

Мониторинг и удаленное управление АРМ (МиУ)

Александр Суховей

Владелец продукта



это централизованная инвентаризация, мониторинг и управление функциями APM и серверов



Инвентаризация инфраструктуры

собирает информацию с APM, серверов и ИТ-служб об оборудовании, настройках и безопасности



Автоматическая аналитика и мониторинг инфраструктуры

выявляет аномалии конфигурации, активности процессов и пользователей



Управление конфигурацией

с помощью установки ПО и обновлений, интерактивных команд, групповых политик и многошаговых сценариев



Контроль съемных устройств

для защиты от утечек данных и от установки вредоносных программ



Удаленная поддержка

с подключением к рабочему столу пользователей и системой управления задачами службы поддержки

Почему возникла **потребность**

1

Высокая нагрузка на ИТ и поддержку

- Большое количество ручных операций
- Долгое ожидание АРМ для новых сотрудников
- Простои сотрудников из бизнес-подразделений из-за несовместимых версий ПО, ошибок конфигураций и сбоев

2

Неполное расследование ИБ-инцидентов

- Отсутствие контроля и централизованного применения настроек ИБ
- Большое время расследования инцидентов
- Отсутствие понимания первоисточника распространения вредоносного ПО

3

Репутационные и экономические риски

- Простои ИТ и бизнес-систем из-за аварий и кибер-атак
- Потеря выручки из-за недоступности систем для клиентов и нарушения сроков контрактов
- Несоответствие требованиям регуляторов, риск штрафов

Проблемы, которые **решает МиУ**

1

Нет прозрачности ИТ инфраструктуры

2

Недостаточный аудит событий инфраструктуры и действий пользователей

3

Отсутствие единой точки управления и контроля парка АРМ и серверов

4

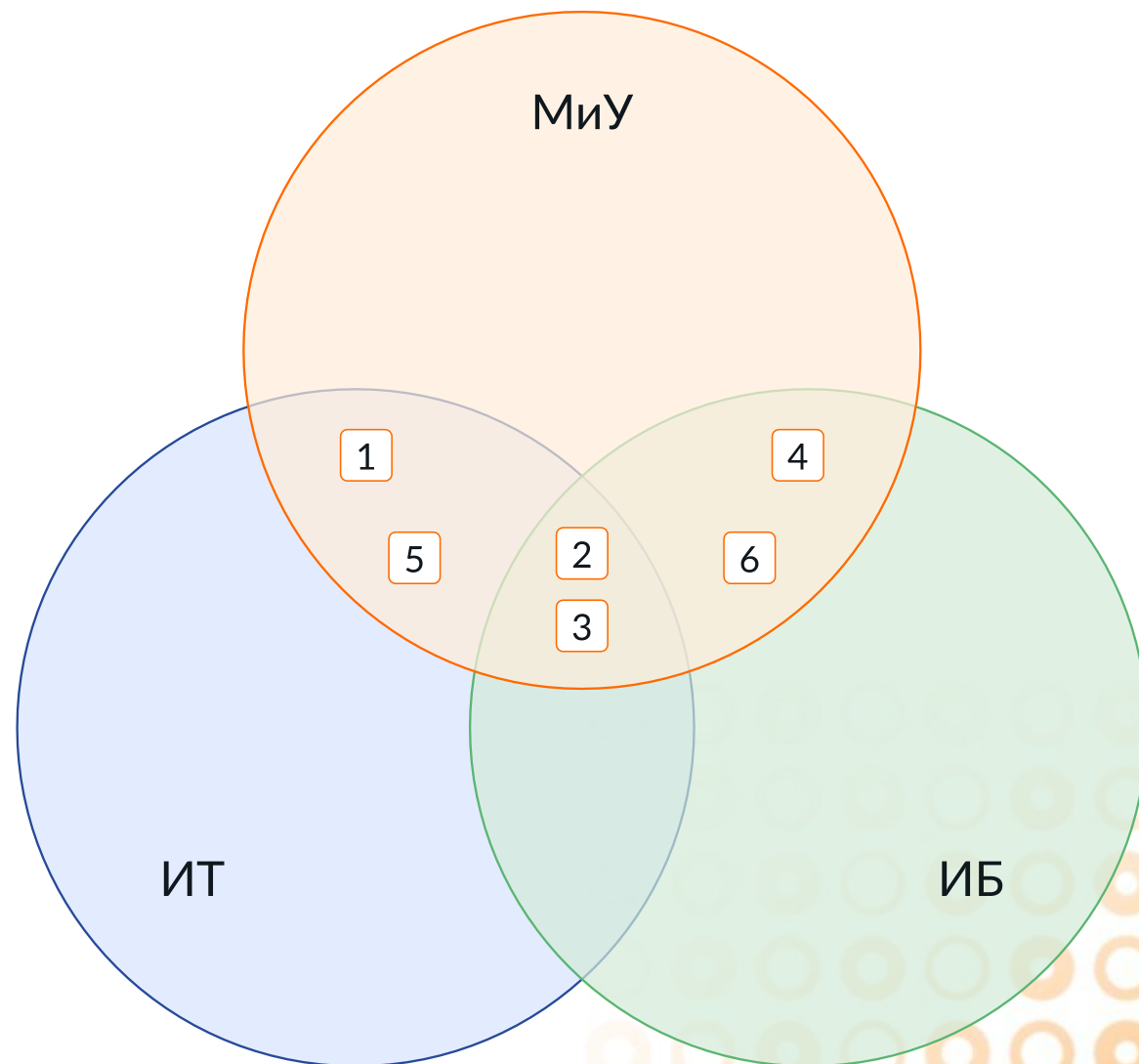
Отсутствие или недостаточность контроля безопасности АРМ, серверов, сетей

5

Трудоёмкие массовые операции конфигурирования АРМ, установки и обновления ПО

6

Риски утечек информации, отсутствие контроля съемных устройств



Цели продукта



Реагировать на угрозы

Но не уменьшать скорость применения изменений –

Time to Market



Повышать скорость изменений

Увеличивать скорость внедрения новых систем и политик в области ИТ/ИБ путем автоматизации задач управления



Контролировать риски безопасности

Контролировать доступ к съемным устройствам и безопасность в режиме реального времени



Поддерживать пользователей

Управлять заявками, предоставлять удаленную поддержку пользователей с подключением к рабочему столу

Преимущества использования МиУ

1

Единое место ведения
Отображение всех инвентарей
с полным перечнем набора
атрибутов

2

Контроль съёмных устройств
Подключение оборудования
под контролем МиУ

3

Удаленная поддержка АРМ
с контролем рабочего стола
без прямого подключения
к АРМ

4

Аналитика и мониторинг АРМ
Контроль активности
пользователей, аудит
событий

5

**Контроль действий
пользователей**
Управление настройками АРМ,
установка ПО

6

**Удаленная установка
и обновление ПО**
в автоматическом или ручном
режиме

7

Формирование отчетов и
Подготовка отчетов
и графических панелей
(дашборды)

8

Контроль аномалий
Ведение списков эталонных
конфигураций, мониторинг
отклонений от эталонов

9

**Своевременные
уведомления**
о событиях в инфраструктуре

Обзор архитектуры



МиУ: Общая архитектура

Единый Агент ЦУГИ — устанавливается на удаленный хост для управления и инвентаризации, сбора данных и передачи их на центральный сервер

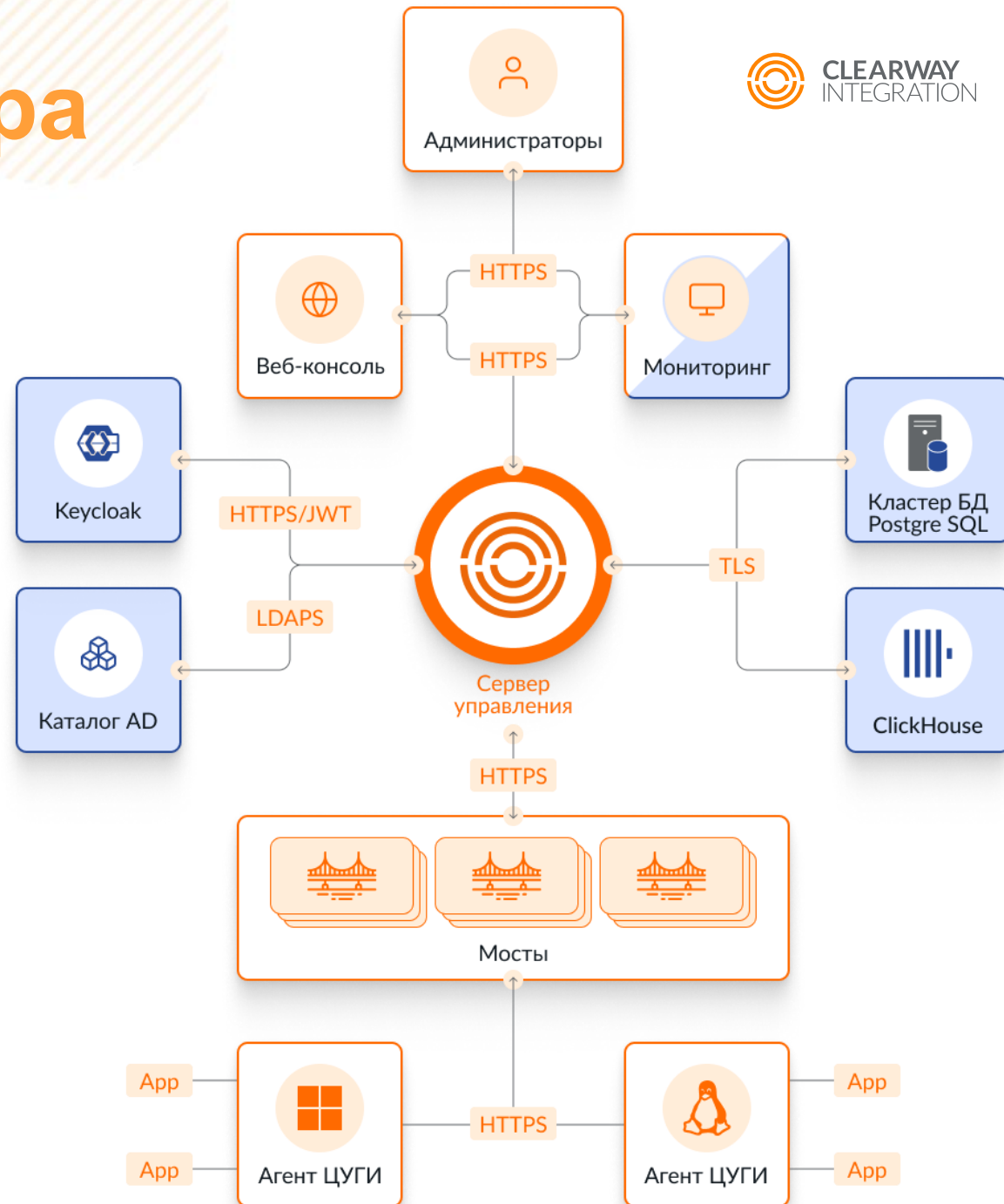
Мосты — принимают сообщения от агентов, публикуют задания для агентов ЦУГИ. Могут объединяться в цепочки; агенты МиУ автоматически выбирают оптимальные мосты

Сервер управления — один или несколько серверов с установленными сервисами расчета и инвентаризации, брокера сообщений и диспетчера агентов

СУБД PostgreSQL и ClickHouse — системы управления базами данных для хранения данных конфигурации, событий и больших объемов инвентаризационной информации

KeyCloak, интегрированный с AD/ALD Pro/SAMBA — авторизует операторов МиУ на основе доменных учетных записей, сопоставляет ролевую модель МиУ доменным группам

Веб-консоль управления и мониторинга — графический интерфейс МиУ и панелей структурированного мониторинга с поддержкой моделей здоровья и интеграции с внешним мониторингом



МиУ: Сервер управления

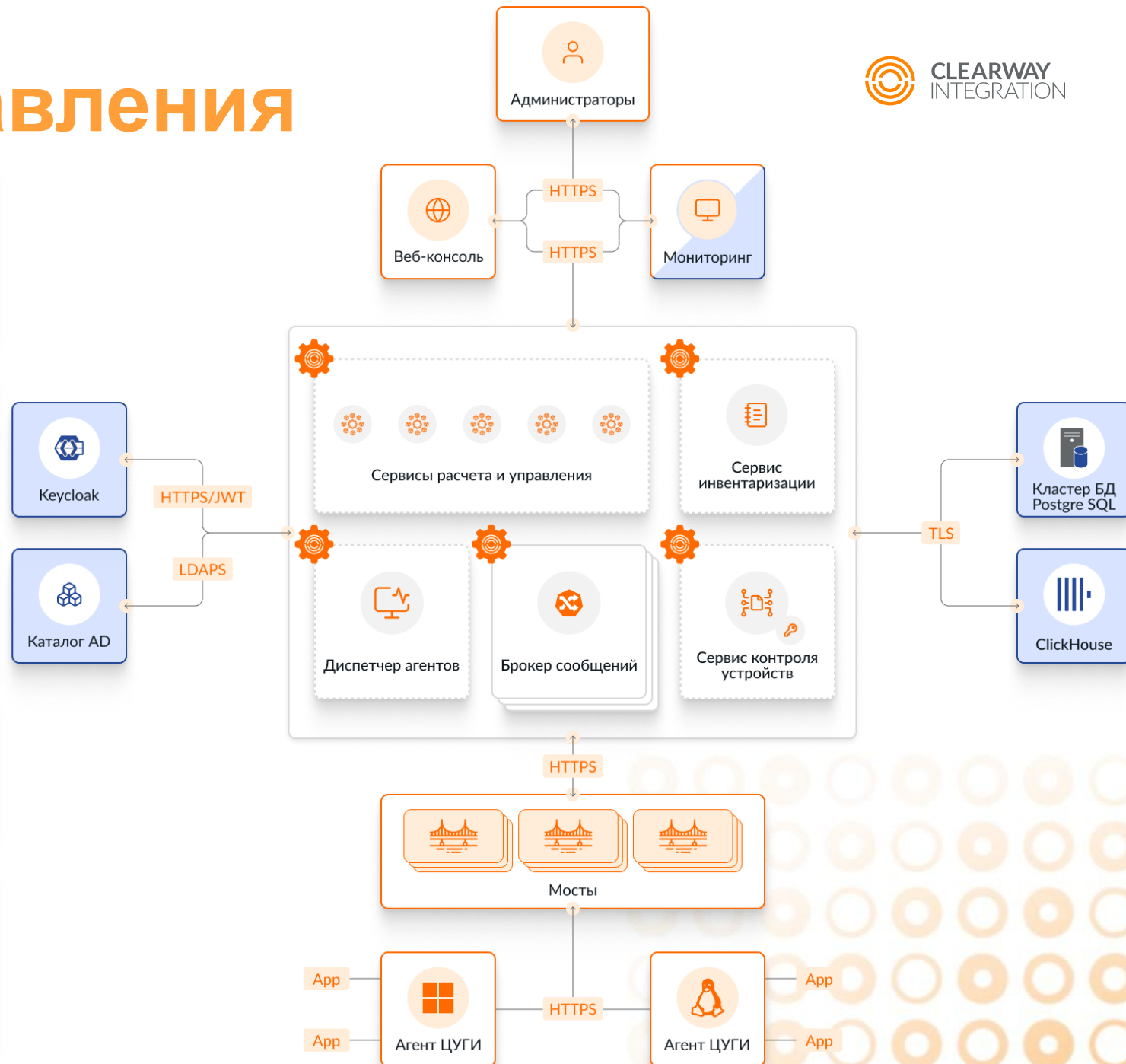
Диспетчер агентов — обеспечивает централизованное администрирование, мониторинг и координацию работы агентов, а также сбор и обработку данных

