НСТС | КУПОЛ

ОПТИМИЗИРУЕМ ПОЛИТИКИ, СОГЛАСУЕМ ДОСТУП, ИЩЕМ ДЫРЫ И ЗАСТАВЛЯЕМ, НАКОНЕЦ, РАБОТАТЬ NGFW (А НЕ ВАС)

+ITI

ОСНОВНЫЕ ЗАДАЧИ РЕШЕНИЙ КЛАССА NSPM

НСТС | КУПОЛ

Оптимизация политик

Как эффективно анализировать и оптимизировать политики безопасности?

Управление политиками

Как централизованно управлять правилами на МЭ разных вендоров?

Мониторинг

Как контролировать состояние подключенных устройств?

Контроль

Как контролировать изменения конфигураций устройств?

Мультивендорная реализация

Как интегрировать решения разных вендоров МЭ в систему управления?

Безопасность

Как обеспечить необходимые уровень доступов и сетевой безопасности компании?

Совместимость

Как интегрировать продукт в существующую инфраструктуру?

Ограничение прав

Как ограничить права доступа пользователей к устройствам?

НОТА КУПОЛ.УПРАВЛЕНИЕ

НОТА | КУПОЛ

Единый мультивендорный центр контроля, управления и оптимизации работы межсетевых экранов, UTM, NGFW

Ценность для клиента

+ Ускорение и унификация настройки из единого интерфейса политик МЭ всех вендоров устройств, установленных в инфраструктуре компании
+ Видимость всех устройств МЭ в сети компании и своевременное нахождение неисправных
+ Быстрый ввод в эксплуатацию новых сегментов сети с помощью клонирования конфигураций на одно или несколько устройств
+ Полная видимость изменений политик на устройствах и возможность быстро найти устройство, политики которого нарушили какие-либо бизнес-процессы компании
+ Оптимально настроенные политики безопасности во всей инфраструктуре компании и отсутствие политик, снижающих пропускную способность сети компании и ее защищенность

Функции

Мониторинг состояния всех установленных МЭ

Подключение и мониторинг состояния доступности подключенных устройств МЭ: UserGate, CheckPoint, Cisco ASA, Fortigate и др.

Управление конфигурациями

Автобэкапирование конфигураций подключенных устройств, их клонирование на другие устройства, сравнение версий между собой и анализ

Интеграция с SIEM/SOAR

Отправка журналов событий продукта «НОТА | КУПОЛ. Управление» в сторонние системы по протоколу Syslog

Управление политиками безопасности

Централизованный контроль и управление политиками / правилами МЭ вендоров: UserGate, CheckPoint, Cisco ASA и др.

Оптимизация правил на всех устройствах

Выявление аномалий в правилах МЭ: избыточных, дублирующихся, теневых и других. Рекомендации по их оптимизации

Администрирование

Предоставление прав доступа в систему локальным пользователям и из Active Directory / Astra Linux Directory. Управление парольной политикой. Журнал событий

ЗАДАЧИ

НОТА | КУПОЛ

Когда актуально?

Анализ доступов	Выявление и устранение ошибок в инфраструктуре
Оптимизация правил доступа	Снижение нагрузки устройства до 30–50%
Оценка рисков несанкционированного доступа в действующей структуре	Устранение (изменение) опасных и потенциально опасных правил
Согласованное изменение политик ИБ, контроль исполнения	Анализ изменений в доступе до внесения
Защита доступов ключевых бизнес-приложений	Контроль доступности: платежных, биллинговых, финансовых приложений

РОЛИ

НСТС | КУПОЛ

Сетевой инженер
(управляет устройствами — автоматизация управления и настройки конфигурации сетевых устройств)

- Автоматизация управления (бэкапы, централизованная настройка, раскатка политик, оптимизация работы устройств)
- Приведение настроек в соответствие с политиками безопасности, предиктивная проверка внедрения планируемых изменений

CISO
(контролер)

- Контроль инфраструктуры установленным политикам, отсутствию уязвимостей и/или возможности их эксплуатации, контроль сетевой инфраструктуры на соответствие политикам безопасности, автоматизация проверки
- Определение политик безопасности

Инженер ИБ

- Контроль и управление политиками на каждом отдельно взятом устройстве
- Контроль отсутствия уязвимостей и/или возможности их эксплуатации
- Определение зон безопасности и межсетевого взаимодействия

АНАЛИЗ ПОЛИТИК

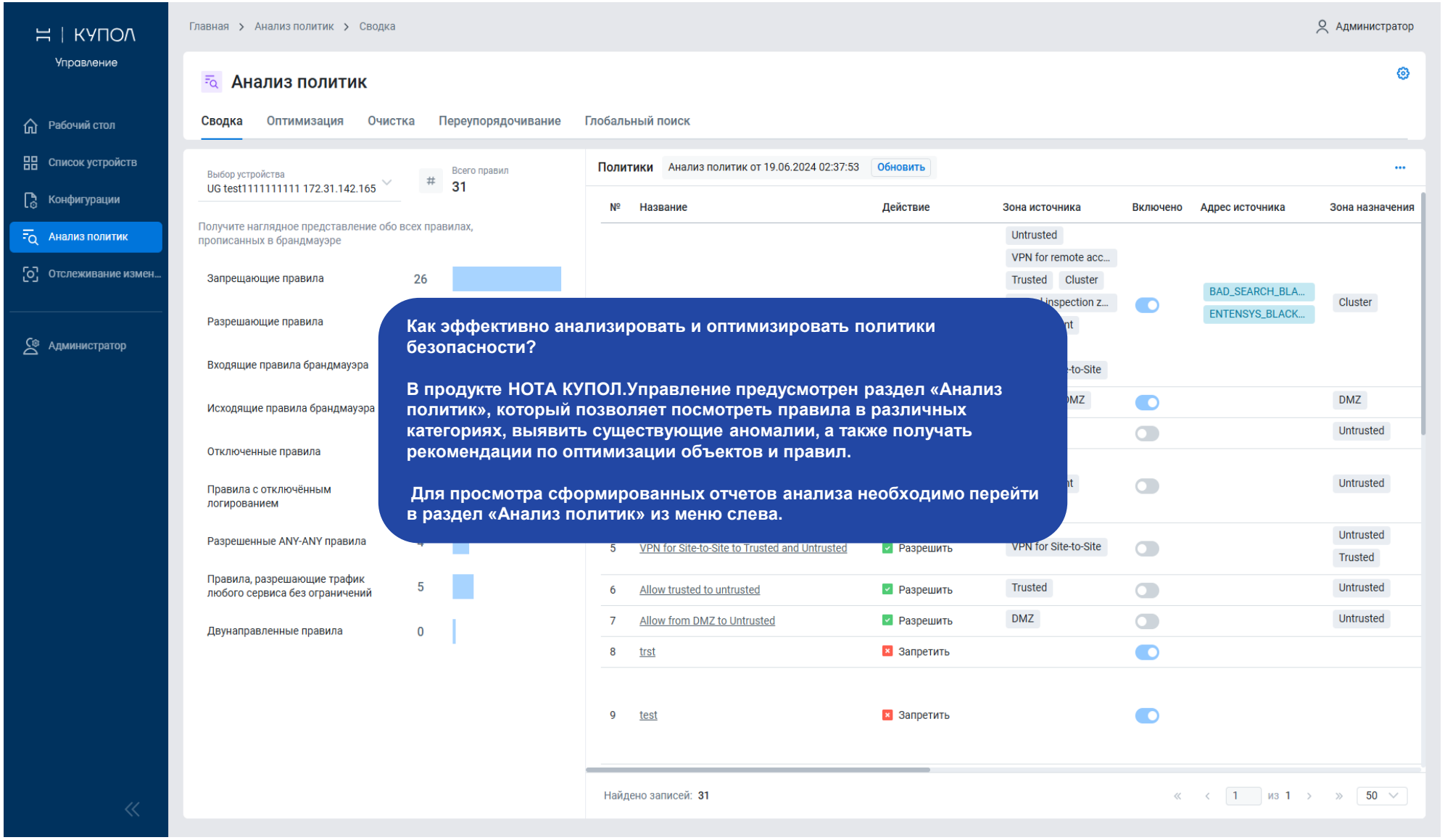
Кто мы?

Инженеры ИБ

Чего мы хотим?

