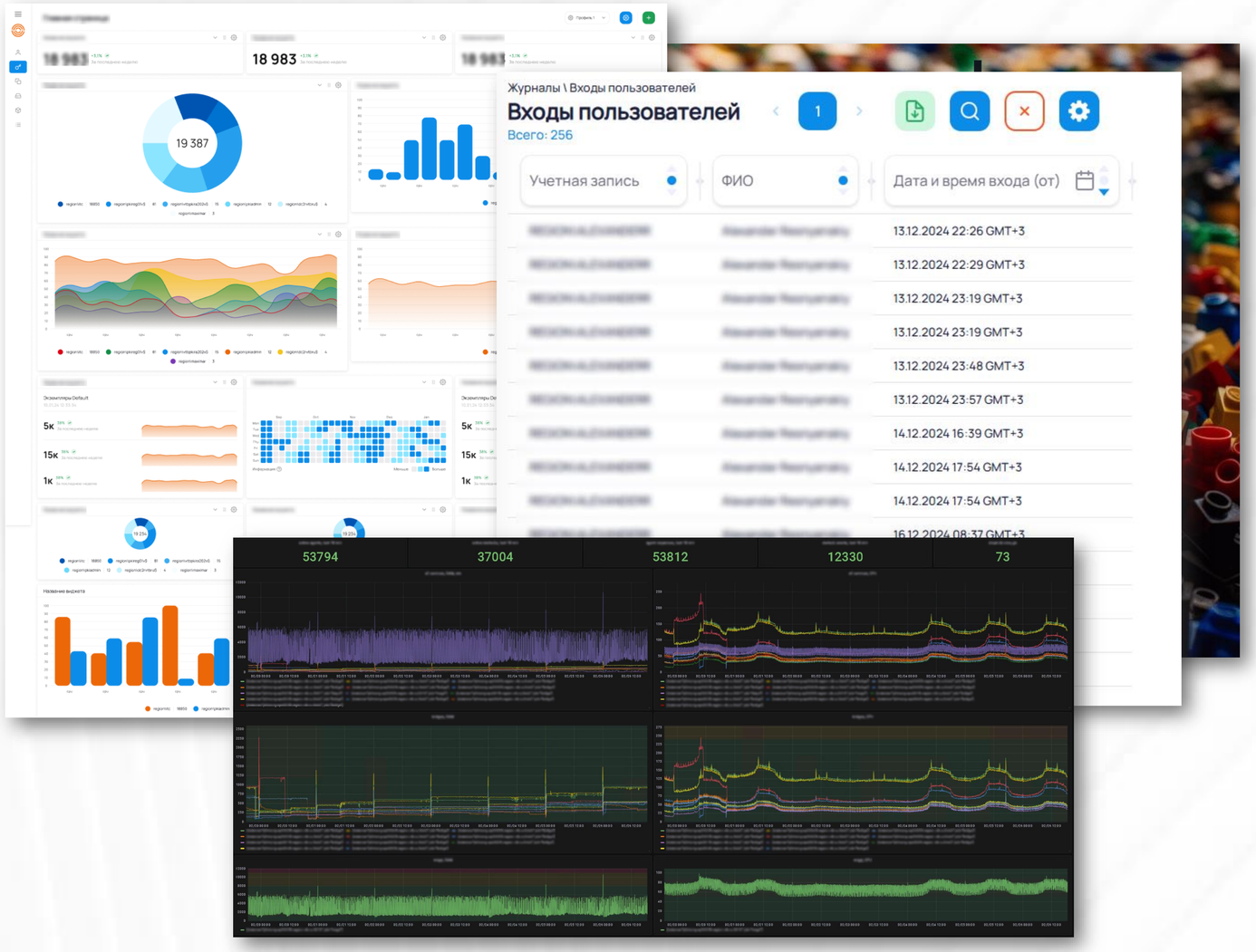
>100млн
Событий контроля доступа с начала эксплуатации

>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



Всё?