Брокер сообщений — обеспечивает внутренние коммуникации МиУ, асинхронность, надежность и снижение связанности компонентов

Сервис контроля устройств — отвечает за централизованное хранение, управление и применение правил контроля доступа к съемным устройствам

Сервис инвентаризации — обрабатывает данные инвентаризации, динамические коллекции и отчеты об уязвимостях CVE

Сервисы расчета и управления — выполняют дополнительную обработку отчетов, событий и взаимодействие с внешними системами



МиУ: Zero Trust

Агент:

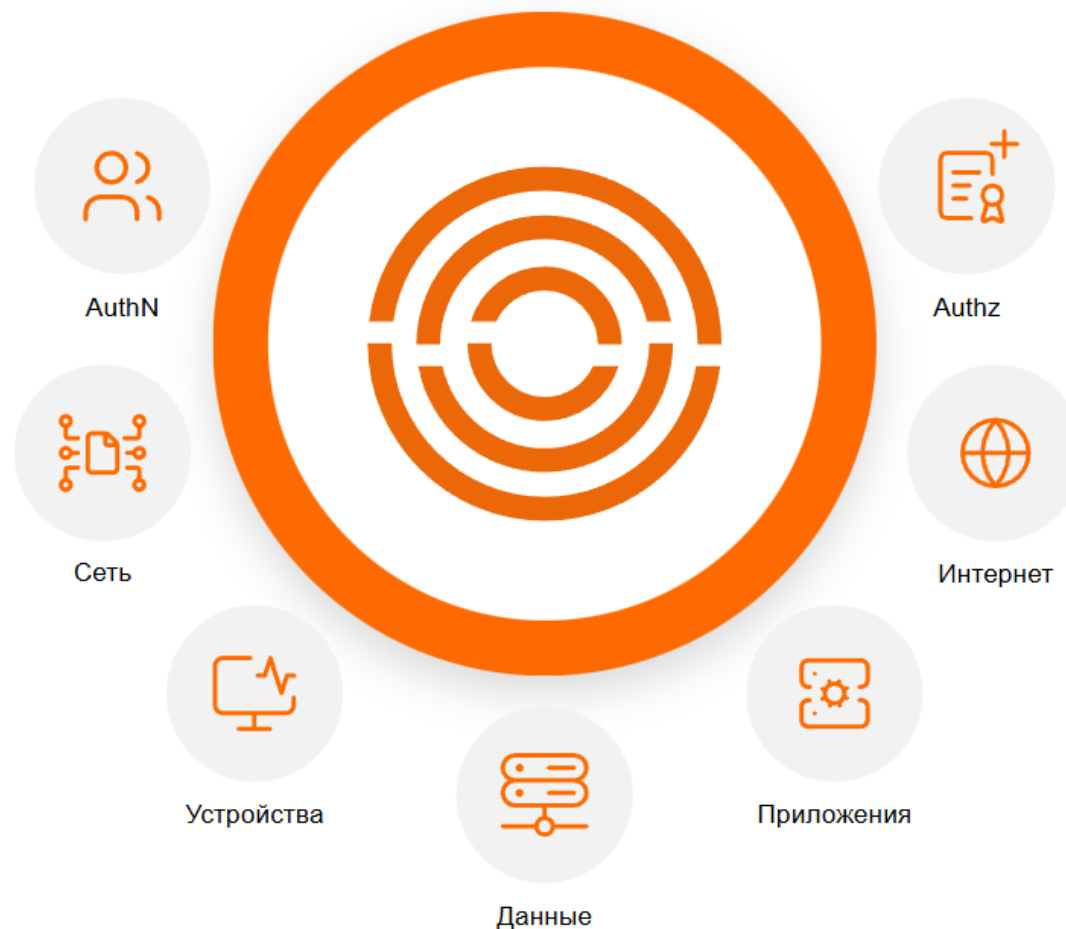
- контексты безопасности агента и модулей
- аутентификация и защита коммуникаций – корпоративные сертификаты
- взаимодействие снизу вверх – к агенту извне никто не обращается, на нем не открыты порты для взаимодействия
- защита конфигурации и данных (подпись ACL)

Сервисы:

- ТУЗ
- Защита секретов (шифрование конфиг. файлов, EXC)
- Защита коммуникаций TLS (внутренних и внешних)

Изоляция и автономия:

- Гранулярная ролевая модель
- Единый агент, множественные серверы управления
- Ограничивающие коллекции



МиУ: Масштабируемость

Минимальная конфигурация (до 5 000 агентов)

Предназначена для пилотного стенда или тестовой среды или малых организаций

Размещение:

- 1 сервер МиУ
- 1 сервер PostgreSQL (может быть размещён совместно)
- 1 сервер ClickHouse
- 1 сервер KeyCloak

Особенности:

- отсутствует отказоустойчивость
- подходит для пилотных внедрений.

Средняя конфигурация (5 000 – 50 000 агентов)

Предназначена для промышленной эксплуатации

Размещение:

- 2 сервера МиУ (фронтенд, бэкэнд)
- 2 и более Моста
- 2 узла PostgreSQL (primary + replica)
- 2 узла ClickHouse
- 1 сервер Keycloak
- 1 сервер мониторинга

Обеспечивается:

- кластерная репликация
- распределение нагрузки

Отказоустойчивая конфигурация (от 50 000 до 200 000 агентов)

Используется в высоконагруженных или критичных средах)

Размещение:

- 3 и более серверов МиУ (распределение сервисов)
- 10 и более Мостов
- отказоустойчивые СУБД
- 1 сервер Keycloak
- 1 сервер мониторинга

Дополнительно:

- географическое резервирование (опционально);
- резервное копирование в отдельный контур

Функции: Инвентаризация

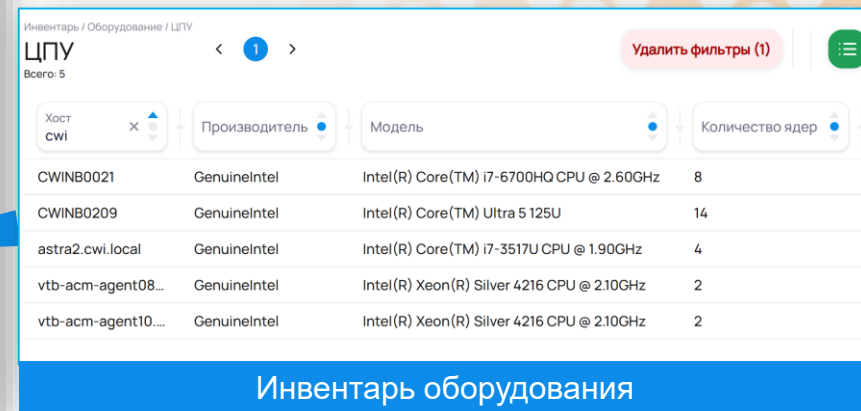
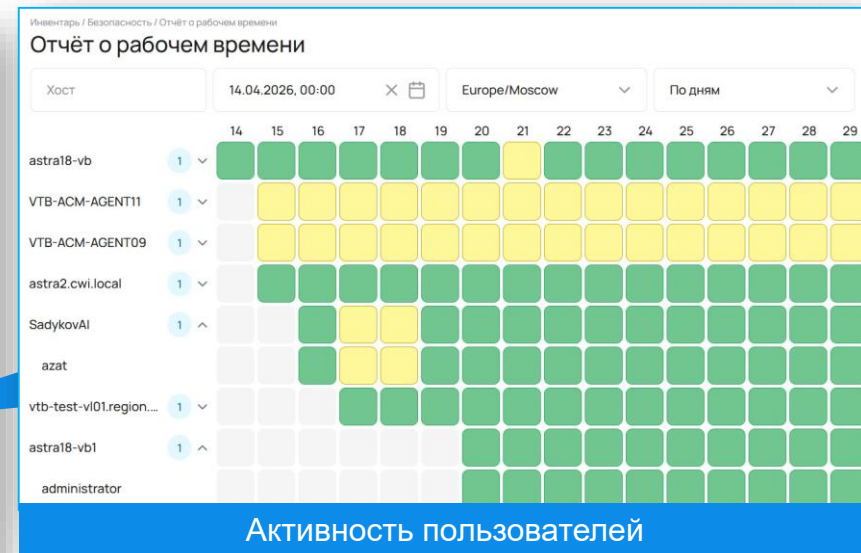
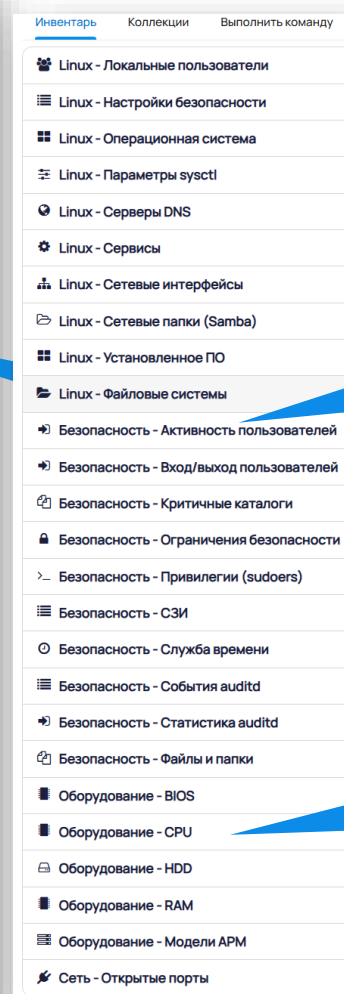
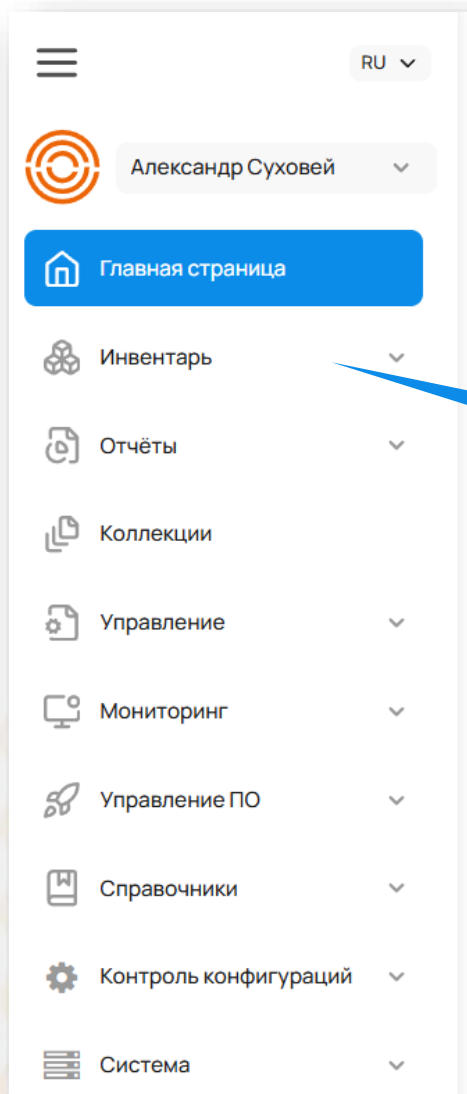


Функции: Инвентаризация

Агентская инвентаризация

с помощью установленного агента МиУ:

- **ОС** — версия, настройки, политики, системные сервисы
- **ПО** — состав, версии и параметры, статус обновления, наличие портативных и устаревших версий
- **Оборудование** — центральные процессоры, сетевые карты, модули памяти и др.
- **Безопасность** — настройки ОС, ПО и учетных записей, делегированные полномочия
- **Активность** — тепловые карты активности пользователей и процессов, события аудита и автоматического запуска



The screenshot shows the 'Инвентарь оборудования' (Hardware Inventory) section of the Clearway Integration web interface. The table displays a list of hardware components, including CPU, RAM, and HDD, with filters for 'Хост' (Host), 'Производитель' (Manufacturer), 'Модель' (Model), and 'Количество ядер' (Number of cores). The table is titled 'ЦПУ' (CPU) and shows a total of 5 items. The table includes a 'Удалить фильтры (1)' (Remove filters (1)) button and a 'Сбросить' (Reset) button.