Мы хотим контролировать соответствие устройства требованиям безопасности, изменениям, происходящим на устройстве. Мы хотим, чтобы политики были настроены безопасно и оптимизированы

АНАЛИЗ ПОЛИТИК

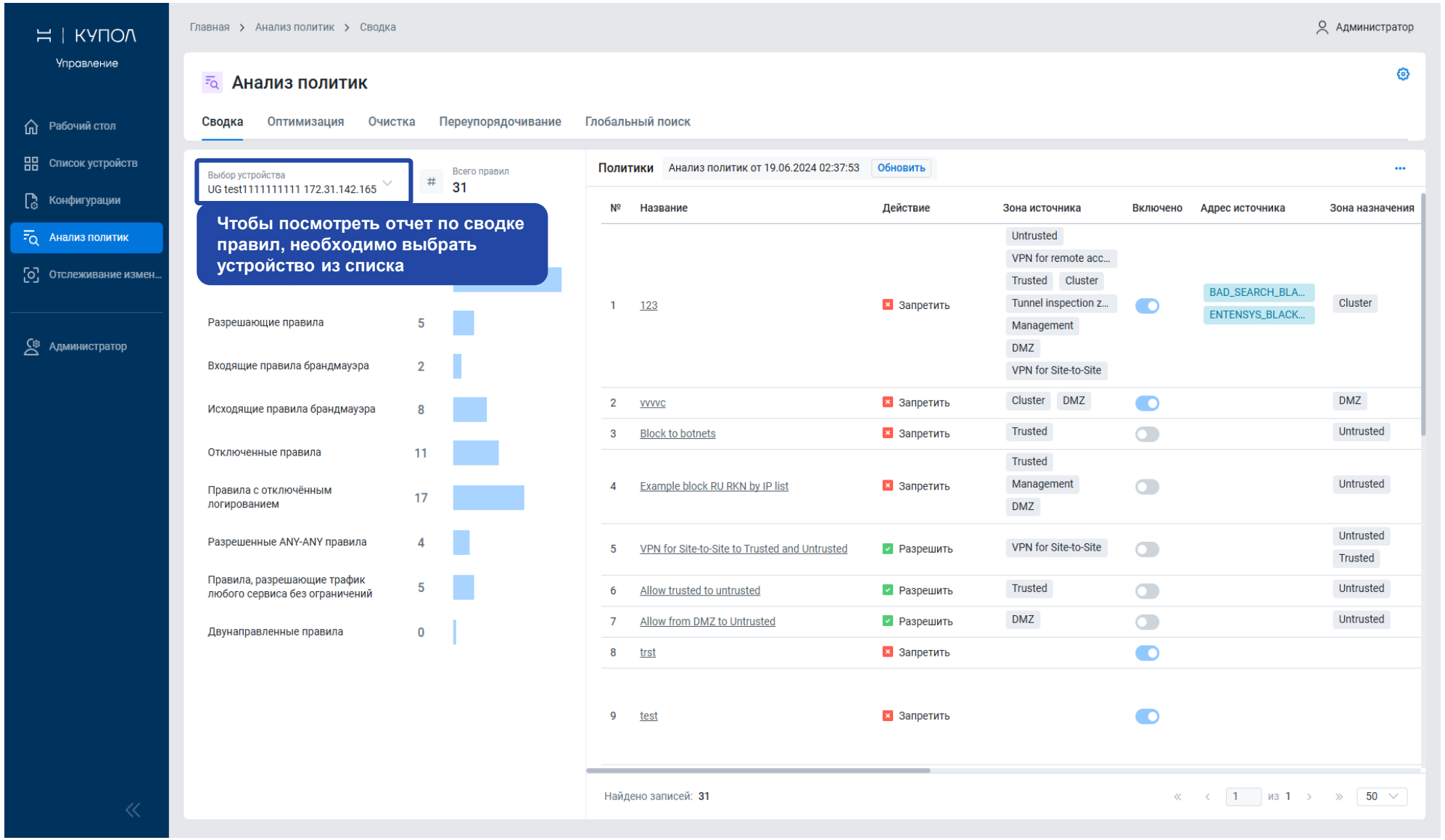


Как эффективно анализировать и оптимизировать политики безопасности?

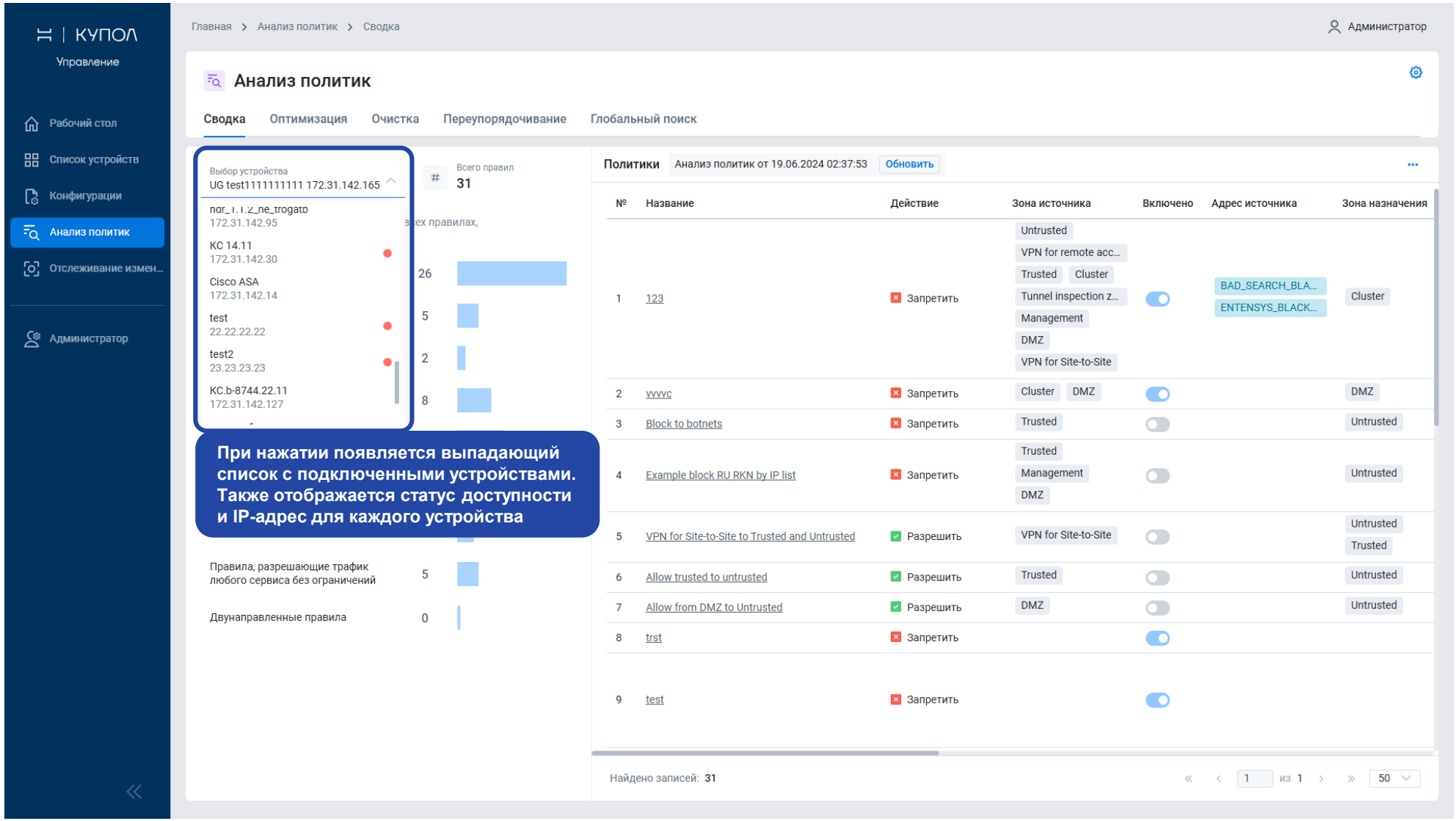
В продукте НОТА КУПОЛ.Управление предусмотрен раздел «Анализ политик», который позволяет посмотреть правила в различных категориях, выявить существующие аномалии, а также получать рекомендации по оптимизации объектов и правил.

Для просмотра сформированных отчетов анализа необходимо перейти в раздел «Анализ политик» из меню слева.