МиУ

Инвентариз

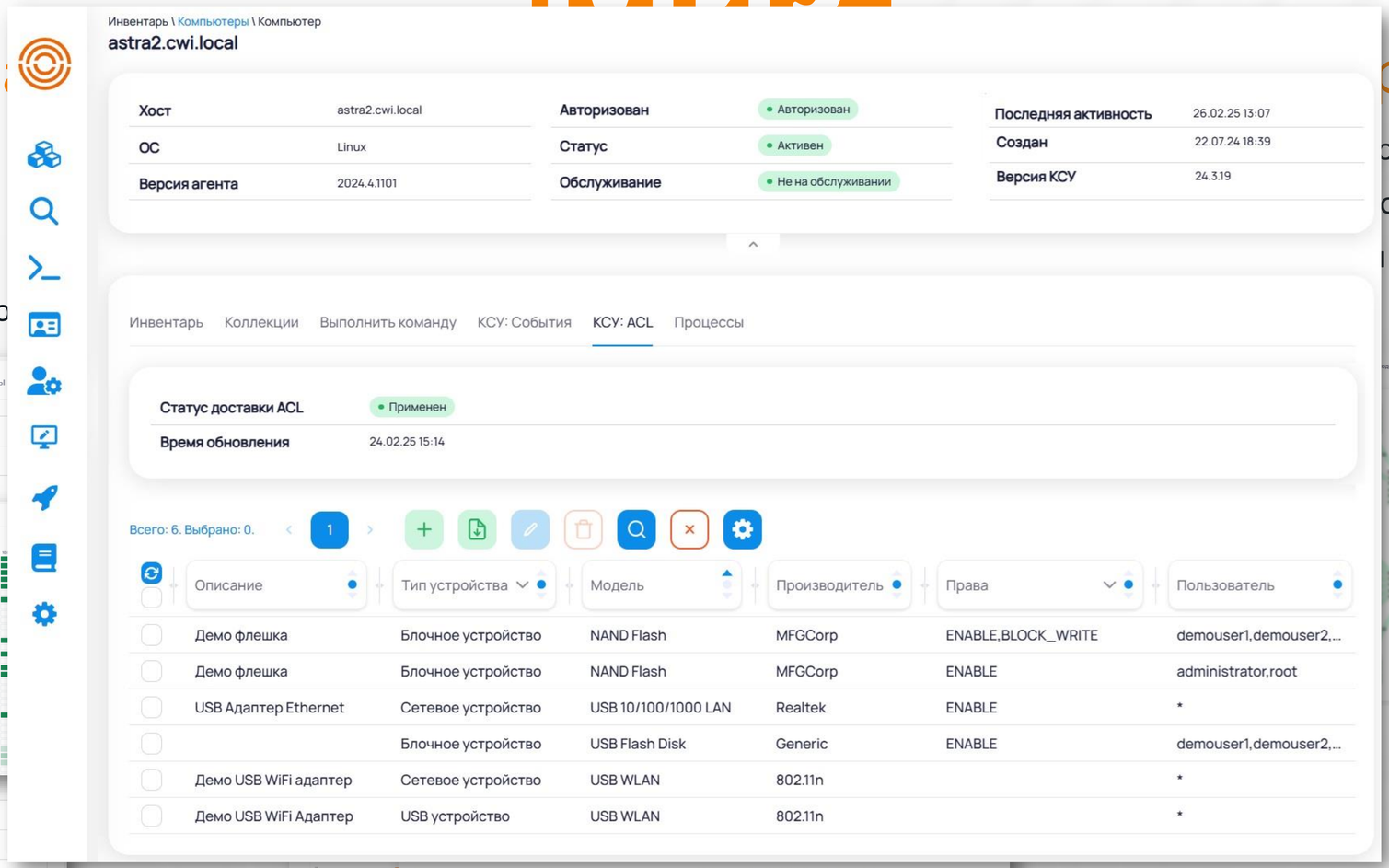
- Оборудование
- Windows, Linux, ПО
- Безопасность
- Сеть, службы катало