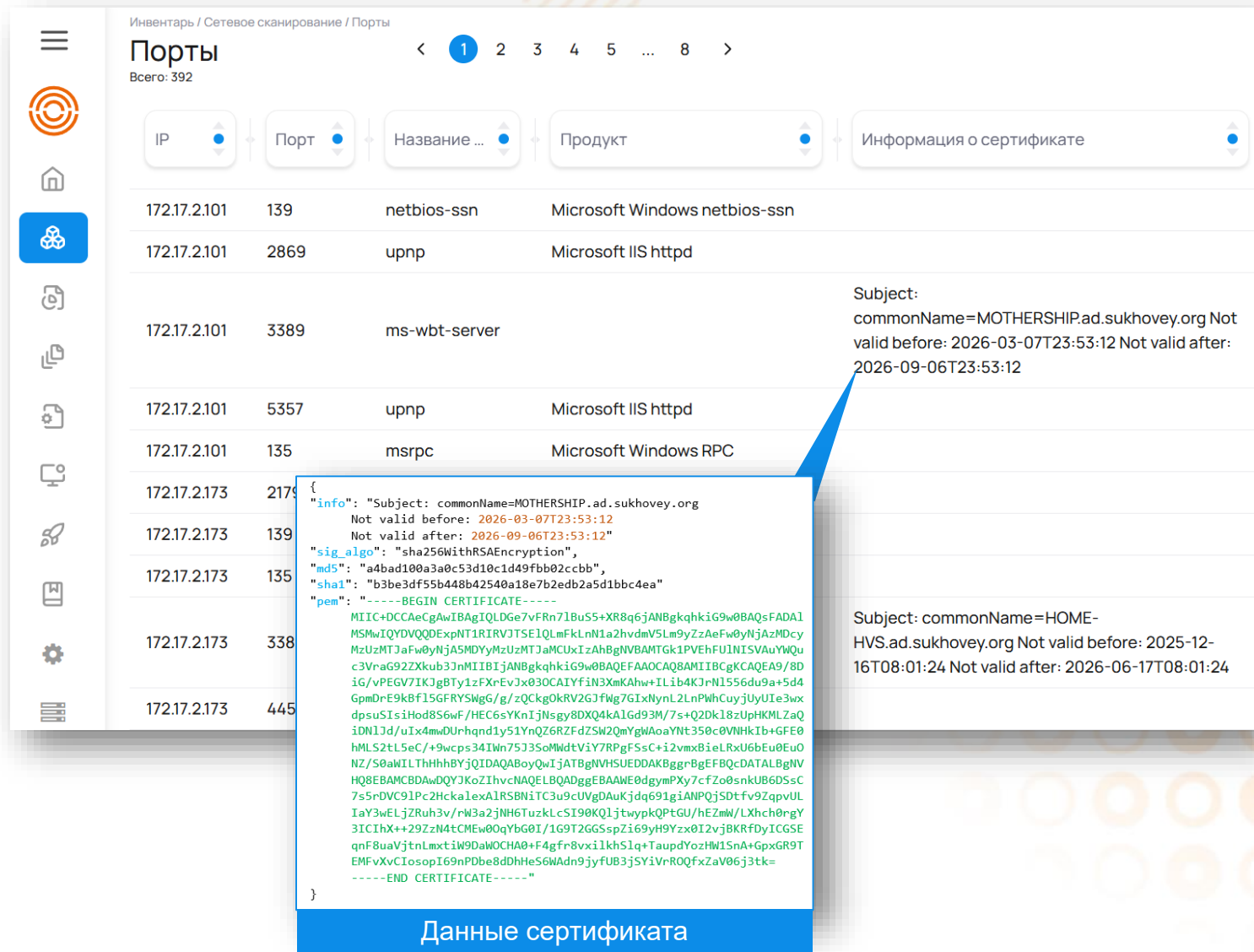
Хост	Производитель	Модель	Количество ядер
CWINB0021	GenuineIntel	Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz	8
CWINB0209	GenuineIntel	Intel(R) Core(TM) Ultra 5 125U	14
astra2.cwi.local	GenuineIntel	Intel(R) Core(TM) i7-3517U CPU @ 1.90GHz	4
vtb-acm-agent08...	GenuineIntel	Intel(R) Xeon(R) Silver 4216 CPU @ 2.10GHz	2
vtb-acm-agent10...	GenuineIntel	Intel(R) Xeon(R) Silver 4216 CPU @ 2.10GHz	2

Функции: Инвентаризация

Безагентская инвентаризация

опрашивает сетевые устройства и внешние сервисы без установки агента МиУ на серверы и устройства:

- **Устройства в сети** — сетевые службы на серверах, АРМ, коммуникационном и офисном оборудовании
- **Сертификаты сетевых служб** — используемые сетевыми сервисами цифровые сертификаты
- **Службы каталога** — пользователи, группы, компьютеры, контейнеры, опубликованные сертификаты в службах LDAP, таких как Microsoft AD, ALD Pro, FreeIPA, Samba 4
- **Сертификаты в каталогах LDAP** — опубликованные в службах каталога доверенные корневые и персональные сертификаты



Инвентарь / Сетевое сканирование / Порты

Порты

Всего: 392

IP	Порт	Название ...	Продукт	Информация о сертификате
172.17.2.101	139	netbios-ssn	Microsoft Windows netbios-ssn	
172.17.2.101	2869	upnp	Microsoft IIS httpd	
172.17.2.101	3389	ms-wbt-server		Subject: commonName=MOTHERSHIP.ad.sukhovey.org Not valid before: 2026-03-07T23:53:12 Not valid after: 2026-09-06T23:53:12
172.17.2.101	5357	upnp	Microsoft IIS httpd	
172.17.2.101	135	msrpc	Microsoft Windows RPC	
172.17.2.173	217			{ "info": "Subject: commonName=MOTHERSHIP.ad.sukhovey.org Not valid before: 2026-03-07T23:53:12 Not valid after: 2026-09-06T23:53:12" "sig_algo": "sha256WithRSAEncryption", "md5": "a4bad100a3a0c53d10c1d49fbb02ccbb", "sha1": "b3be3df55b448b42540a18e7b2edb2a5d1bbc4ea" "pem": "-----BEGIN CERTIFICATE----- MIIC+DCCAeCgAwIBAgIQLDGe7vFRn71BuS5+XR8q6jANBgkqhkiG9w0BAQsFADA1 MSMwIQYDVQQLExpNTIRVJTSElQLmFkLnN1a2hvdmV5Lm9yZzAeFw0yNjAzMDcy MzUzMjIaFw0yNjAzMDcyMzUzMjIaMCUxIzAhBgNVBAMTGk1PVEhFU1NISVAAUyWQu c3VraG92ZXkub3JnMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA9/8D iG/vPEGV7IKJgBTy1zFXrEvJx030CAIYfIN3XmKAhw+ILib4KJrN1556du9a+5d4 GpmDrE9kBf15GFRYSWgG/g/zQCKgOkRV2GJfwg7GIxNynL2LnPWhCuyjUyUIE3wx dpsuSIsiHod8S6wF/HEC6sYKnIjNsgy8DXQ4kAlGd93M/7s+Q2Dk18zUpHkMLZaQ iDN1Jd/uIx4mw0Urhqnd1y51YnQZ6RZFdzSW2QmYgWAoaYNT350c0VNHkIb+GFE0 hML52tL5eC/+9wcp34Iwn75J35oMwdtViY7RPGFsC+i2vmxBieLRxU6bEu0Eu0 NZ/S0aWILThHhBYjQIDAQABoYQwIjATBgNVHUUEDDAKBgggrBgEFBQcDATAALBgNV HQ8EBAMCBDAwDQYJKoZIhvcNAQELBQADggEBAAME0dgympXY7cfZo0snkUB6DSuL 7s5rDVC91Pc2HckalexAlRSBNiTC3u9cUVgDAuKjddq691giANPQjSDtFv9ZqpVUL IaY3wELjZRUh3v/rW3a2jNH6TuzklcSI90KQ1jtwypkQPTGU/hEZmW/LXhch0rGY 3IC1hX++29ZzN4tCMEw0qYbG0I/1G9T2GG5spZi69yH9Yzx0I2vjBKRfDyICGSE qnF8uaVjtnLmxtiW9DaMOCHA0+F4gfr8vxlkh51q+TaupYozHW15nA+GpxGR9T EMFvXvCIosopI69nPDbe8dDHHeS6WAdn9jyFUB3jSYiVrRoQfxZaV06j3tk= -----END CERTIFICATE-----" }
172.17.2.173	139			
172.17.2.173	135			
172.17.2.173	338			Subject: commonName=HOME- HVS.ad.sukhovey.org Not valid before: 2025-12- 16T08:01:24 Not valid after: 2026-06-17T08:01:24
172.17.2.173	445			

Данные сертификата

Функции: Инвентаризация

Используйте более 70 инвентарей по умолчанию

Создавайте новые и дополняйте существующие инвентари в графическом конструкторе

Автоматически группируйте компьютеры в динамические коллекции на основе данных инвентаризации

Оптимизируйте объемы данных с помощью тонких настроек:

- частота выполнения
- глубина хранения
- передача только изменений

Коллекции

Всего: 12. Выбрано: 0

Название	Количество	Тип	Дата создания	Автор
☐ Бухгалтерия	3	Статическая	01.04.2026 14:05:15	Nikita Enes
☐ Все компьютеры	24	Динамическая	11.03.2026 13:46:05	itc.module.wsmam
☐ Все компьютеры Linux	22	Динамическая	11.03.2026 13:46:05	itc.module.wsmam
☐ Все компьютеры Windows	10	Динамическая	11.03.2026 13:46:03	itc.module.wsmam
☐ Все серверы МиУ	6	Динамическая	11.03.2026 13:46:06	itc.module.wsmam
☐ Дашборд	10	Статическая	20.04.2026 10:24:57	Александр Суховой
☐ Дизайнеры	1	Статическая	07.04.2026 13:55:25	Anton Pavlov
☐ Кассиры	10	Динамическая	17.03.2026 15:51:39	Andrey Kaidalov
☐ Разработчики	1	Статическая	16.04.2026 15:58:01	Operator Novosibir...
☐ Тест - ОП	1	Статическая	01.04.2026 15:52:10	Александр Суховой
☐ Филиал СПб		Статическая	22.04.2026 14:59:53	Александр Суховой
☐ Хосты с				Александр Суховой

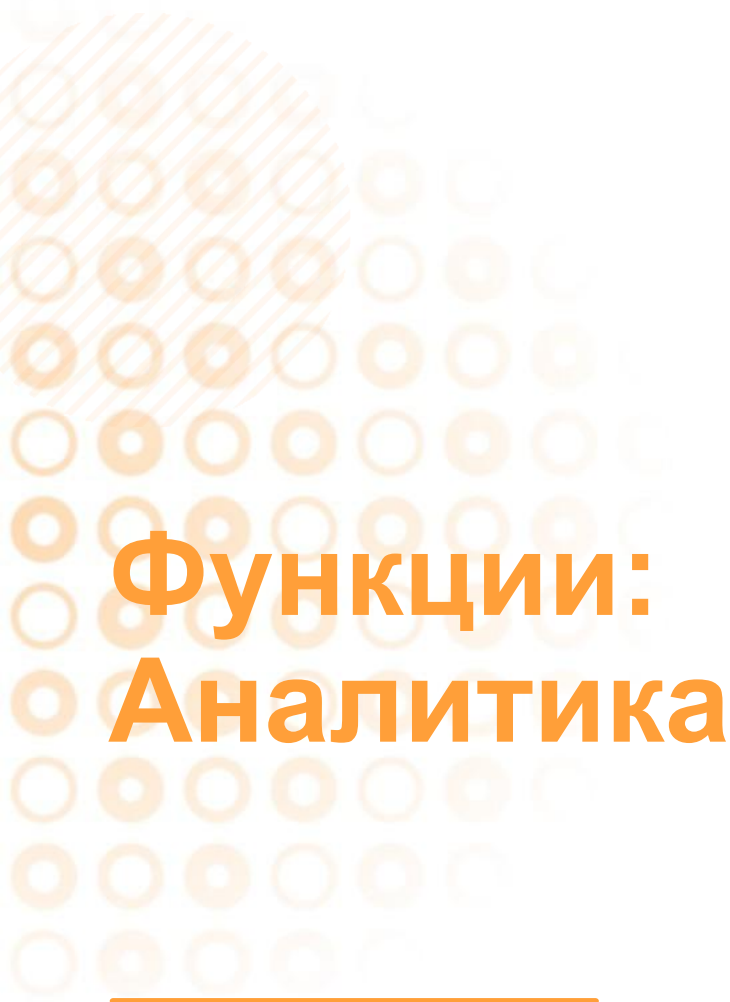
Запрос для формирования коллекции

и или

Инвентарь	Linux - Сервисы
Имя	содержит
Инвентарь	Linux - Сервисы
Имя	=
	itcdispd.service

Правила членства на основе инвентарей

=
!=
>
>=
<
<=
содержит
не содержит



Функции: Аналитика

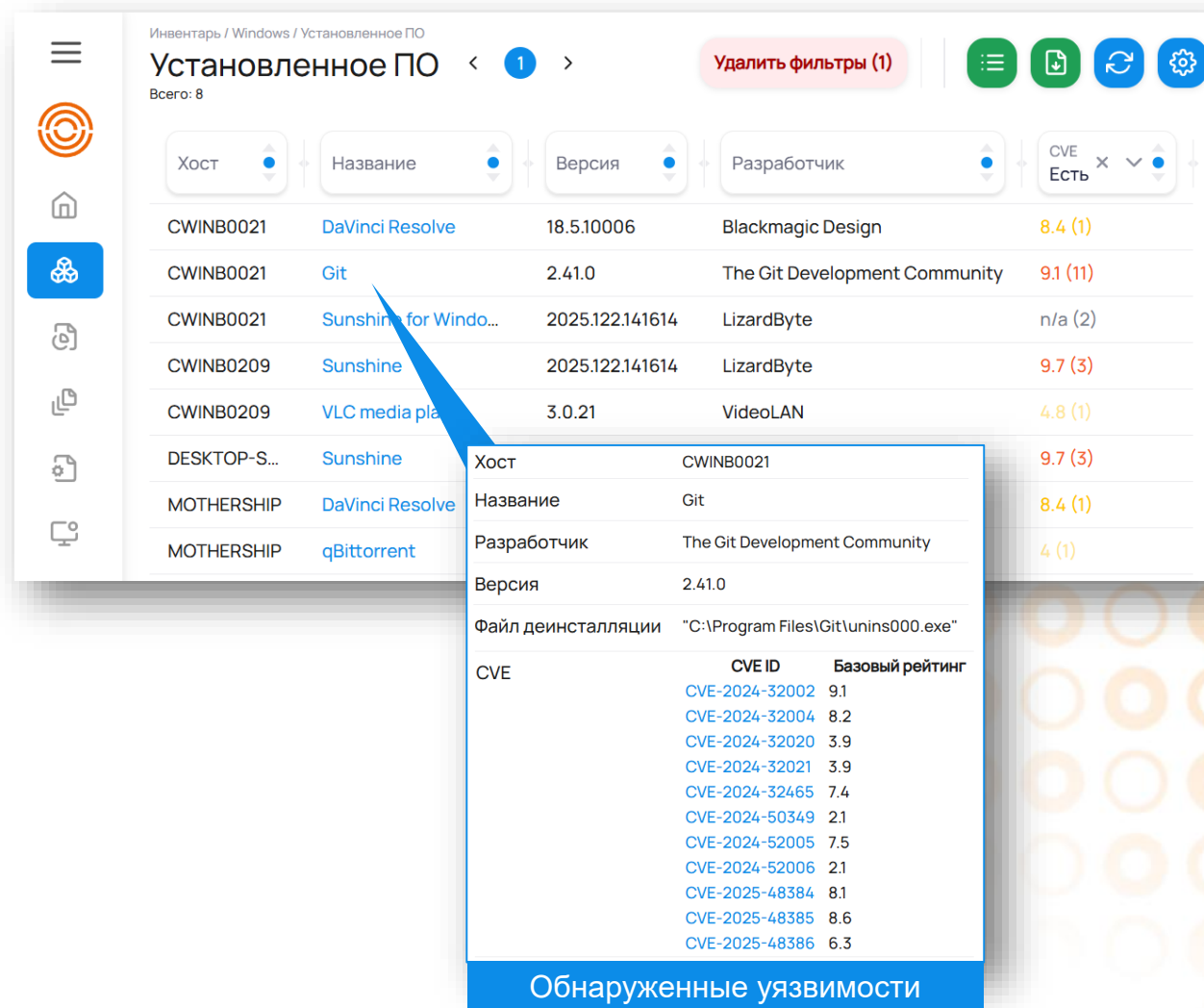


Функции: Аналитические

Уязвимости CVE

Выявляйте устаревшее и потенциально уязвимое ПО

- **База CVE** — самая популярная база уязвимостей ПО
- **Локальный справочник** — база уязвимостей автоматически загружается в МиУ и доступна локально
- **Автоматическое обновление** — загрузка с официального сайта CVE или сайта Клируэй
- **Автоматическое обнаружение** — выявленные уязвимости отмечаются в инвентаре установленного ПО Windows и Linux