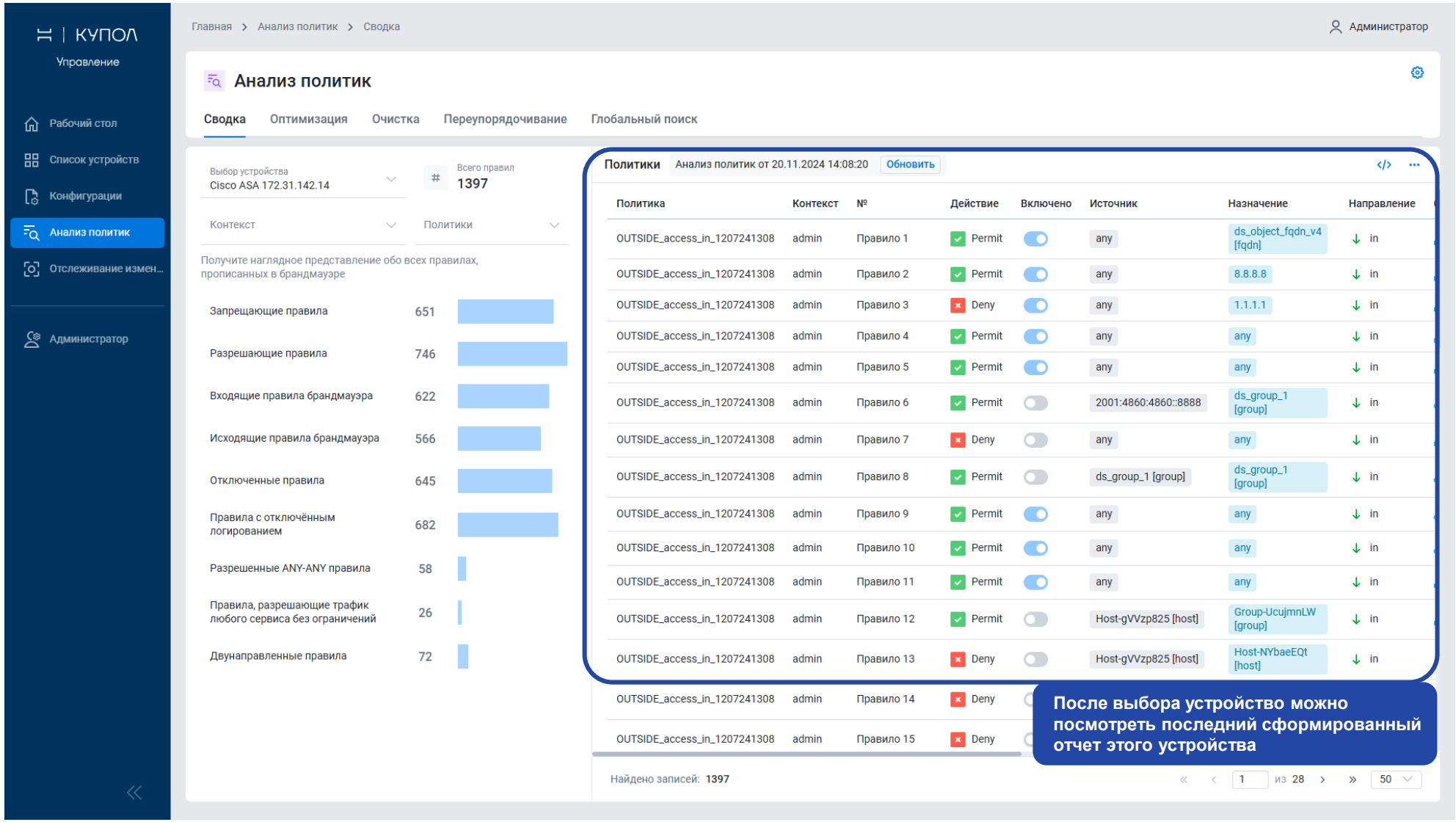
АНАЛИЗ ПОЛИТИК — СВОДКА



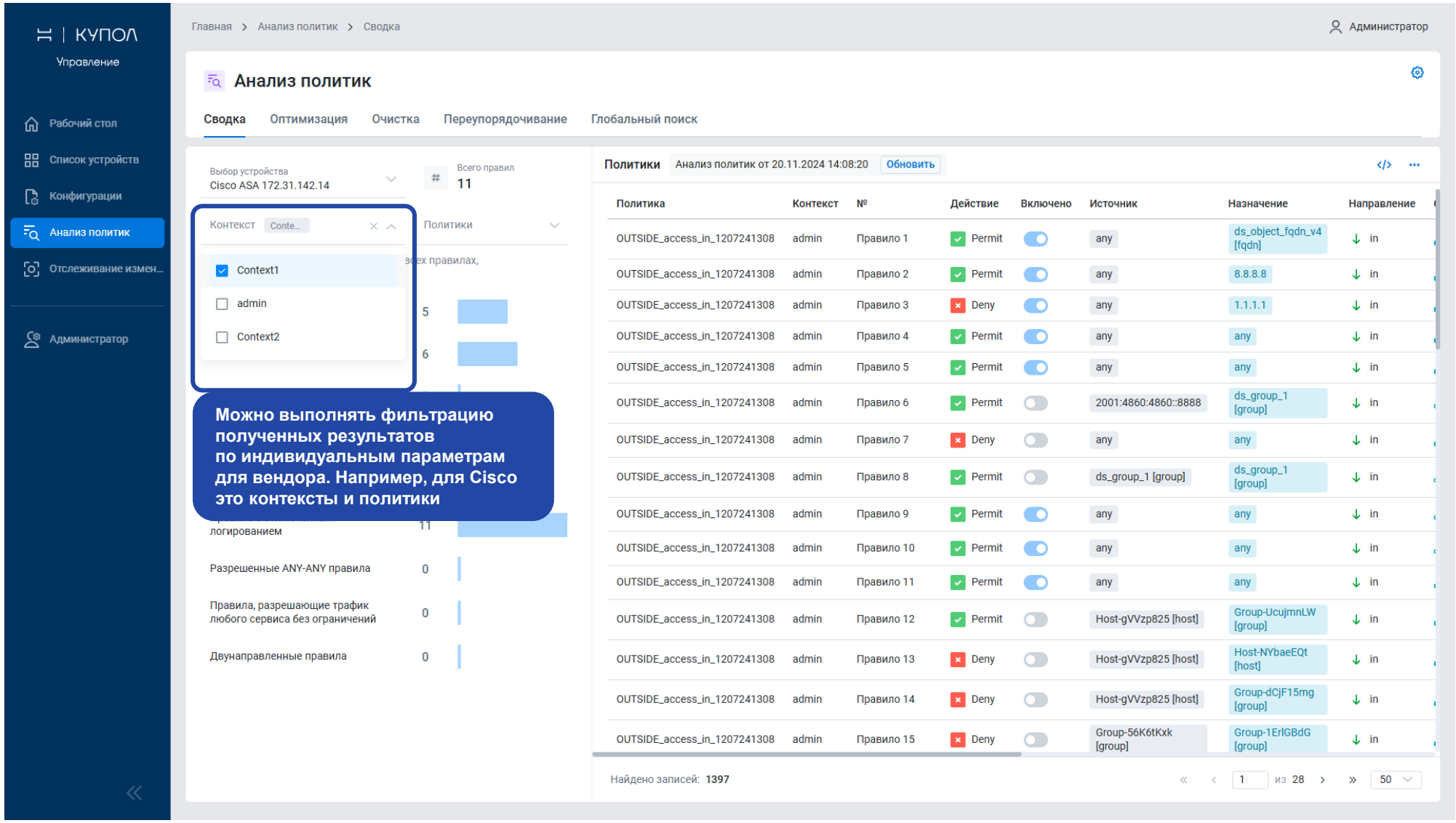
АНАЛИЗ ПОЛИТИК — СВОДКА



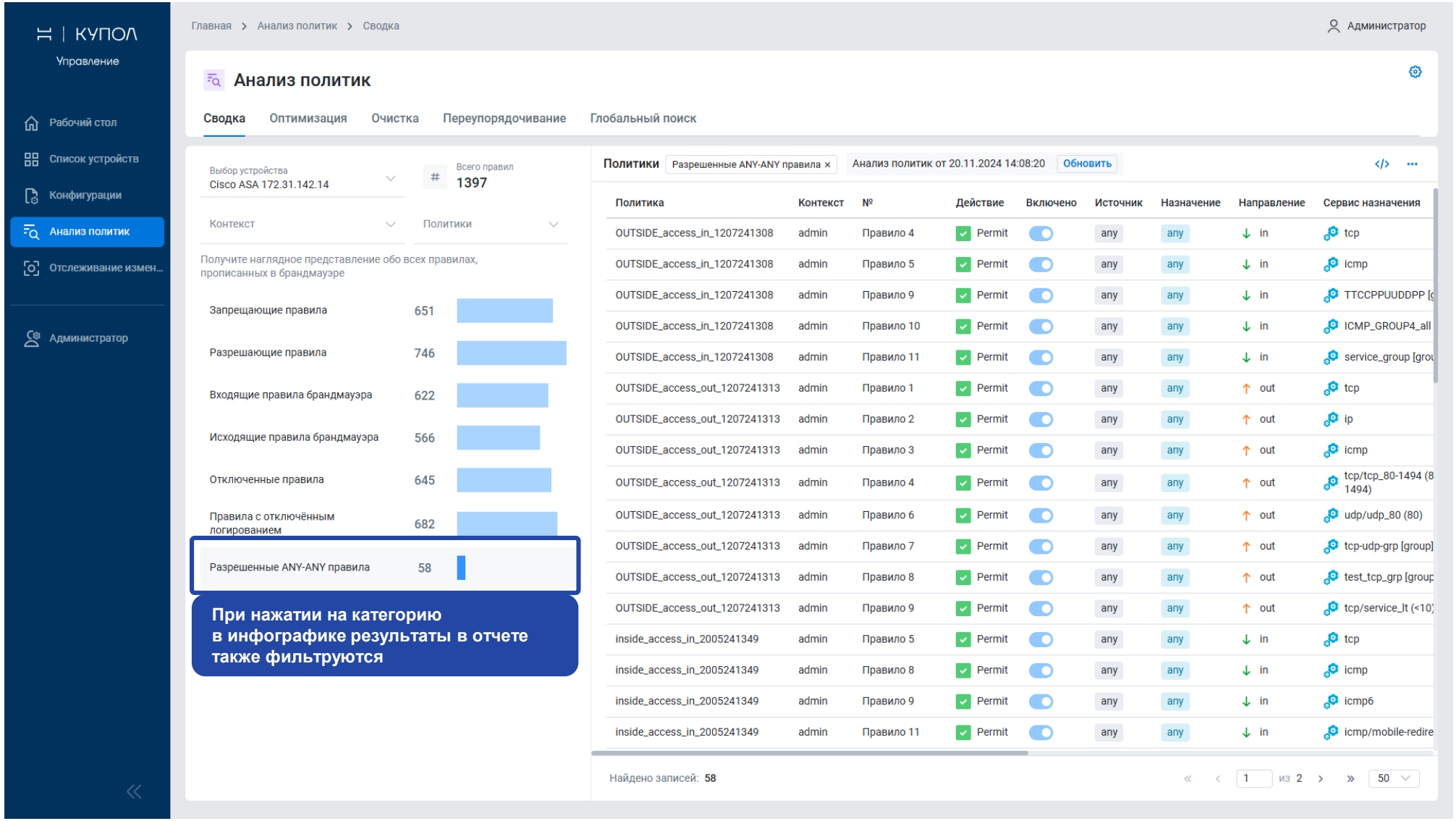