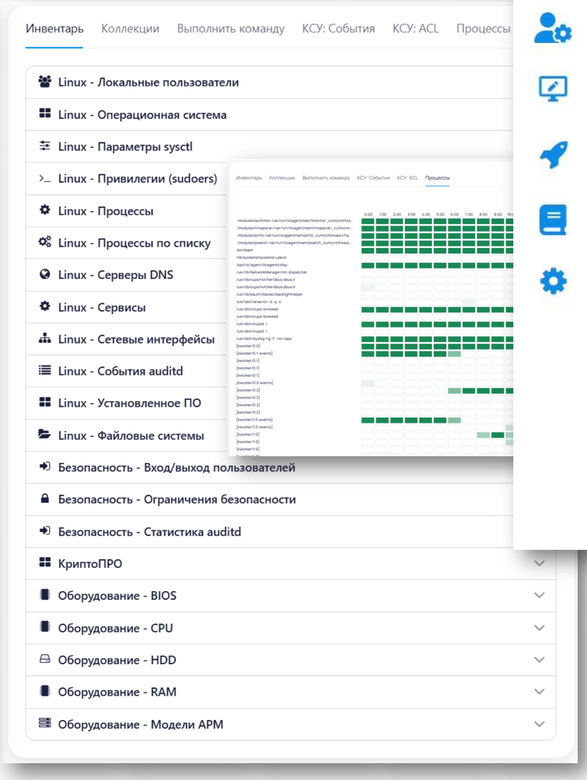
равление

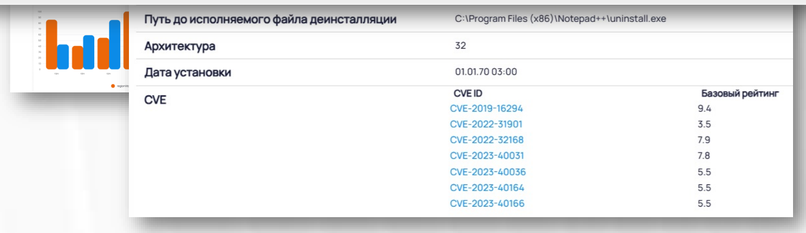
овка ПО и обновлений

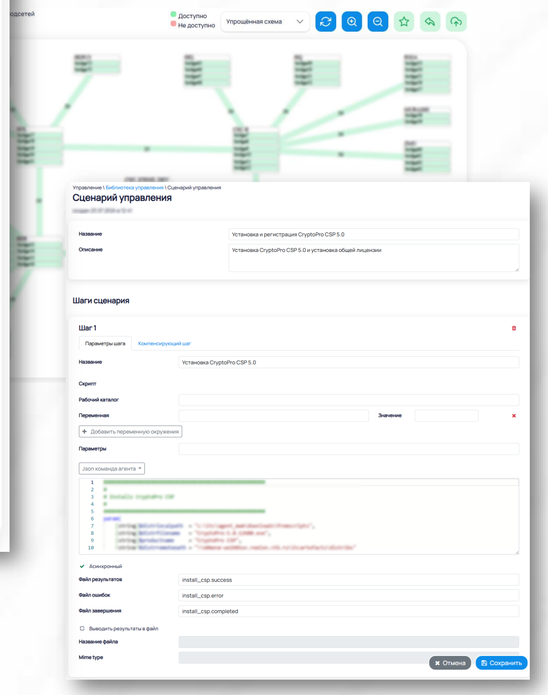
овые политики и Workflow

и подсети









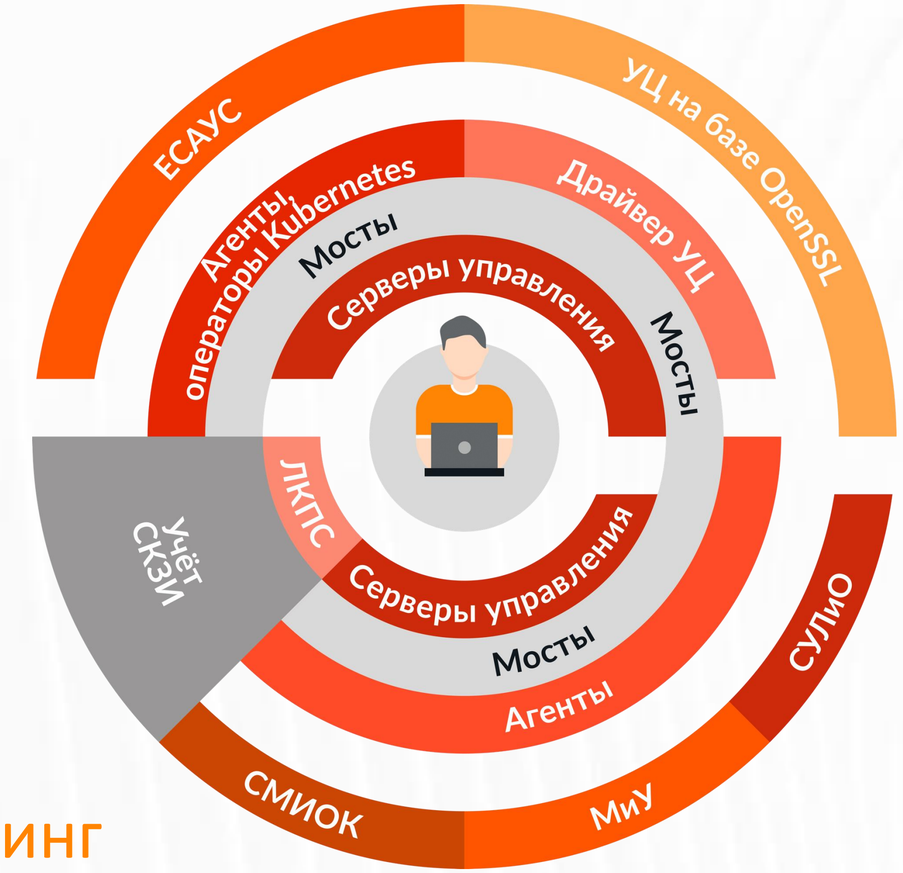
CLEARWAY INTEGRATION

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

CLEARWAY INTEGRATION

Москва, улица Магистральная 4-я, д. 11

info@clearwayintegration.com

+7 495 142 13 15

clearwayit.ru