Инвентарь / Windows / Установленное ПО

Установленное ПО

Всего: 8

Удалить фильтры (1)

Хост | Название | Версия | Разработчик | CVE

CWINB0021	DaVinci Resolve	18.5.10006	Blackmagic Design	8.4 (1)
CWINB0021	Git	2.41.0	The Git Development Community	9.1 (11)
CWINB0021	Sunshine for Windo...	2025.122.141614	LizardByte	n/a (2)
CWINB0209	Sunshine	2025.122.141614	LizardByte	9.7 (3)
CWINB0209	VLC media pla	3.0.21	VideoLAN	4.8 (1)
DESKTOP-S...	Sunshine			9.7 (3)
MOTHERSHIP	DaVinci Resolve			8.4 (1)
MOTHERSHIP	qBittorrent			4 (1)

Хост: CWINB0021

Название: Git

Разработчик: The Git Development Community

Версия: 2.41.0

Файл деинсталляции: "C:\Program Files\Git\unins000.exe"

CVE	CVE ID	Базовый рейтинг
	CVE-2024-32002	9.1
	CVE-2024-32004	8.2
	CVE-2024-32020	3.9
	CVE-2024-32021	3.9
	CVE-2024-32465	7.4
	CVE-2024-50349	2.1
	CVE-2024-52005	7.5
	CVE-2024-52006	2.1
	CVE-2025-48384	8.1
	CVE-2025-48385	8.6
	CVE-2025-48386	6.3

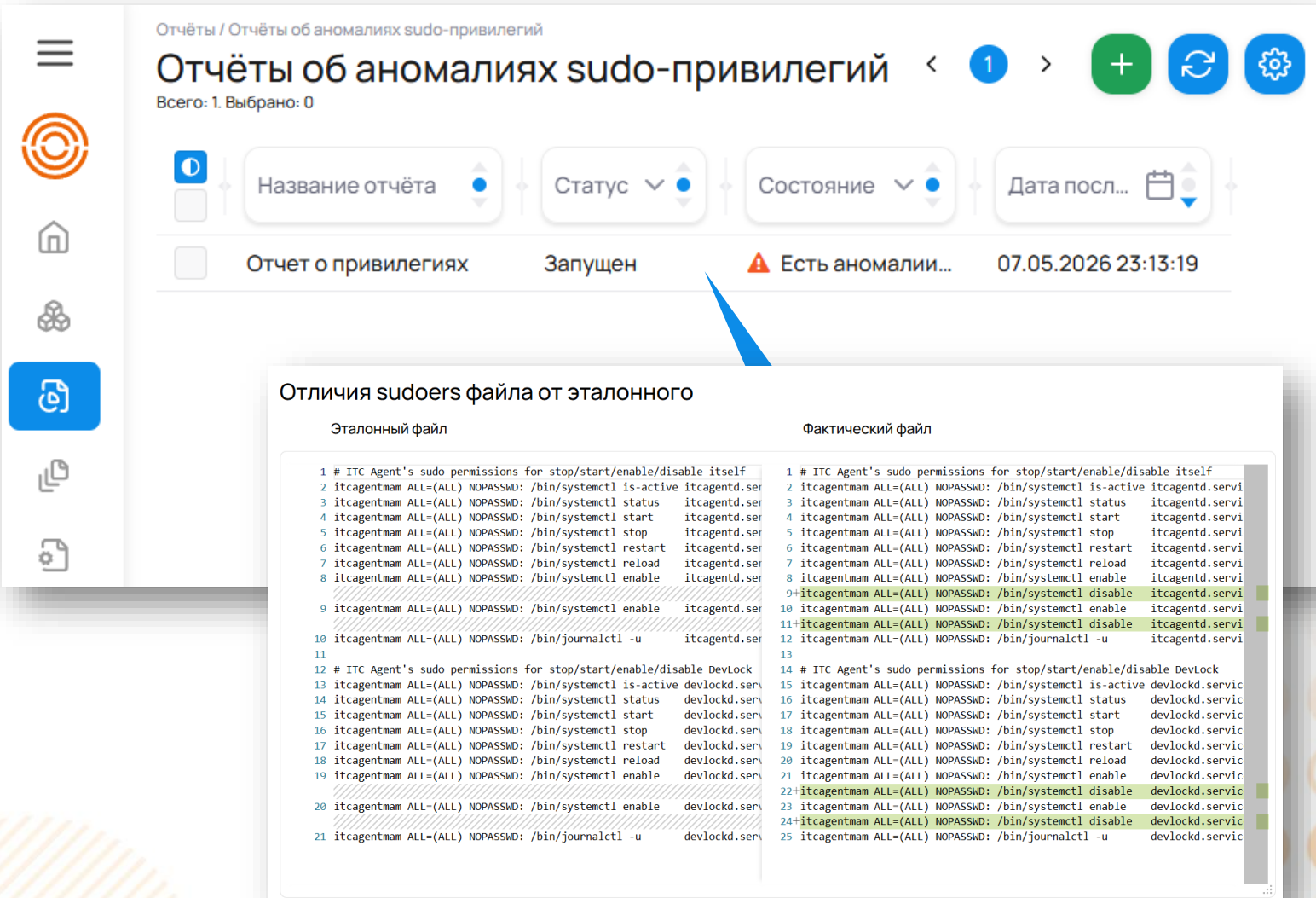
Обнаруженные уязвимости

Функции: Аналитические

Отчеты

Отслеживайте аномалии конфигурации с помощью встроенных отчетов

- **Аномалии sudo-привилегий** — проверяйте делегирование административных полномочий на APM Linux
- **Белый список ПО** — выявляйте ПО, не соответствующее политикам ИБ компании
- **Белый список процессов** — контролируйте все запускаемые процессы на наиболее критичных АРМ
- **Аномалии доступности агентов** — обнаруживайте попытки нарушения работы агентов
- **Аналитика ПО** — выявляйте портативное ПО, скопированное на АРМ в нарушение политик ИБ



Отчёты / Отчёты об аномалиях sudo-привилегий

Отчёты об аномалиях sudo-привилегий

Всего: 1. Выбрано: 0

Название отчёта | Статус | Состояние | Дата посл...

Отчет о привилегиях	Запущен	Есть аномалии...	07.05.2026 23:13:19
---------------------	---------	------------------	---------------------

Отличия sudoers файла от эталонного

Эталонный файл	Фактический файл
1 # ITC Agent's sudo permissions for stop/start/enable/disable itself	1 # ITC Agent's sudo permissions for stop/start/enable/disable itself
2 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl is-active itcagentd.serv	2 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl is-active itcagentd.servi
3 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl status itcagentd.serv	3 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl status itcagentd.servi
4 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl start itcagentd.serv	4 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl start itcagentd.servi
5 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl stop itcagentd.serv	5 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl stop itcagentd.servi
6 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl restart itcagentd.serv	6 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl restart itcagentd.servi
7 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl reload itcagentd.serv	7 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl reload itcagentd.servi
8 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable itcagentd.serv	8 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable itcagentd.servi
9 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable itcagentd.serv	9+itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl disable itcagentd.servi
10 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable itcagentd.serv	11+itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl disable itcagentd.servi
11 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable itcagentd.serv	12 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable itcagentd.servi
12 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable itcagentd.serv	13 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable itcagentd.servi
13 # ITC Agent's sudo permissions for stop/start/enable/disable DevLock	14 # ITC Agent's sudo permissions for stop/start/enable/disable DevLock
14 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl is-active devlockd.serv	15 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl is-active devlockd.servic
15 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl status devlockd.serv	16 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl status devlockd.servic
16 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl start devlockd.serv	17 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl start devlockd.servic
17 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl stop devlockd.serv	18 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl stop devlockd.servic
18 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl restart devlockd.serv	19 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl restart devlockd.servic
19 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl reload devlockd.serv	20 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl reload devlockd.servic
20 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable devlockd.serv	21 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable devlockd.servic
21 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable devlockd.serv	22+itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl disable devlockd.servic
22 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable devlockd.serv	23 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable devlockd.servic
23 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable devlockd.serv	24+itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl disable devlockd.servic
24 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable devlockd.serv	25 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable devlockd.servic
25 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable devlockd.serv	26 itcagentmam ALL=(ALL) NOPASSWD: /bin/systemctl enable devlockd.servic

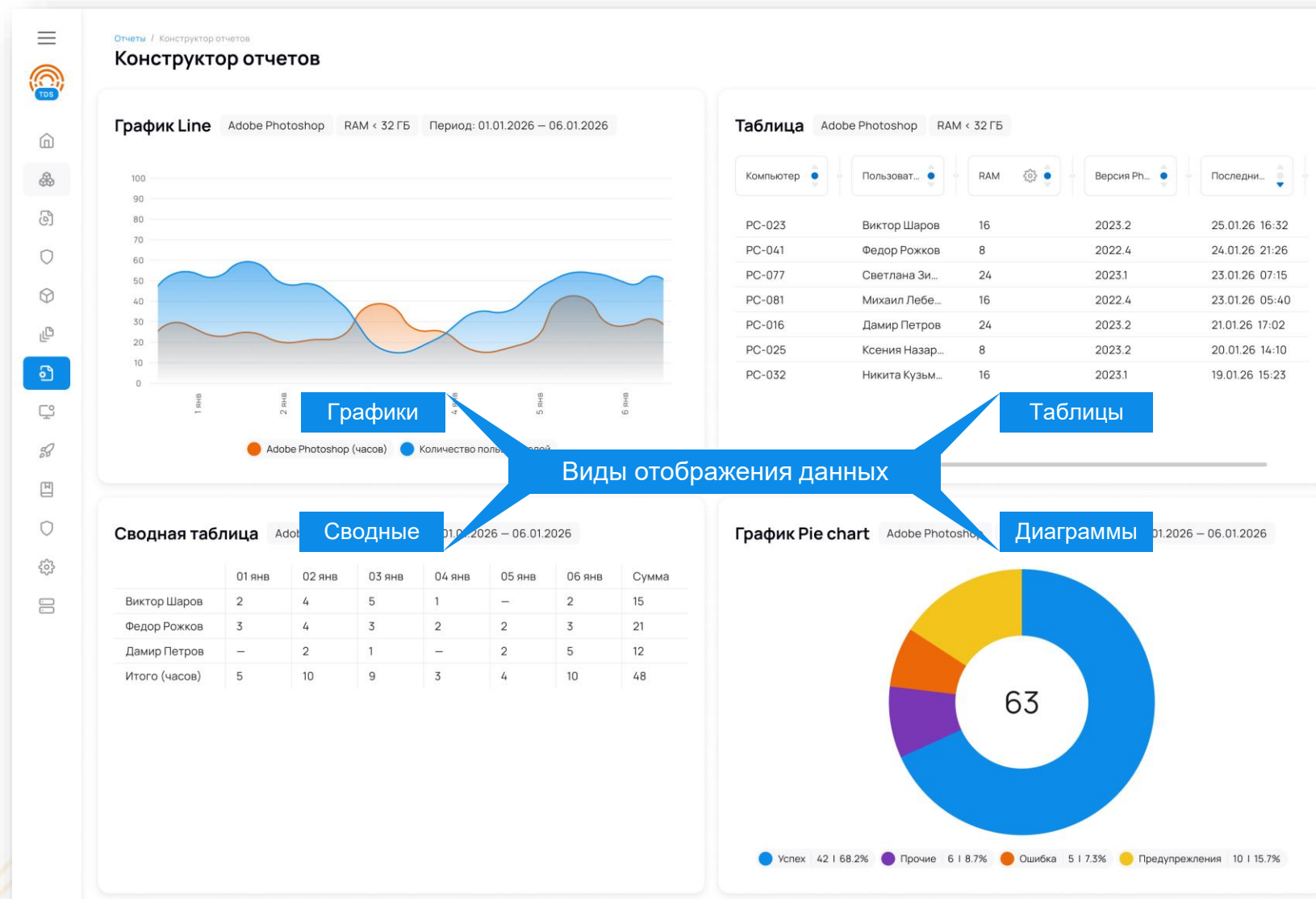
Подробная информация об аномалии административных привилегий

Функции: Аналитические

Конструктор отчетов

Создавайте наглядные отчеты по всем данным инвентарей

- **Дашборды** — компоуните графические панели с различными представлениями информации в удобном и мощном конструкторе — как на главной странице МиУ
- **Сводные таблицы** — создавайте отчеты, анализирующие данные на пересечении множества инвентарей
- **По расписанию и требованию** — настраивайте создание отчетов автоматически или создавайте их вручную
- **Уведомления и рассылки** — получайте почтовые уведомления о новых отчетах, обнаруженных аномалиях, а также копии отчетов