АНАЛИЗ ПОЛИТИК — СВОДКА



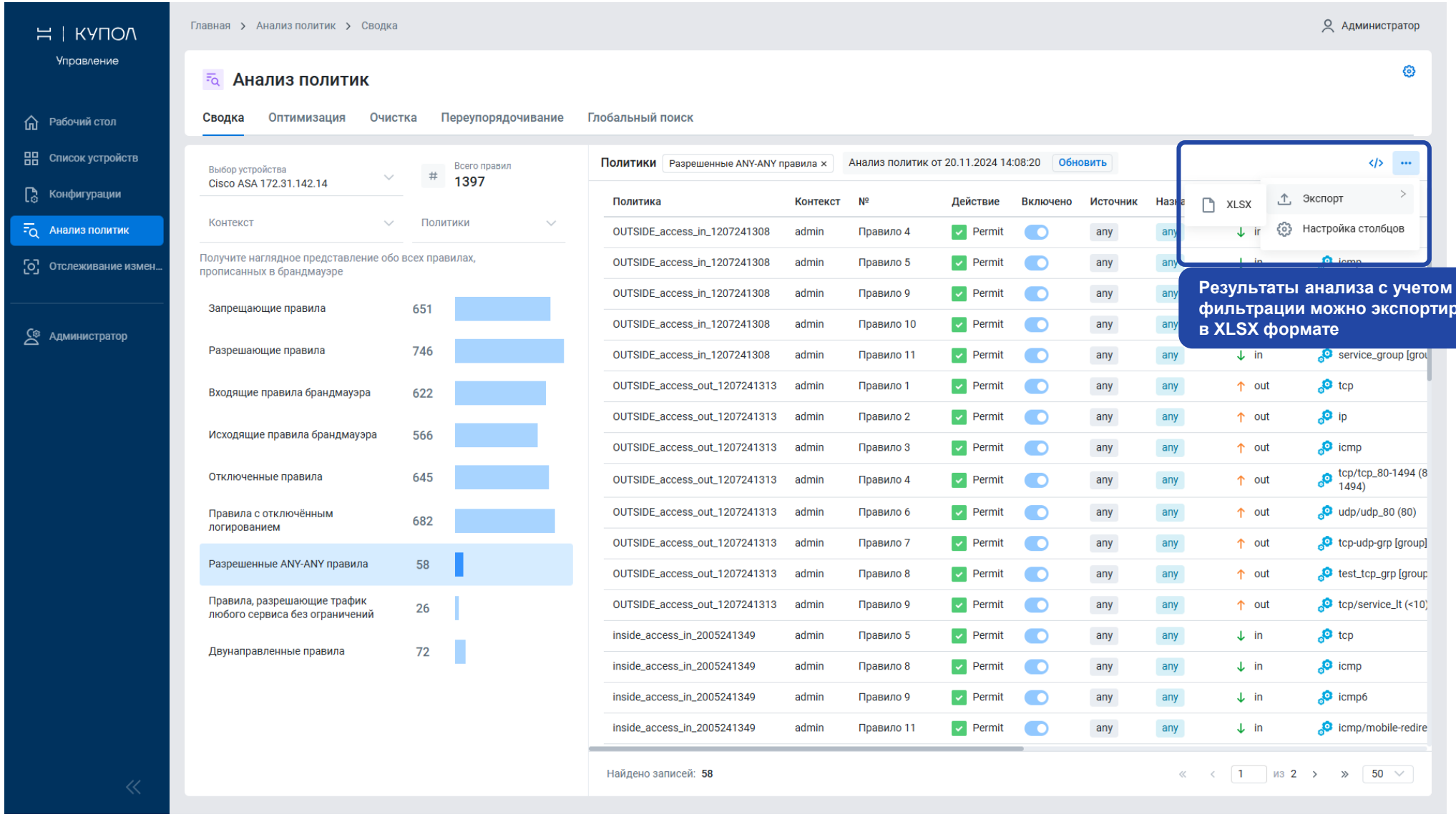
АНАЛИЗ ПОЛИТИК — СВОДКА



АНАЛИЗ ПОЛИТИК — СВОДКА

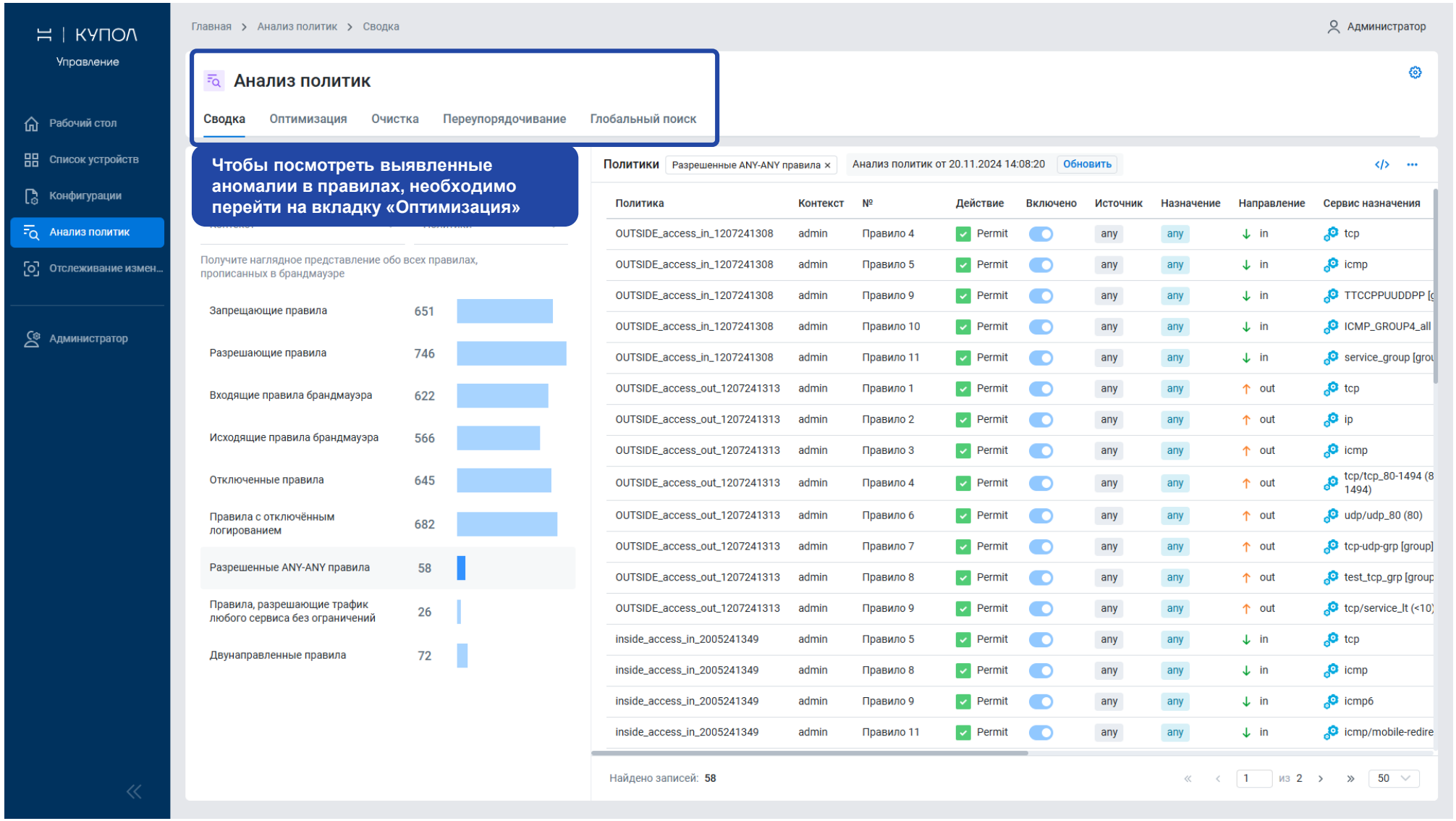