Функции: Мониторинг

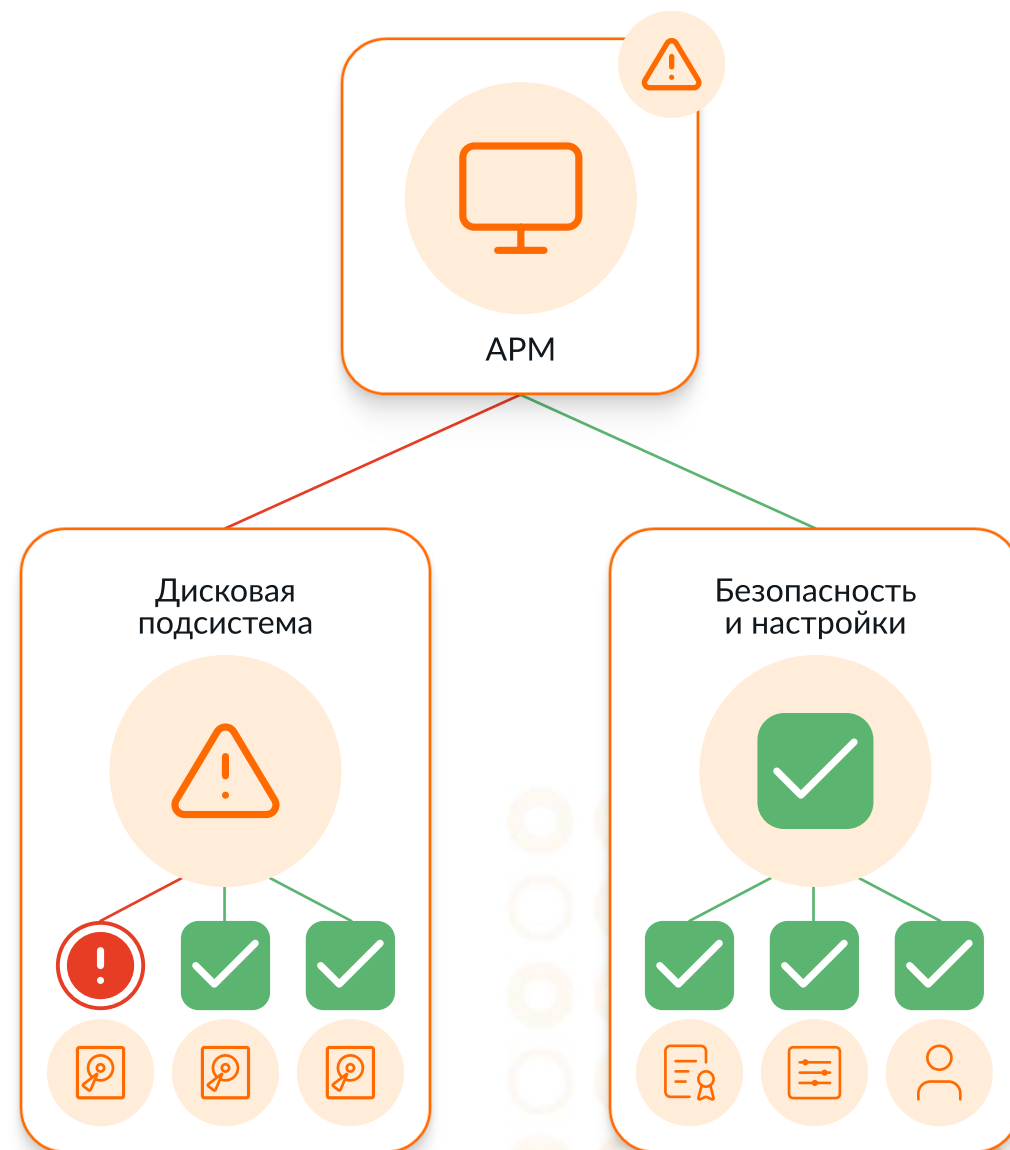
Структурированный мониторинг — сводное состояние распределенных информационных систем на основе иерархических **моделей здоровья**

Автоматический мониторинг — обнаружение и постановка на мониторинг в соответствии с установленными **пакетами мониторинга**

Мониторы — поддерживаются три типа мониторов

- **Метричные** предоставляют параметры производительности ОС и сервисов
- **Инвентарные** отслеживают соответствие данных инвентарей настроенным порогам
- **Агрегатные** позволяют создавать иерархическую модель инвентаря с использованием всех других типов мониторов

Автоматические оповещения по электронной почте при достижении метриками критических значений, определенных в моделях здоровья



Функции: Мониторинг

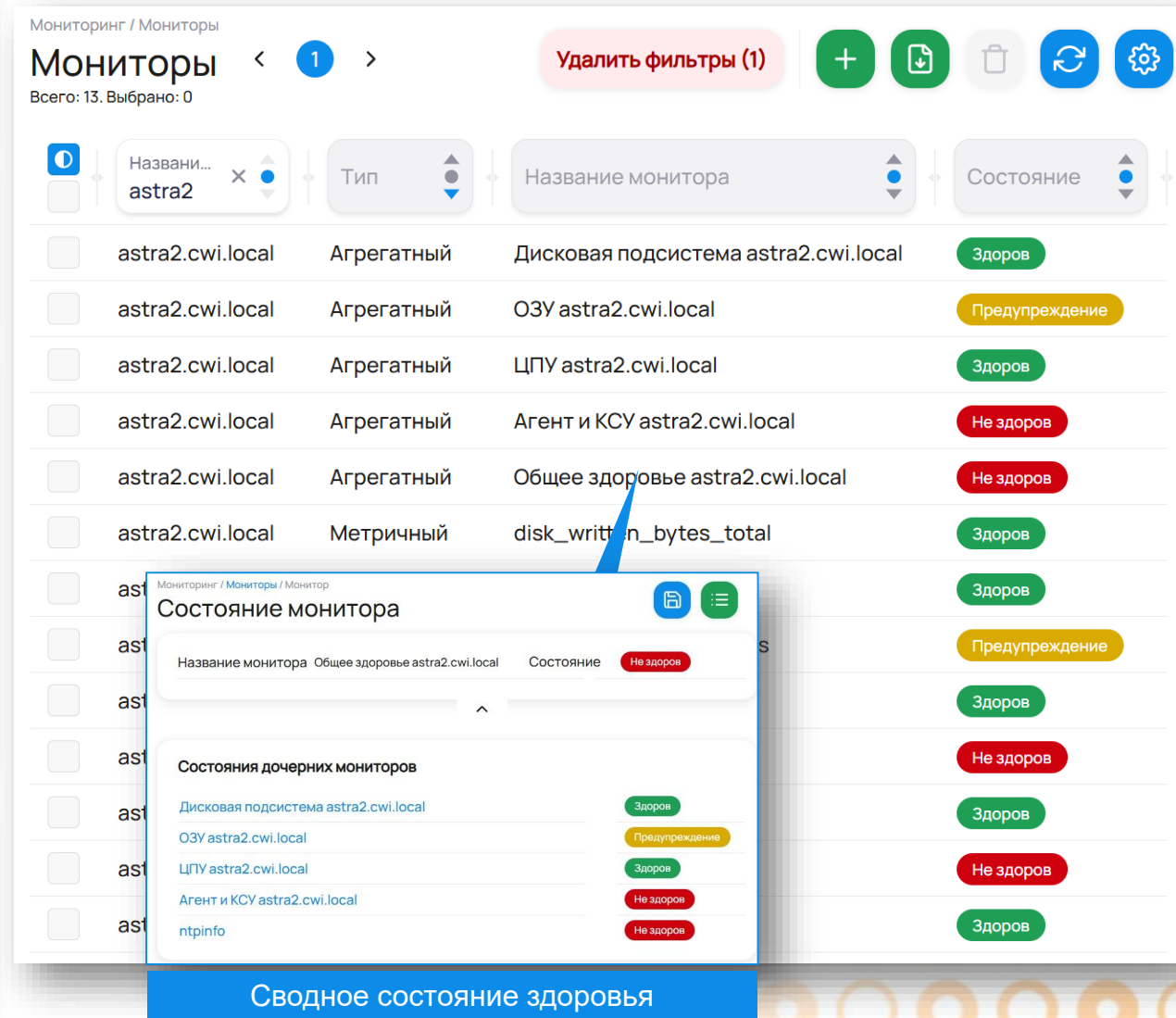
Структурированный мониторинг — сводное состояние распределенных информационных систем на основе иерархических **моделей здоровья**

Автоматический мониторинг — обнаружение и постановка на мониторинг в соответствии с установленными **пакетами мониторинга**

Мониторы — поддерживаются три типа мониторов

- **Метричные** предоставляют параметры производительности ОС и сервисов
- **Инвентарные** отслеживают соответствие данных инвентарей настроенным порогам
- **Агрегатные** позволяют создавать иерархическую модель инвентаря с использованием всех других типов мониторов

Автоматические оповещения по электронной почте при достижении метриками критических значений, определенных в моделях здоровья



Мониторинг / Мониторы

Мониторы

Всего: 13. Выбрано: 0

Удалить фильтры (1)

Названи... x astra2 Тип Название монитора Состояние

☐	astra2.cwi.local	Агрегатный	Дисковая подсистема astra2.cwi.local	Здоров
☐	astra2.cwi.local	Агрегатный	ОЗУ astra2.cwi.local	Предупреждение
☐	astra2.cwi.local	Агрегатный	ЦПУ astra2.cwi.local	Здоров
☐	astra2.cwi.local	Агрегатный	Агент и KCU astra2.cwi.local	Не здоров
☐	astra2.cwi.local	Агрегатный	Общее здоровье astra2.cwi.local	Не здоров
☐	astra2.cwi.local	Метричный	disk_written_bytes_total	Здоров
☐	astra2.cwi.local			Здоров
☐	astra2.cwi.local			Предупреждение
☐	astra2.cwi.local			Здоров
☐	astra2.cwi.local			Не здоров
☐	astra2.cwi.local			Здоров
☐	astra2.cwi.local			Не здоров
☐	astra2.cwi.local			Здоров

Мониторинг / Мониторы / Монитор

Состояние монитора

Название монитора: Общее здоровье astra2.cwi.local Состояние: Не здоров

Состояния дочерних мониторов

- Дисковая подсистема astra2.cwi.local: Здоров
- ОЗУ astra2.cwi.local: Предупреждение
- ЦПУ astra2.cwi.local: Здоров
- Агент и KCU astra2.cwi.local: Не здоров
- ntpinfo: Не здоров

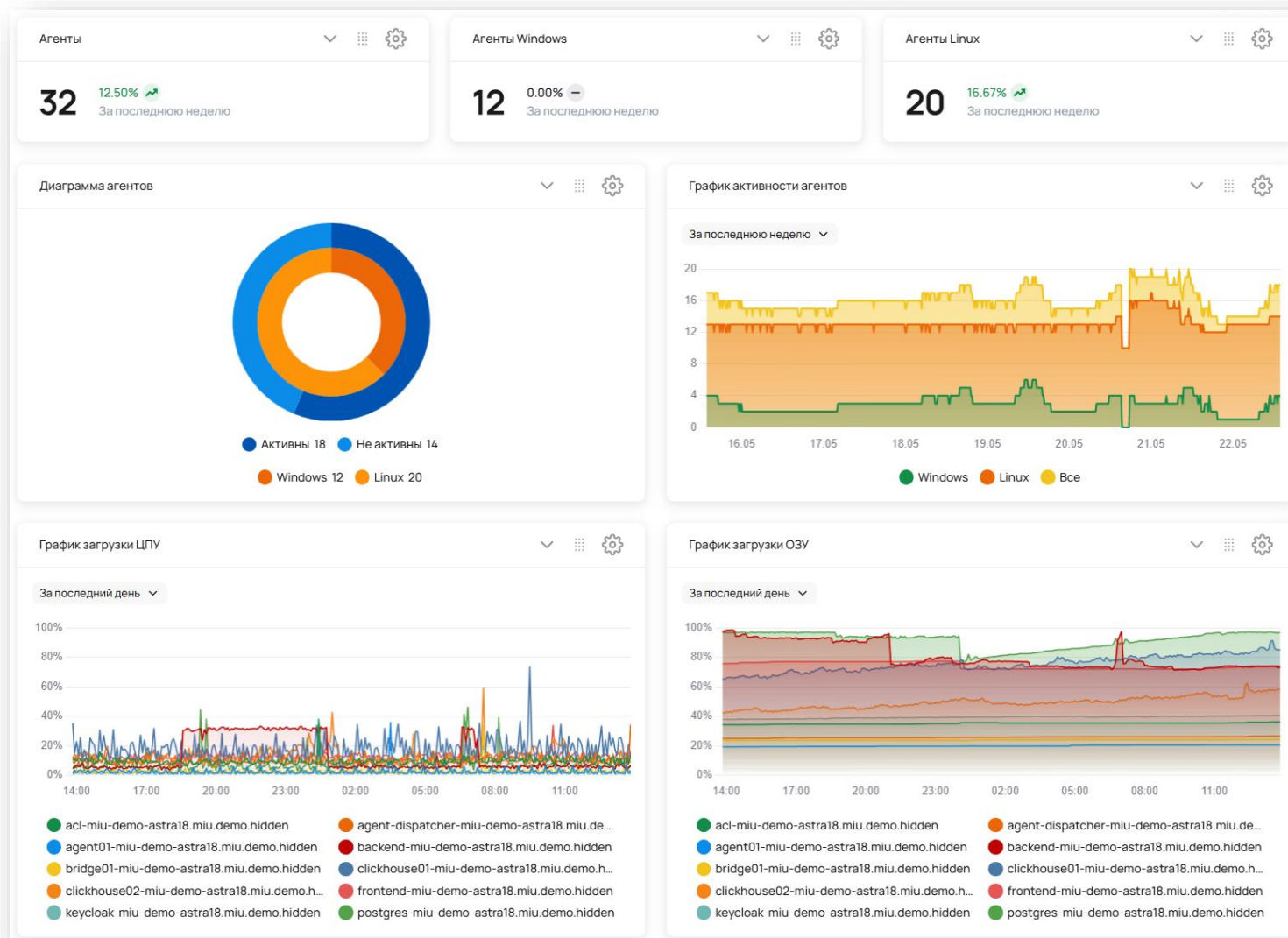
Сводное состояние здоровья

Функции: Мониторинг

Графики и дашборды — сводные таблицы и настраиваемые графические панели для мониторинга отдельных серверов и распределенных систем