АНАЛИЗ ПОЛИТИК — СВОДКА



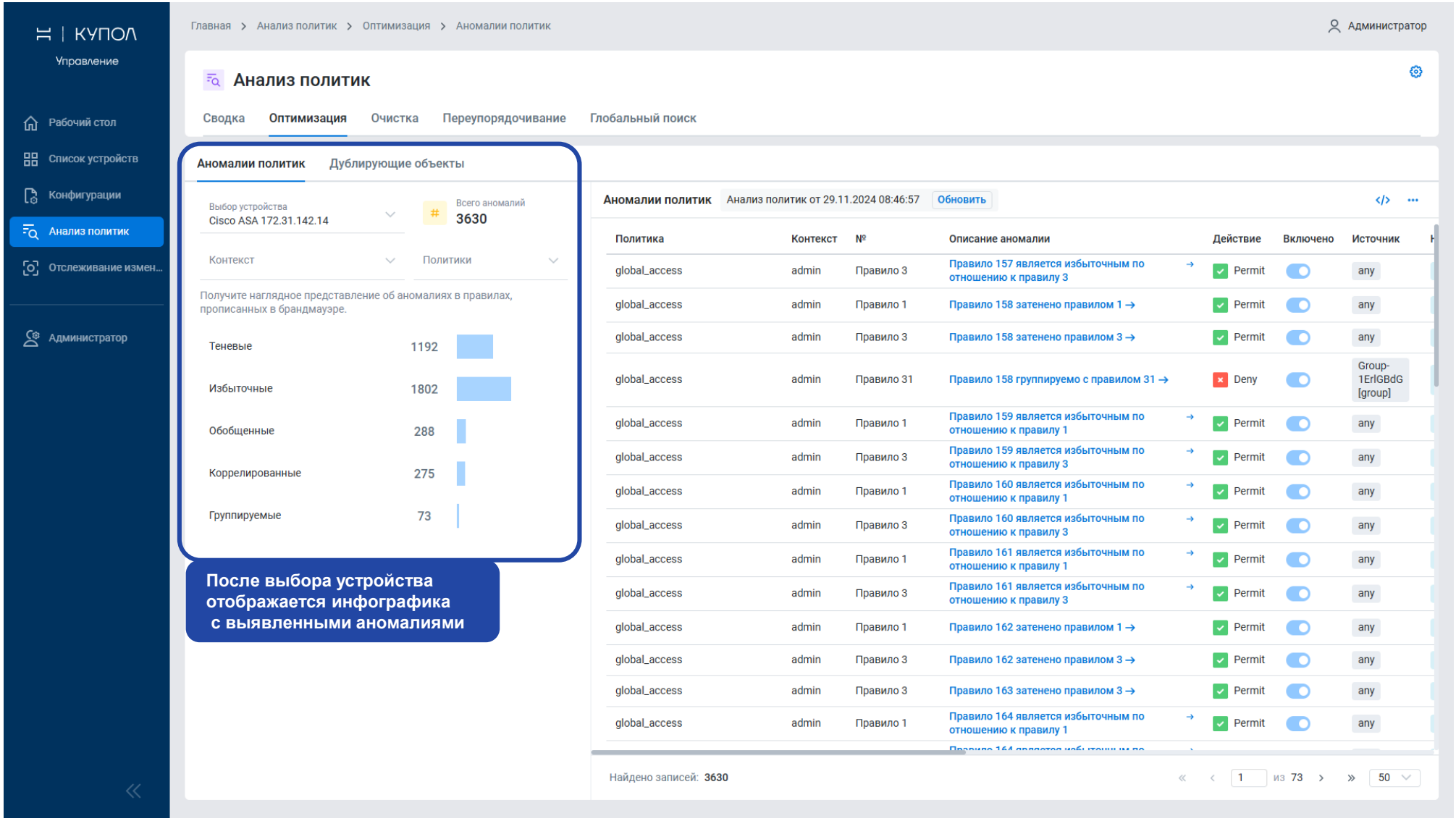
АНАЛИЗ ПОЛИТИК — АНОМАЛИИ ПОЛИТИК

НСТС | КУПОЛ

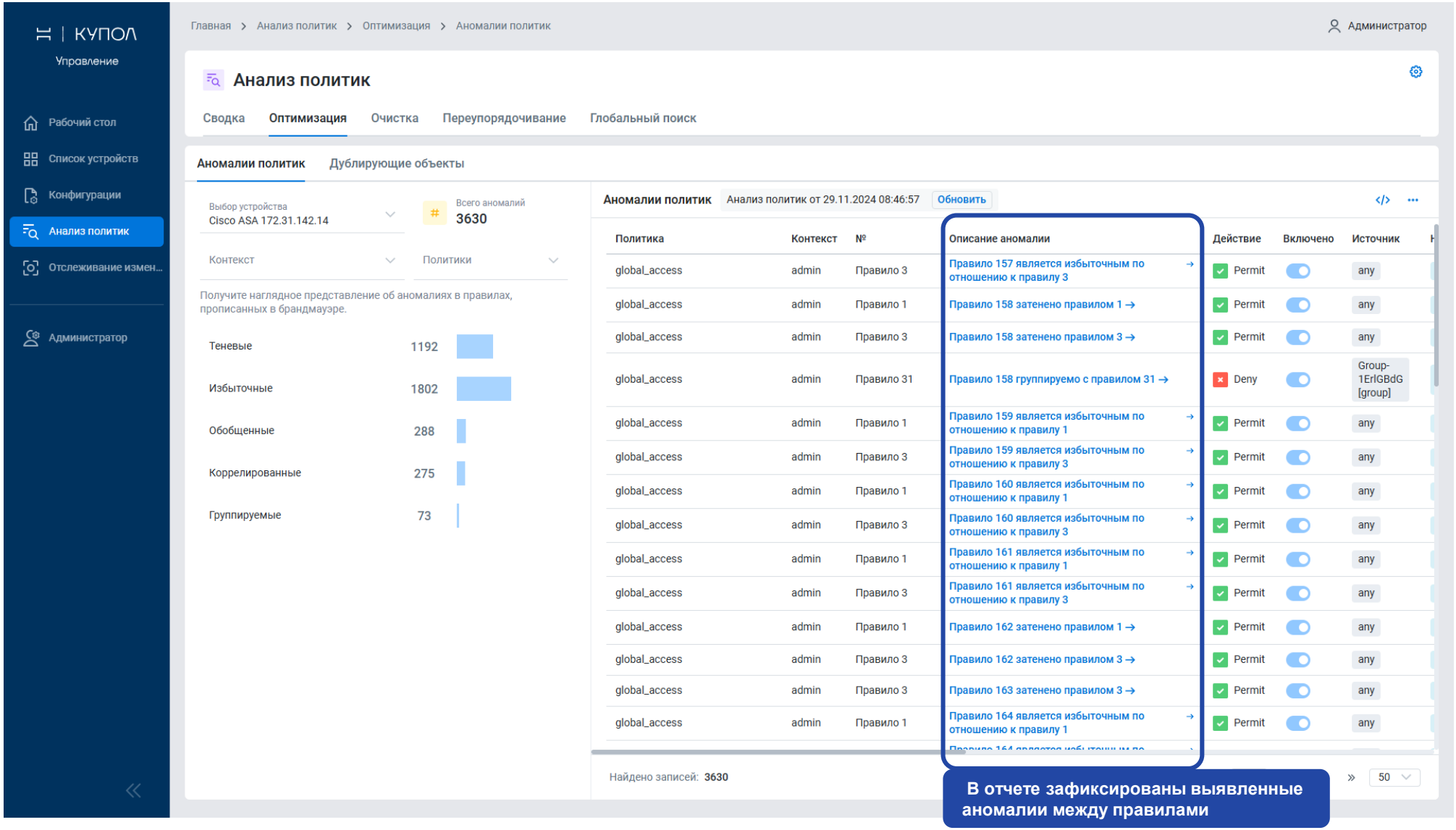