Различные способы визуализации

- Простые и сводные таблицы
- Тепловые карты
- Графики
- Круговые диаграммы



Функции: Управление



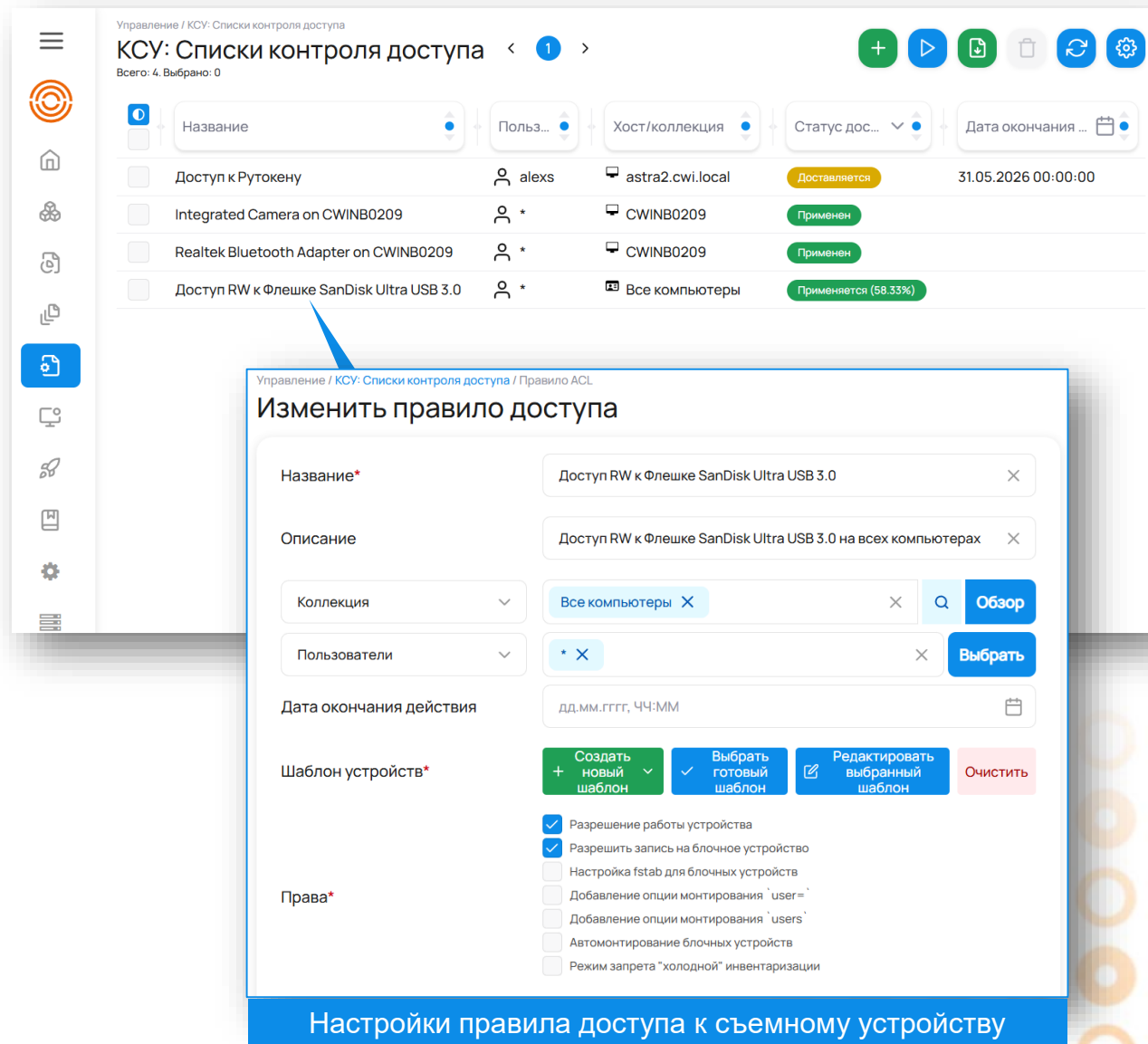
Функции: КСУ

Контроль съемных устройств — защищайте АРМ от неконтролируемого использования любых периферийных устройств от USB-накопителей и токенов до МФУ, Wi-Fi и Bluetooth-адаптеров

Модель разрешений «белый список» — по умолчанию запрещены все устройства кроме ограниченного настраиваемого списка периферии, необходимой для функционирования АРМ

Гранулированный контроль — разрешайте доступ к отдельным устройствам и группам устройств для пользователей и групп, отдельных АРМ и коллекций из десятков тысяч компьютеров

Временные правила — назначайте постоянные правила доступа или временные с датой истечения



Управление / КСУ: Списки контроля доступа

КСУ: Списки контроля доступа

Всего: 4. Выбрано: 0

Название	Польз...	Хост/коллекция	Статус дос...	Дата окончания ...
☐ Доступ к Руткену	alex	astra2.cwi.local	Доставляется	31.05.2026 00:00:00
☐ Integrated Camera on CWINB0209	*	CWINB0209	Применен	
☐ Realtek Bluetooth Adapter on CWINB0209	*	CWINB0209	Применен	
☐ Доступ RW к Флешке SanDisk Ultra USB 3.0	*	Все компьютеры	Применяется (58.33%)	

Изменить правило доступа

Название*

Описание

Коллекция

Пользователи

Дата окончания действия

Шаблон устройств*

- ☒ Создать новый шаблон
- ☒ Выбрать готовый шаблон
- ☐ Редактировать выбранный шаблон
-

Права*

- ☒ Разрешение работы устройств
- ☒ Разрешить запись на блочное устройство
- ☐ Настройка fstab для блочных устройств
- ☐ Добавление опции монтирования `user =`
- ☐ Добавление опции монтирования `users`
- ☐ Автомонтирование блочных устройств
- ☐ Режим запрета "холодной" инвентаризации

Настройки правила доступа к съемному устройству

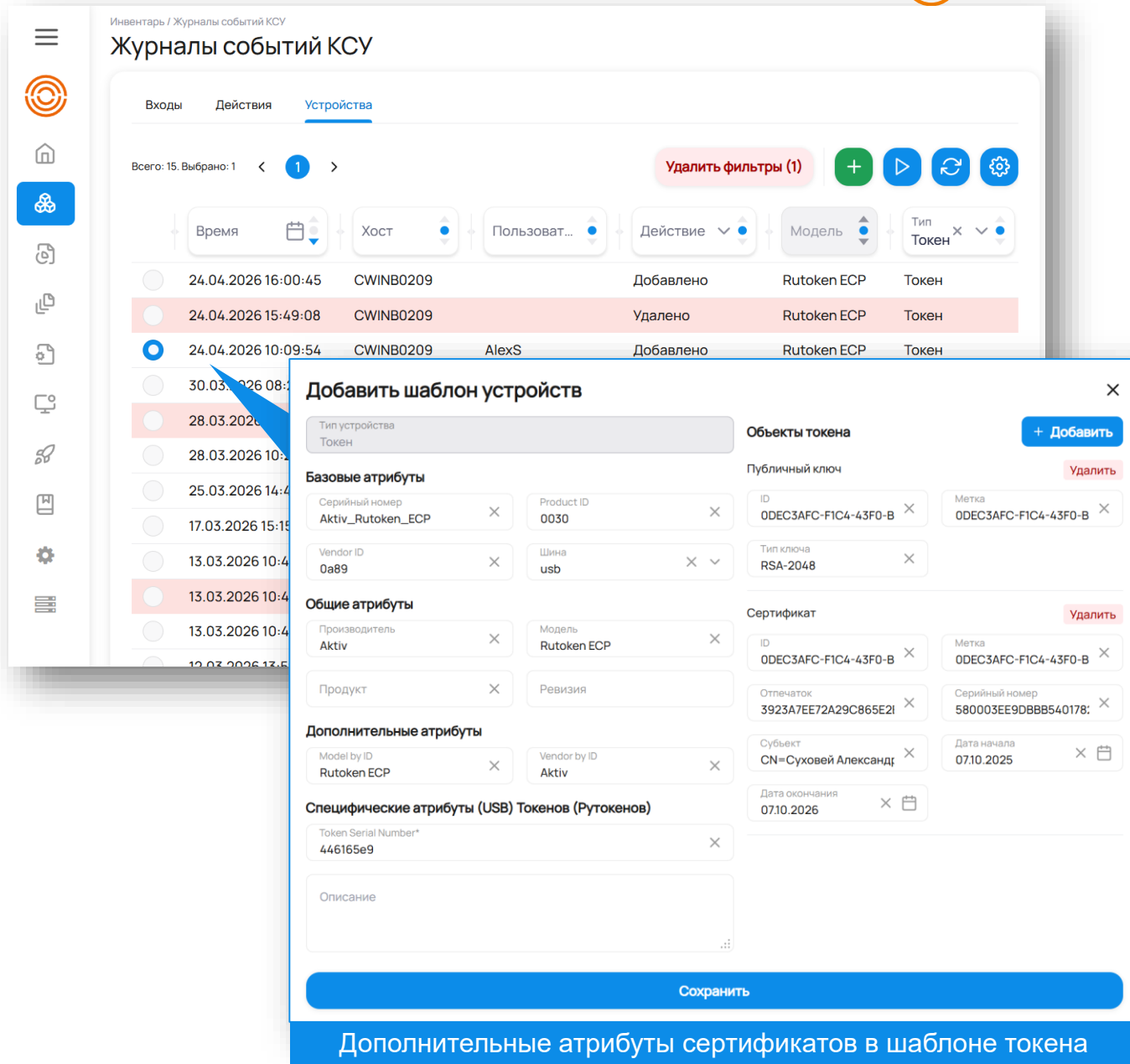
Функции: КСУ

Инвентаризация сертификатов — при подключении токенов КСУ считывает публичную часть информации о сертификатах на токене и отображает ее в событиях аудита

Тонкая настройка доступа — для сетевых устройств и токенов на основе таких атрибутов как MAC-адрес и атрибуты сертификатов на токене

Правила из событий — создавайте предзаполненные шаблоны устройств и правила доступа из событий подключения устройств к АРМ

Тестирование правил — проверяйте влияние нового правила на пользователей и АРМ до применения правила на большом количестве компьютеров



Инвентарь / Журналы событий КСУ

Журналы событий КСУ

Входы Действия Устройства

Всего: 15. Выбрано: 1 < 1 >

Удалить фильтры (1) + ▶ ↺ ⚙

Время Хост Пользоват... Действие Модель Тип Токен

24.04.2026 16:00:45	CWINB0209		Добавлено	Rutoken ECP	Токен
24.04.2026 15:49:08	CWINB0209		Удалено	Rutoken ECP	Токен
24.04.2026 10:09:54	CWINB0209	AlexS	Добавлено	Rutoken ECP	Токен
30.03.2026 08:...					
28.03.2026					
28.03.2026 10:...					
25.03.2026 14:4...					
17.03.2026 15:15					
13.03.2026 10:4...					
13.03.2026 10:4...					
13.03.2026 10:4...					
13.03.2026 13:5...					

Добавить шаблон устройств

Тип устройства: Токен

Объекты токена: + Добавить

Публичный ключ: Удалить

Базовые атрибуты

Серийный номер: Aktiv_Rutoken_ECP	Product ID: 0030	ID: 0DEC3AFC-F1C4-43F0-B	Метка: 0DEC3AFC-F1C4-43F0-B
Vendor ID: 0a89	Шина: usb	Тип ключа: RSA-2048	

Общие атрибуты

Производитель: Aktiv	Модель: Rutoken ECP	ID: 0DEC3AFC-F1C4-43F0-B	Метка: 0DEC3AFC-F1C4-43F0-B
Продукт:	Ревизия:	Отпечаток: 3923A7EE72A29C865E2I	Серийный номер: 580003EE9DBB540178:

Дополнительные атрибуты

Model by ID: Rutoken ECP	Vendor by ID: Aktiv	Субъект: CN=Суховой Александр	Дата начала: 07.10.2025
Специфические атрибуты (USB) Токенов (Рутокенов)		Дата окончания: 07.10.2026	

Token Serial Number*: 446165e9

Описание

Сохранить

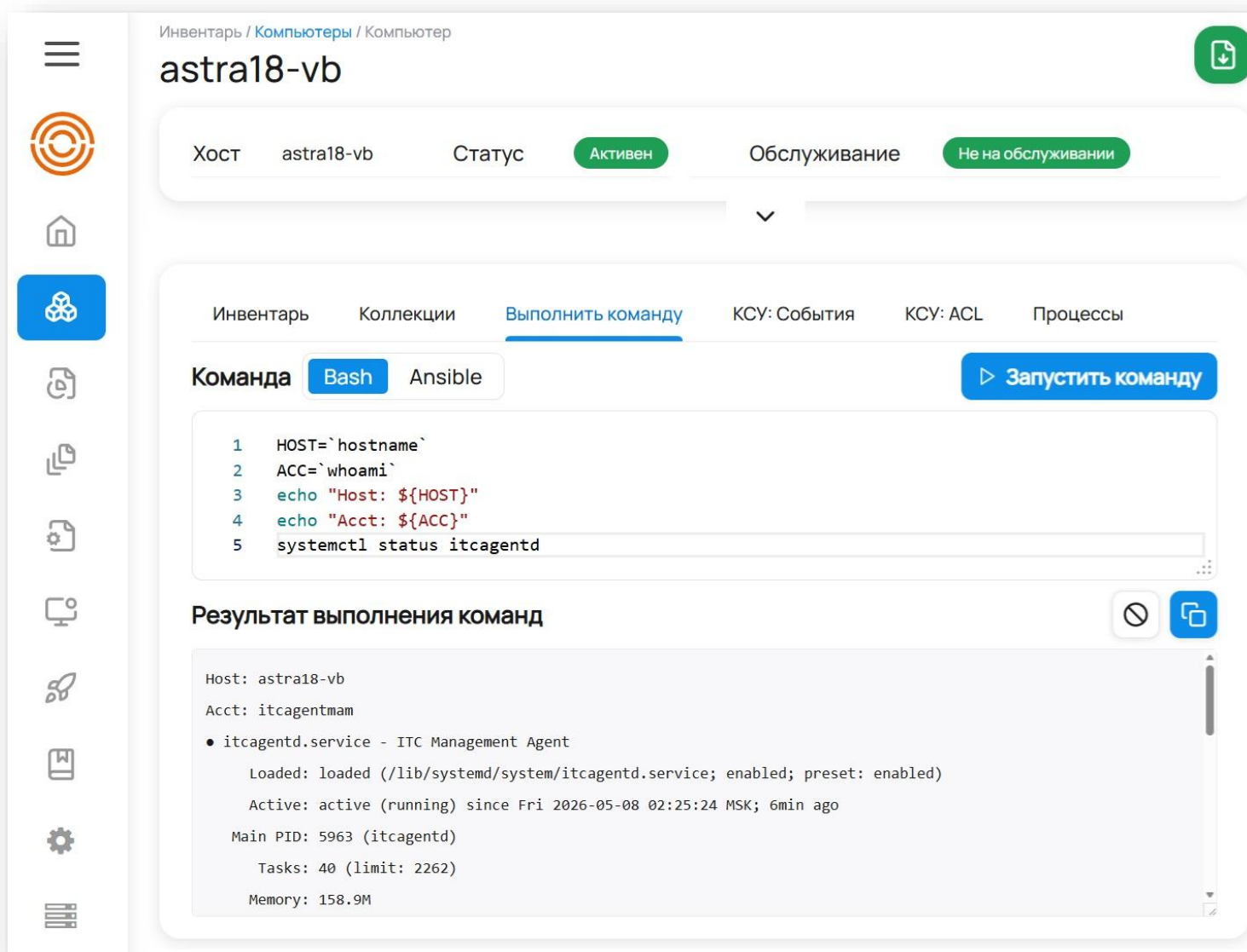
Дополнительные атрибуты сертификатов в шаблоне токена

Функции: Интерактивные команды

Командная строка с поддержкой bash, PowerShell и Ansible для Linux и Windows

Встроенный редактор с подсветкой синтаксиса и автозаполнением для работы с отдельными командами и целыми скриптами

История результатов выполнения команд сохраняется до перехода на другую страницу



Инвентарь / Компьютеры / Компьютер

astra18-vb

Хост: astra18-vb Статус: **Активен** Обслуживание: **Не на обслуживании**

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

Команда: **Bash** Ansible **▶ Запустить команду**

```
1 HOST=`hostname`
2 ACC=`whoami`
3 echo "Host: ${HOST}"
4 echo "Acct: ${ACC}"
5 systemctl status itcagentd
```

Результат выполнения команд

Host: astra18-vb
Acct: itcagentmam

- itcagentd.service - ITC Management Agent
 - Loaded: loaded (/lib/systemd/system/itcagentd.service; enabled; preset: enabled)
 - Active: active (running) since Fri 2026-05-08 02:25:24 MSK; 6min ago
 - Main PID: 5963 (itcagentd)
 - Tasks: 40 (limit: 2262)
 - Memory: 158.9M

Функции: Режим обслуживания

Ставьте на паузу

- агента
- контроль съемных устройств
- модули агента

Вручную или по расписанию

- настраивайте расписания режима обслуживания для различных коллекций
- или
- включайте и выключайте режим по необходимости для одного или нескольких АРМ

Система / Окна обслуживания

Окна обслуживания

01.05.2026

Понедельник 27	Вторник 28	Среда 29	Четверг 30	Пятница 1	Суббота 2	Воскресенье 3
Ежедневный бекап	Ежедневный бекап	Ежедневный бекап	Ежедневный бекап	Ежедневный бекап	Техобслуживание серверов	Техобслуживание серверов
Бухгалтерия 17:00 - 18:00	Бухгалтерия 17:00 - 18:00	Бухгалтерия 17:00 - 18:00	Бухгалтерия 17:00 - 18:00	Бухгалтерия 17:00 - 18:00	Хосты сетевого обнаружения	Хосты сетевого обнаружения 00:00 - 06:00
Ежедневная сдача кассы	Ежедневная сдача кассы	Ежедневная сдача кассы				Ежедневная сдача кассы
Кассиры 19:00 - 19:30	Кассиры 19:00 - 19:30	Кассиры 19:00 - 19:30				Кассиры 19:00 - 19:30

Инвентарь / Компьютеры

Компьютеры

Всего: 24. Выбрано: 1

Хост	ОС	Статус	Обслуживание
☒ astra2.cwi.local	linux	Активен	На обслуживании
☐ CWINB0209	windows	Активен	На обслуживании
☐ CWINB0021	windows	Активен	На обслуживании
☐ astra18-vb1	linux	Активен	На обслуживании
☐ bridge01-miu-...	linux	Активен	
☐ cwinb0114	windows	Не активен	
☐ vtb-test-vl01.r...	linux	Не активен	
☐ keycloak-miu-...	linux	Активен	

Режим обслуживания

Функции: Управление ПО

Установка и обновление ПО

Загружайте дистрибутивы в точки распространения МиУ или используйте корпоративные репозитории

Управление лицензиями

Назначайте лицензии для автоматического распределения при установке ПО

Контроль использования ПО и лицензий

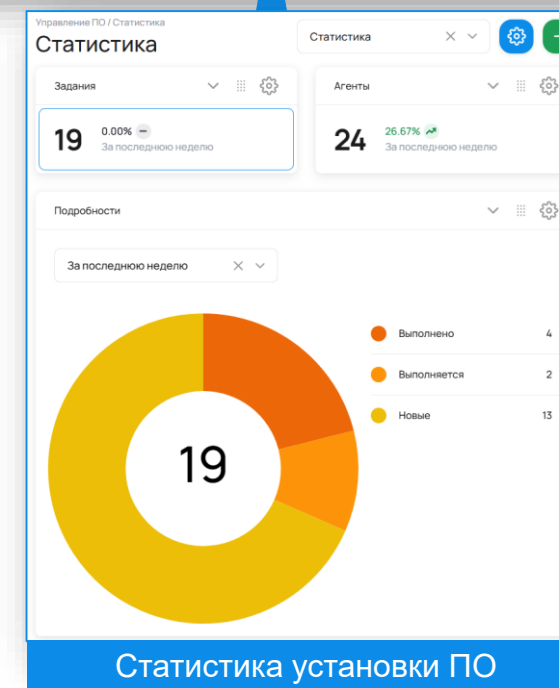
Используйте отчеты об использовании ПО и лицензий пользователями АРМ для планирования закупок

Управление ПО / Дистрибутивы

Дистрибутивы < 1 >

Всего: 3. Выбрано: 0

☐	Название	Версия	Дата загрузки	Релиз	Активен
☐	Draw.io v29.6.1 Debian	29.6.1	25.03.2026 16:07:03	✓	✓
☐	Kaspersky Endpoint Security for Linux (KESL)...	12.3.0	13.03.2026 09:26:24	✓	✓
☐	Kaspersky Endpoint Security for Linux (KESL)...	12.3.1	13.03.2026 10:32:58	✓	✓



Функции: Политики

Принудительное применение

- Настроек агента
- Параметров блокировки экрана
- Политик сложности паролей

Подключаемые модули для расширения набора контролируемых настроек операционной системы, безопасности и прикладного ПО

Управление / Библиотека политик

Библиотека политик < 1 >

Всего: 1. Выбрано: 0

	Название	Описание	Дата создания	Автор политики
☐	Политики настроек агента	Политики настроек агента	13.03.2026 09:51:23	Александр Суховой
☐	Базовая корпоративная политика	Набор правил проверки сложности паролей ...	11.03.2026 13:25:05	Operator Novosibirsk

Управление / Библиотека политик / Редактирование политики

Редактирование политики

 + Добавить раздел

Название* Политики настроек агента

Описание* Политики настроек агента

Разделы политики

Мост	https://bridge01.cwi.local	
Стоимость	1	
Вес	1	

master_servers

Редактирование политики

 + Добавить раздел

Максимальное количество доставляемых сообщений в 10-секундный интервал

Настройка профилирования работы Агента

Изменение интервала поллинга

Список мостов агента МиУ

Модули политики

Функции: Помощник по паролям

Помощник по паролям упрощает пользователям АРМ создание стойких паролей, соответствующих политикам ИБ

Вся мощь регулярных выражений для создания расширенных правил сложности паролей

Разные правила сложности паролей для разных категорий АРМ

Локальная проверка сложности пароля без передачи данных по сети

Правила

Название правила	Паттерн	Сообщение о несоответствии	Сообщение о соответствии
Минимум 8 символов	<code>^.{8,}\$</code>	Пароль слишком короткий	Пароль содержит не менее 8 символов
Есть цифра	<code>.*[0-9].*</code>	Нет цифр	Содержит хотя бы одну цифру
Нет русских букв	<code>^[^а-яА-Я]*\$</code>	Есть русские буквы	Нет русских букв
Есть спецсимвол	<code>[[:punct:]]</code>	Нет спецсимвола	Есть спецсимвол
Есть строчная буква	<code>.*[a-z].*</code>	Нет строчных букв	Содержит строчные буквы
Есть заглавная буква	<code>.*[A-Z].*</code>	Нет заглавных букв	Содержит заглавные буквы

Проверка сложности пароля

Новый пароль:

Результат тестирования: **Найдены ошибки**

Есть заглавная буква	Содержит заглавные буквы	✓
Есть цифра	Содержит хотя бы одну цифру	✓
Есть строчная буква	Содержит строчные буквы	✓
Нет русских букв	Есть русские буквы	✗
Минимум 8 символов	Пароль содержит не менее 8 символов	✓
Есть спецсимвол	Есть спецсимвол	✓

Помощник по паролям на АРМ пользователя

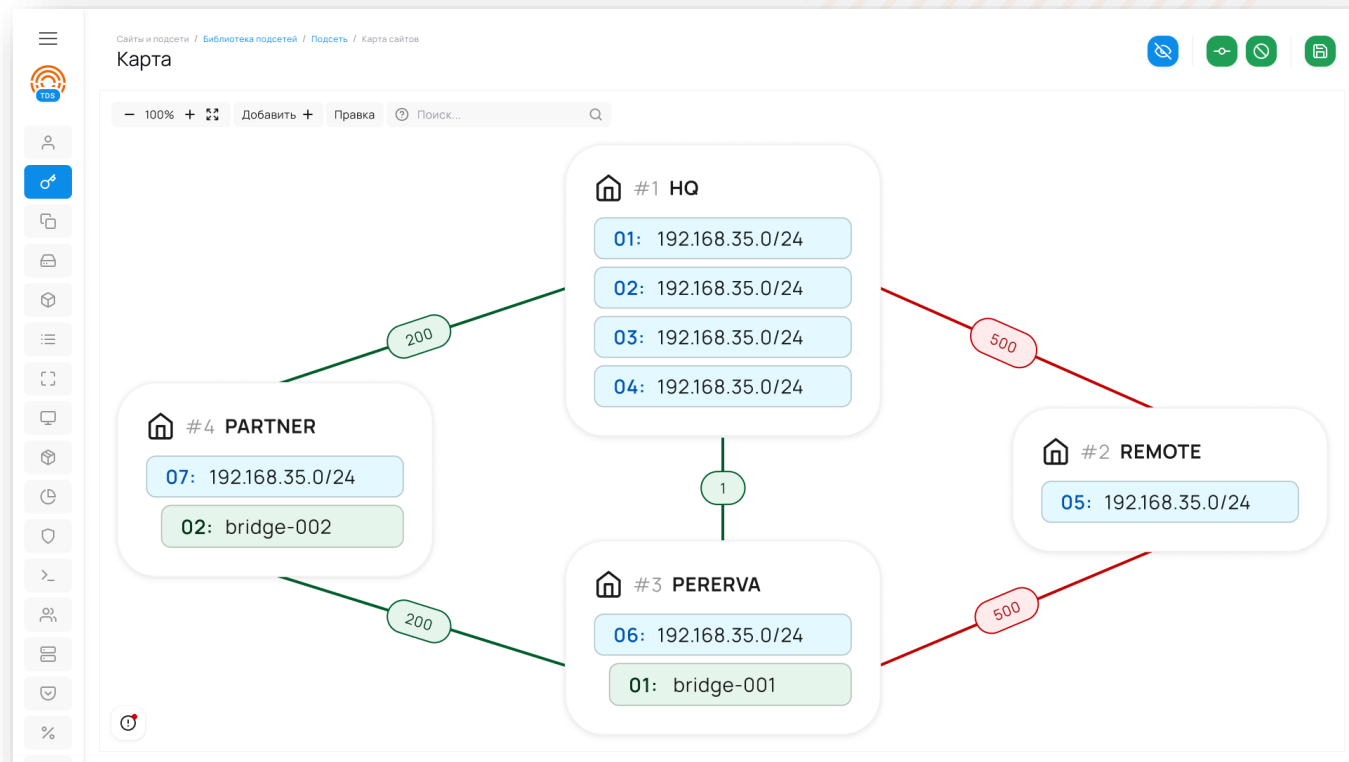
Функции: Сайты и подсети

Сайты и подсети — аналог функции Active Directory для автоматического поиска ближайших сетевых сервисов

Стоимость межсайтового взаимодействия используется для поиска оптимального маршрута

Автоматическая регистрация Мостов для получения агентом списка оптимальных мостов в зависимости от своей подсети

Интеграция для использования функции другими распределенными информационными системами



Пример поиска агентом в сайте **HQ** ближайшего моста:

- Мосты расположены в сайтах **PERERVA** и **PARTNER**
- Агент получает список из двух мостов, упорядоченный по стоимости

Результат: агент подключается к мосту **bridge-001** в сайте **PERERVA** с наименьшей стоимостью канала **1**.

Функции: Удаленная поддержка и подключение к рабочему столу

Заявки на поддержку создаются пользователями на APM через приложение Клируэй или операторами поддержки в интерфейсе МиУ

Подключение к APM в отдельную сессию или в сессию пользователя с подтверждением и контролем мыши/клавиатуры

Поддержка протоколов SSH, RDP, VNC, встроенных и собственных клиентов и серверов RDP

Защищенный туннель использует транспорт агента и не требует открытия портов SSH, RDP, VNC на APM в корпоративную сеть

Система / Поддержка / Библиотека заявок на поддержку

Библиотека заявок на поддержку

Всего: 2. Выбрано: 1

Взять в работу Подключиться к APM

	Имя хоста	Описание	ФИО пользователя	Статус заявки	ФИО ответственного ...
☐	CWINB0209	Проблема с ПО	Alexander Sukhovey (Demo)	Новая	
☒	CWINB0209	Не работает принтер	Andrey Kaidalov	В работе	Александр Суховей

Настройки защищенного туннеля

APM оператора* astra2.cwi.local Обзор

APM пользователя* CWINB0209 Обзор

Служба* RDP Shadow (Custom, Удаленный помощник)

Время жизни* 1 час

Создать туннель

Создание туннеля

Настройки защищенного туннеля

astra2.cwi.local CWINB0209

Инициализация Первый агент подключился Второй агент подключился Установлено подключение