АНАЛИЗ ПОЛИТИК — АНОМАЛИИ ПОЛИТИК

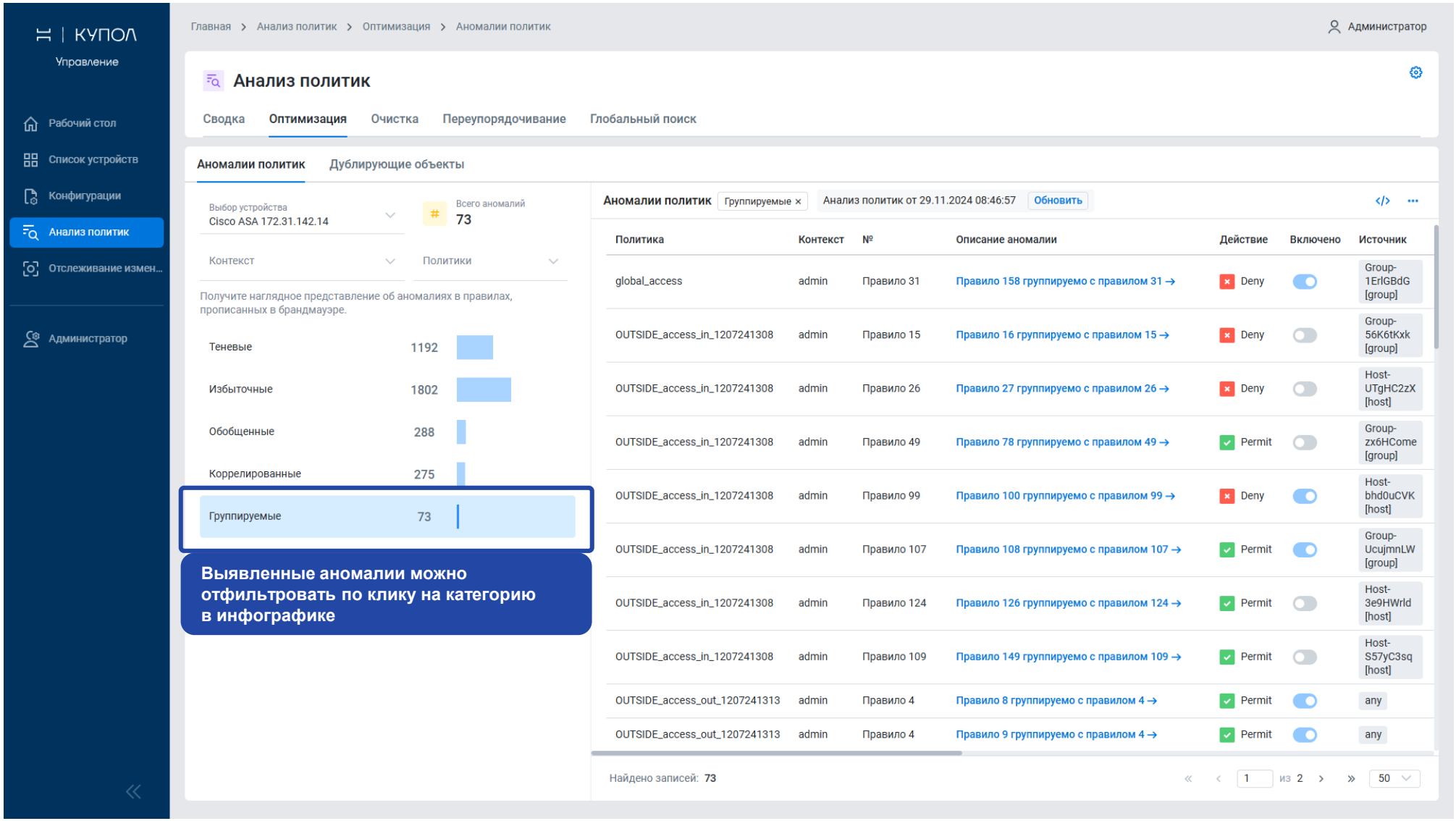
НСТС | КУПОЛ



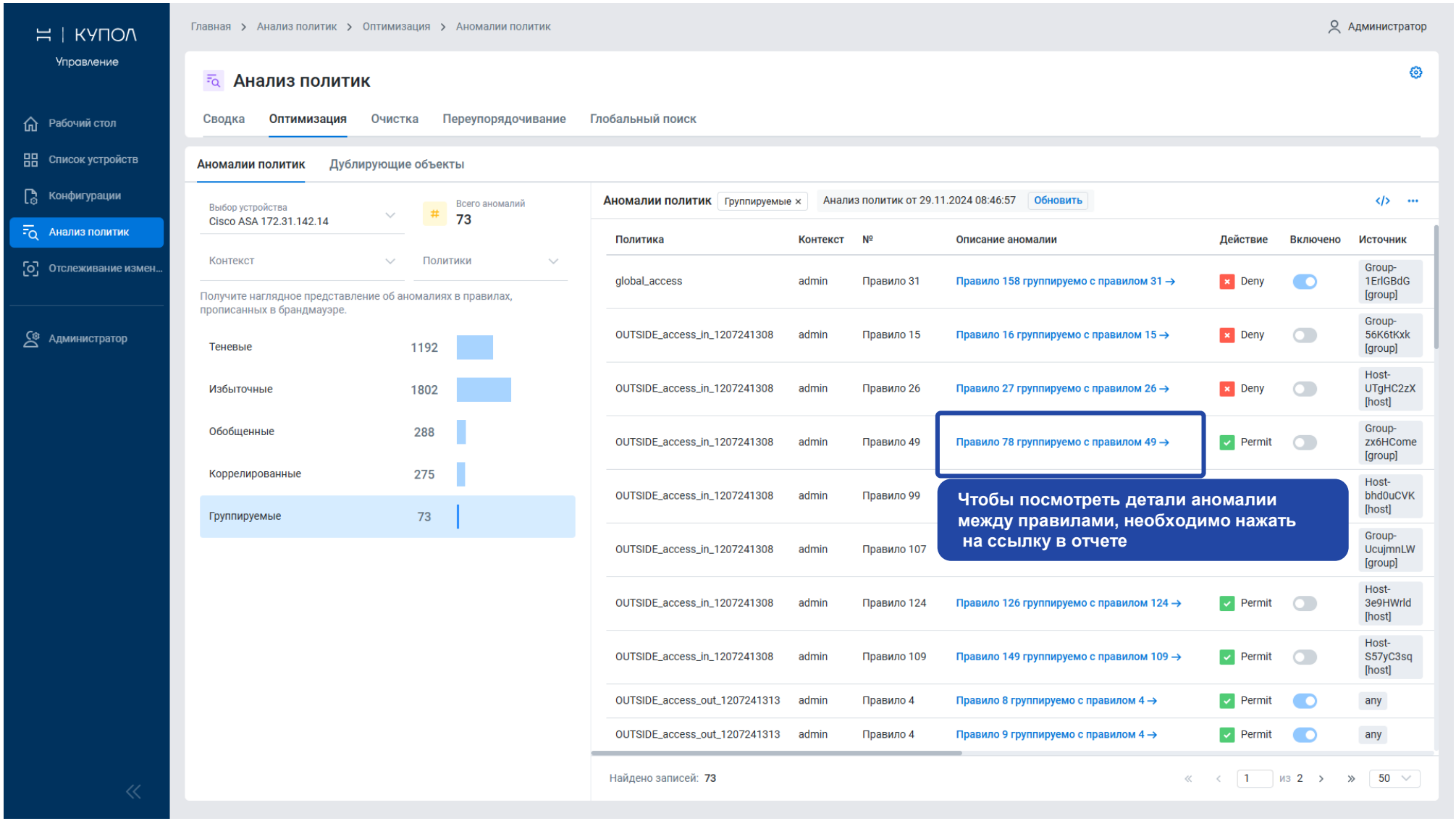
АНАЛИЗ ПОЛИТИК — АНОМАЛИИ ПОЛИТИК