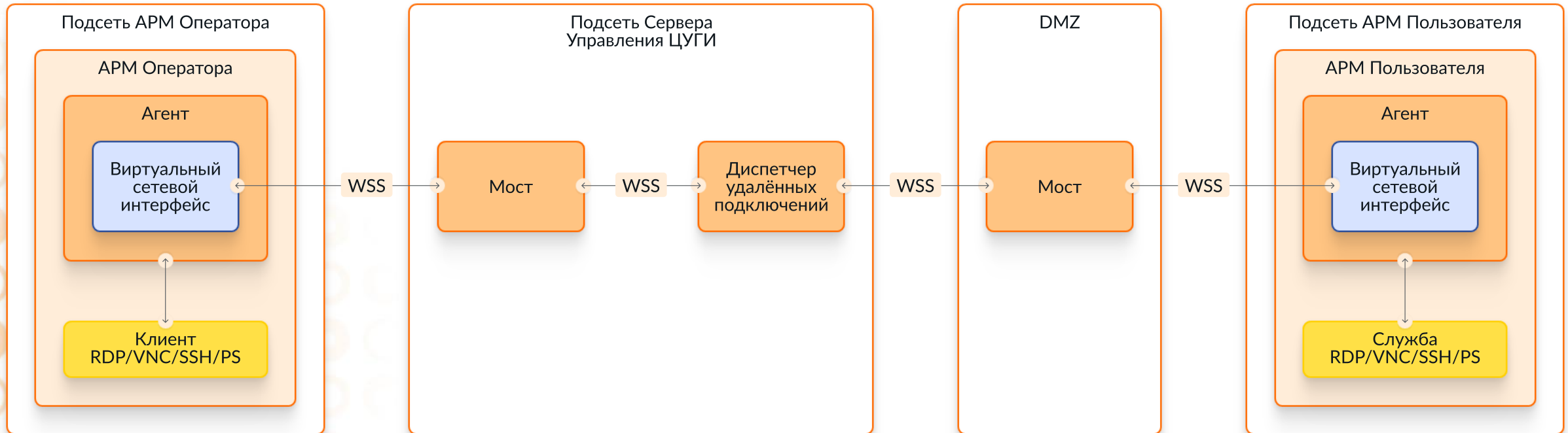
Подключиться

Подключение к APM

SSH
RDP
VNC
RDP Shadow (IP туннель)
✓ RDP Shadow (Custom, Удаленный помощник)

Протоколы

Схема взаимодействия



Протоколы: графическая сессия

RDP	Windows	Linux
Windows	✓*	✓
Linux	✓	✓

- ✓ используется любой поддерживаемый платформой клиент/сервер RDP
- ✓ работа при отсутствии прямого сетевого доступа между APM
- ✓ работа в контуре Inet через механизм цепочек мостов

* для Windows поддерживается подключение в сессию пользователя с помощью стандартного клиента RDP от Microsoft

VNC	Windows	Linux	macOS
Windows	✓	✓	✓*
Linux	✓	✓	✓*
macOS	✓	✓	✓*

- ✓ используется любой поддерживаемый платформой клиент/сервер VNC
- ✓ работа при отсутствии прямого сетевого доступа между APM
- ✓ работа в контуре Inet через механизм цепочек мостов

* для входа в сессию пользователя требуется запуск стороннего VNC сервера

Протоколы: командная строка

SSH	Windows	Linux	macOS
Windows	✓	✓	✓
Linux	✓	✓	✓
macOS	✓	✓	✓

- ✓ работа при отсутствии прямого сетевого доступа между APM
- ✓ работа в контуре Inet через механизм цепочек мостов

POWER SHELL	Windows
Windows	🕒*

- ✓ поддержка туннелирования удаленной сессии power shell
- ✓ работа при отсутствии прямого сетевого доступа между APM
- ✓ работа в контуре INET через механизм цепочек мостов

* в разработке

Функции: Системные



Функции: Ролевая модель

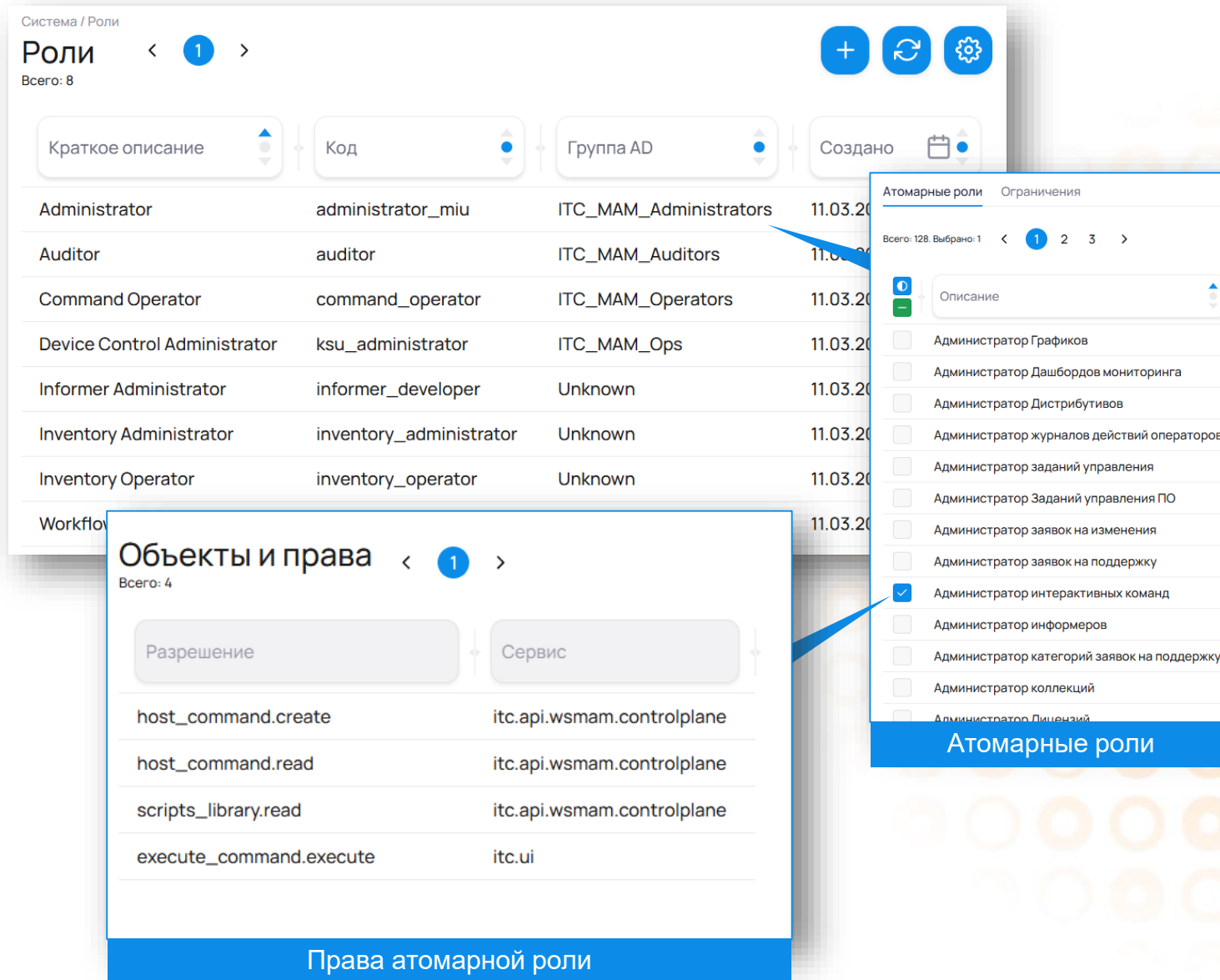
Гибкая и гранулярная ролевая модель, построенная на трех уровнях иерархии:

- **Права** на объекты по модели **CRUD**: create, read, update, delete
- **Атомарные роли** — подмножества прав доступа к отдельному типу объектов
- **Пользовательские роли** — группы атомарных ролей, соответствующие обязанностям сотрудников

Интеграция со службами каталога для сопоставления доменных групп и пользовательских ролей МиУ

Подробный аудит действий операторов МиУ: вход и выход в интерфейс МиУ, создание, изменение и удаление объектов

Ограничивающие коллекции и режим утверждения изменений для наиболее критичных действий и объектов



Система / Роли

Роли < 1 > Всего: 8

Краткое описание	Код	Группа AD	Создано
Administrator	administrator_miu	ITC_MAM_Administrators	11.03.20
Auditor	auditor	ITC_MAM_Auditors	11.03.20
Command Operator	command_operator	ITC_MAM_Operators	11.03.20
Device Control Administrator	ksu_administrator	ITC_MAM_Ops	11.03.20
Informer Administrator	informer_developer	Unknown	11.03.20
Inventory Administrator	inventory_administrator	Unknown	11.03.20
Inventory Operator	inventory_operator	Unknown	11.03.20
Workflow			11.03.20

Объекты и права < 1 > Всего: 4

Разрешение	Сервис
host_command.create	itc.api.wsmam.controlplane
host_command.read	itc.api.wsmam.controlplane
scripts_library.read	itc.api.wsmam.controlplane
execute_command.execute	itc.ui

Атомарные роли

Ограничения

Всего: 128. Выбрано: 1 < 1 2 3 >

Описание

- ☐ Администратор Графиков
- ☐ Администратор Дашбордов мониторинга
- ☐ Администратор Дистрибутивов
- ☐ Администратор журналов действий операторов
- ☐ Администратор заданий управления
- ☐ Администратор Заданий управления ПО
- ☐ Администратор заявок на изменения
- ☐ Администратор заявок на поддержку
- ☒ Администратор интерактивных команд
- ☐ Администратор информеров
- ☐ Администратор категорий заявок на поддержку
- ☐ Администратор коллекций
- ☐ Администратор Лицензий

Права атомарной роли

Интеграция с продуктами ЦУГИ

Загрузка сертификатов,
из системам ЦУГИ СМАОК
и МиУ, инвентаризированных
с помощью агентов и модуля
сетевого сканирования

Связывание сертификатов
с местами установки. Данные
о местах установки поступают
от:

- Агенты МиУ и СМАОК
- Сетевое сканирование
- МиУ КСУ – модуль агента для,
контроля съемных устройств
(токенов)

Отображение загруженных
сертификатов в едином списке



Сертификаты \ Мои сертификаты \ Карточка сертификата

Карточка сертификата

Основная информация

Информационная система 0004 Система мониторинга [Изменить](#)

Стрим Внутренний мониторинг [Изменить](#)

Кому выдан zabbix.clearwayintegration.com

Удостоверяющий центр CWI Enterprise CA 1, O=Clearway Integration, C=RU

Начало действия 23.02.2024 17:39

Окончание действия 09.02.2026 12:44

Серийный номер 4f00000030cdfbf7f5534734d000000...

Шаблон

SAN dns=zabbix.clearwayintegration.com, dns=zabbix

EKU TLS Web Serv

Уведомлять об истечении за (количество дней) 60 (по умолчанию)

Статусы

Статус обновления Обновлен (статус обновлен: 19.12.2025 13:11 ЛКПС Админ)

Плановая дата замены Указать дату

Статус отзыва Действующий

Тип выпуска Неизвестно [Изменить](#)

Дата проверки отзыва 06.01.2026 09:00

Дата смены статуса отзыва 24.06.2025 09:04

Владелец Ответственные Места установки ЗНИ История изменений Комментарий Связать

Места установки

МИУ:zabbix.clearwayintegration.com:443

cwi-azure-zbx.onprem.clearwayintegration.com

[+ Добавить](#)

Отображение мест использования сертификата

Планы



Дорожная карта

- Расширение инвентаризации служб времени
- **Многочисленные улучшения** графического интерфейса

- Пользовательский **магазин приложений**, публикация ПО
- Централизованные настройки модулей и параметров агента
- Интеграция с системой Clearway СКЗИ 2.0
- Интеграция с системой Clearway **EXC**
- Архивный режим агентов

2026

1-й
квартал

2-й
квартал

3-й
квартал

4-й
квартал

- Валидатор инвентарей
- **Новые инвентари** в стандартной поставке: автозапуск, локальные группы, обновления Windows, история браузера и др.
- **Управление настройками** служб времени
- Централизованные настройки МиУ

- **Новые инвентари** в стандартной поставке: локальные и AD сертификаты, события аудита Windows и др.
- **Аналитика использования** ПО и лицензий
- Push инсталляция агента
- Встроенная справка и база знаний
- Новые групповые политики
- **Установка ОС** по сети

Лицензирование и поддержка



Лицензирование

1

Лицензирование модулей

Для каждого модуля, установленного на отдельном хосте при развертывании программного продукта на базе ПО ЦУГИ, необходимо приобретение соответствующей лицензии

2

Ограничения лицензирования

Все модули и функции ПО ЦУГИ делятся на две группы: **базовые и прикладные**. Каждый модуль и функция ПО ЦУГИ имеет свою метрику лицензирования

3

Сроки действия лицензий

Срочная лицензия

Обновления системы доступны в течение всего срока действия лицензии.

Бессрочная лицензия

Обновления системы доступны в течение первого года использования. Со второго года лицензия на право обновления приобретается отдельно.

Лицензирование

Модули	Метрики лицензирования
Полнофункциональная система МиУ с ограничением на 1000 пользователей	С ограничением на 1000 Агентов и не более 100 коллекций
Модуль серверной панели управления, контроля, настроек и инвентаризации APM	На один контур управления
Модуль агента "Базовая инвентаризация APM" для Windows и Linux	Без ограничения по количеству APM
Модуль расширения агента для инвентаризации установленного ПО (требуется для анализа по справочнику CVE	Без ограничения по количеству агентов
Модуль расширения агента для управления съемными носителями (КСУ)	Без ограничения по количеству APM
Модуль сравнения инвентаризации Установленного ПО по белому списку	На один контур управления
Модуль сервера ЦУГИ формирования базовых отчетов по справочнику CVE для установленному ПО	Без ограничения по количеству экземпляров
Модуль расширенной инвентаризации LDAP-каталогов (FreeIPA, ALD Pro, SAMBA 4)	На один контур управления
Модуль формирования журналов	На один контур управления
Функция контроля рабочего времени	На один контур управления
Модуль настройки, синхронизации и мониторинга системного времени ОС	На один контур управления

Дополнительные услуги сопровождения

Выходим за рамки реагирования: анализ и профилактика

Глубокий аудит

- Поиск слабых мест в настройке и архитектуре;
- Анализ внешних факторов, включая интеграции и стороннее ПО.

Проактивные услуги

- Обновление компонентов ЦУГИ;
- Мониторинг за ключевыми показателями продуктов;
- Профилактические работы в технологические окна;
- Оптимизация конфигураций для снижения нагрузки.

Обучение

- Проведение обучения работе с продуктами для ключевых пользователей;
- Консультирование по регулярным работам и сложным кейсам.



По итогам разработки и разворачивания архитектуры мы можем обеспечить быструю миграцию и подключение (до **10 000 АРМ** за **1** рабочий день)

О компании

Clearway Integration — российский разработчик ПО для управления и мониторинга Информационных систем, разработчик продуктов, помогающих повысить управляемость и информационную безопасность. Компания создает эффективные решения на базе платформы ЦУГИ, повышающие уровень безопасности и автоматизации ИТ-инфраструктуры компаний.

Clearway Integration — надежный поставщик ИТ- и ИБ-продуктов отечественной разработки для импортозамещения иностранных решений.



Получите готовое решение

 Знакомство с продуктами