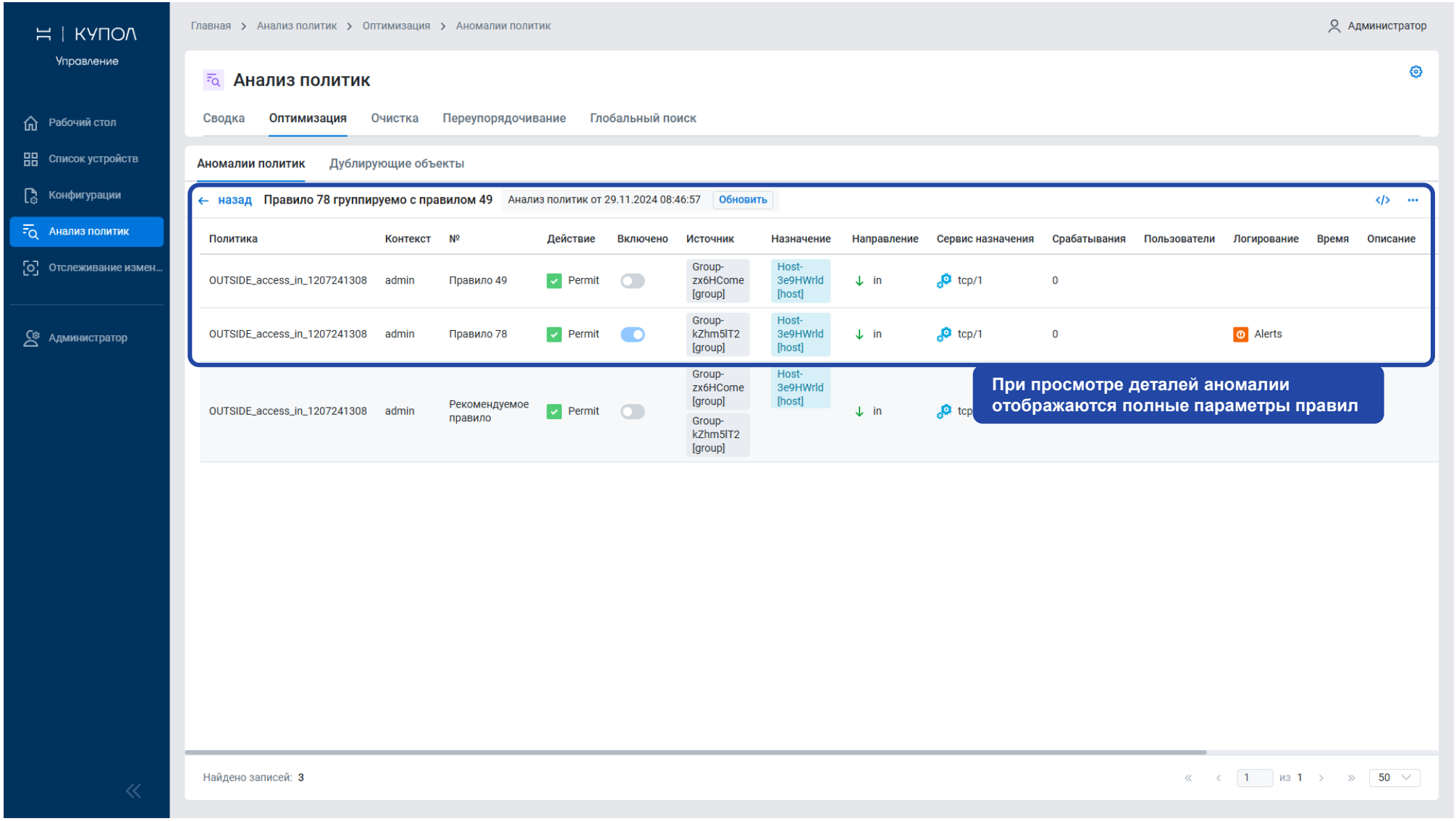
АНАЛИЗ ПОЛИТИК — АНОМАЛИИ ПОЛИТИК



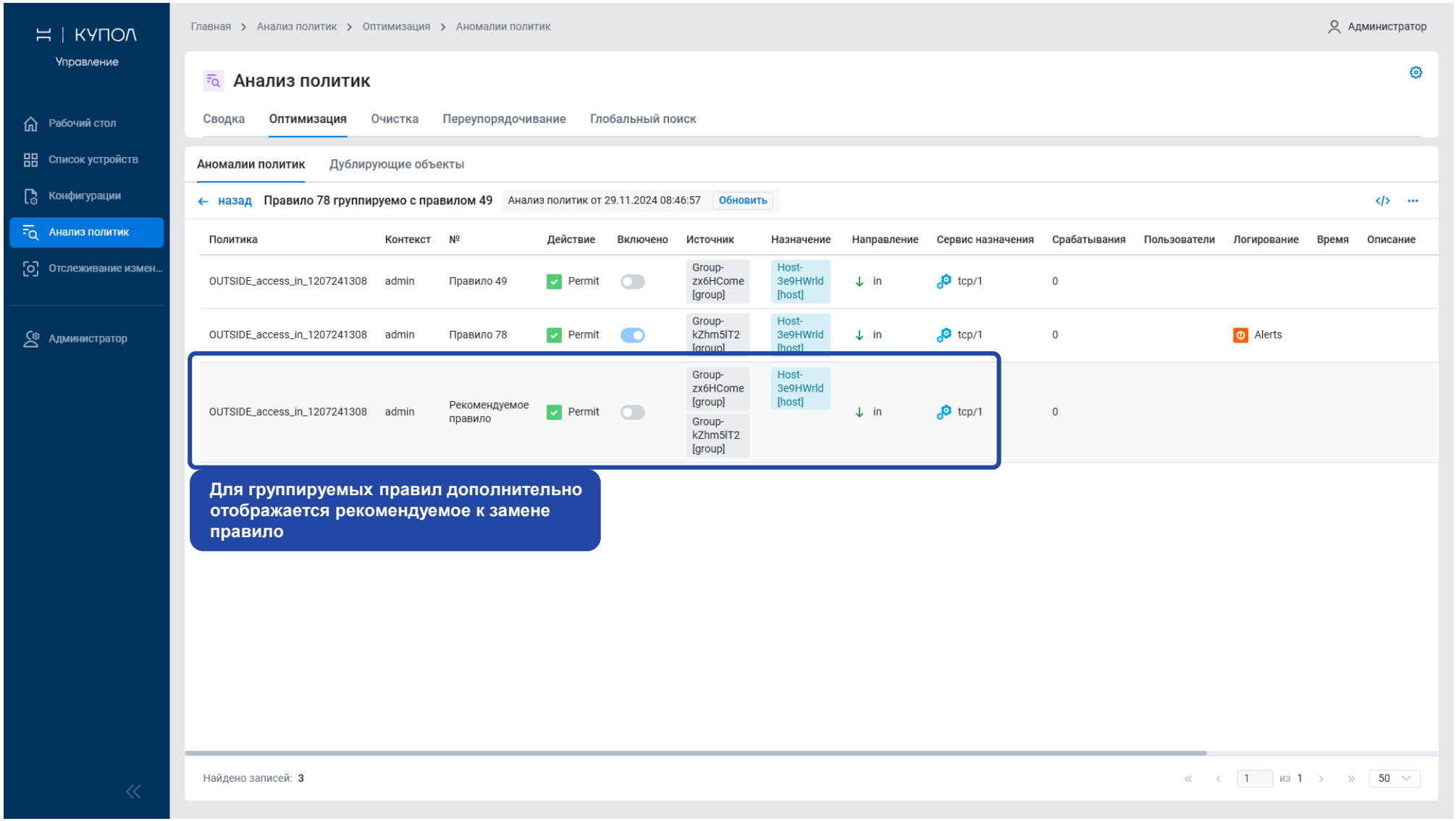
АНАЛИЗ ПОЛИТИК — АНОМАЛИИ ПОЛИТИК



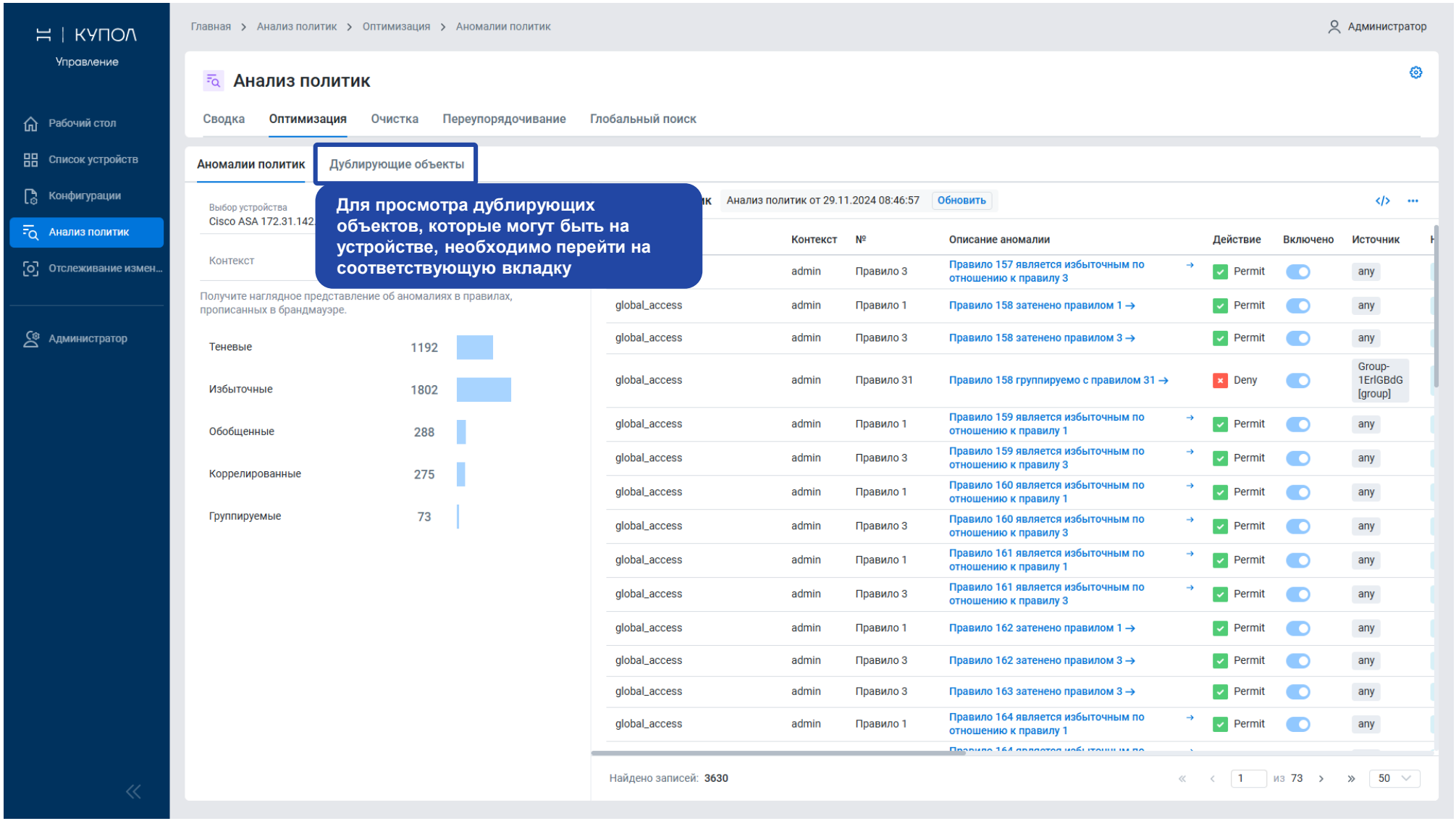
АНАЛИЗ ПОЛИТИК — АНОМАЛИИ ПОЛИТИК



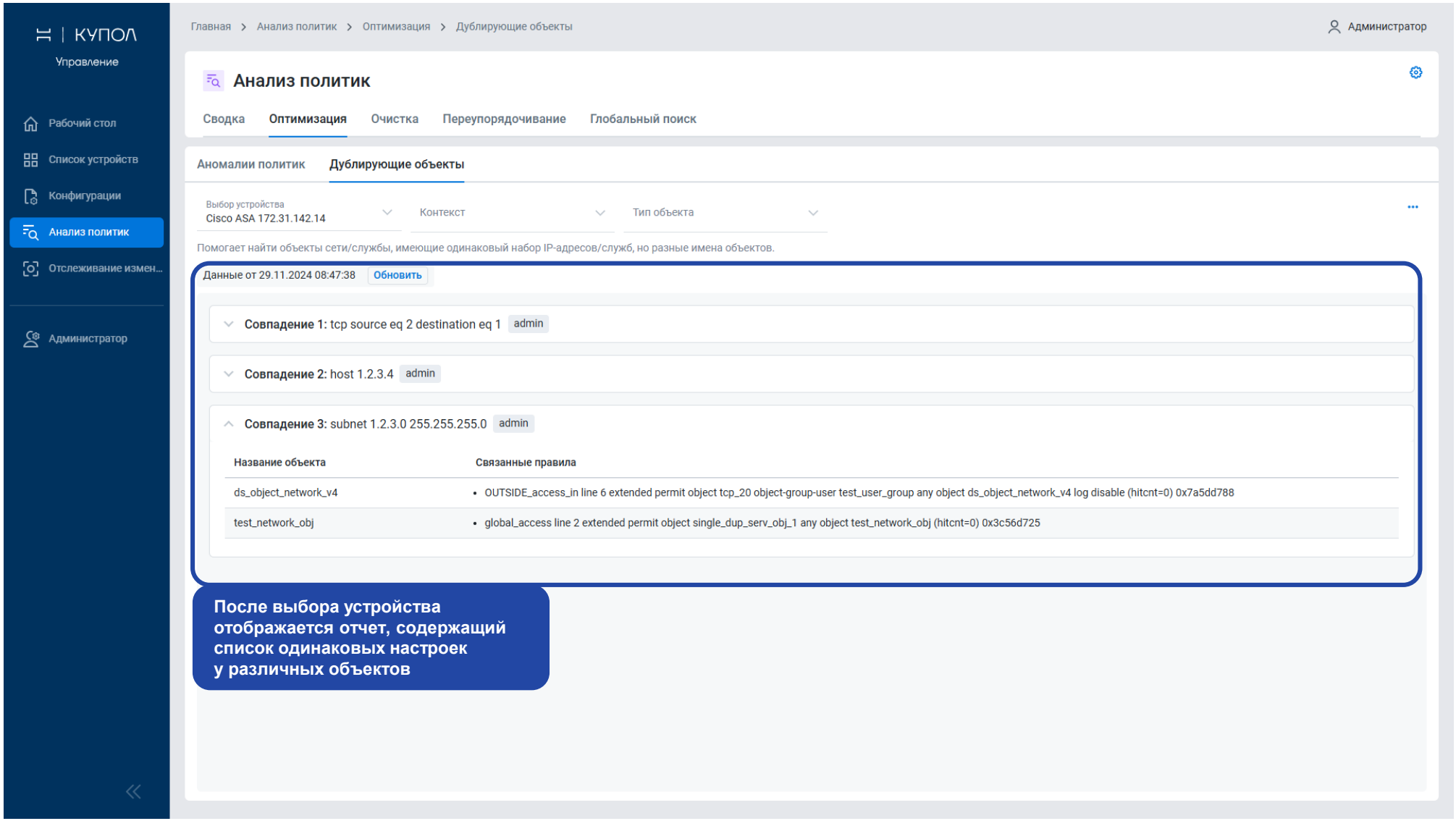
АНАЛИЗ ПОЛИТИК — АНОМАЛИИ ПОЛИТИК



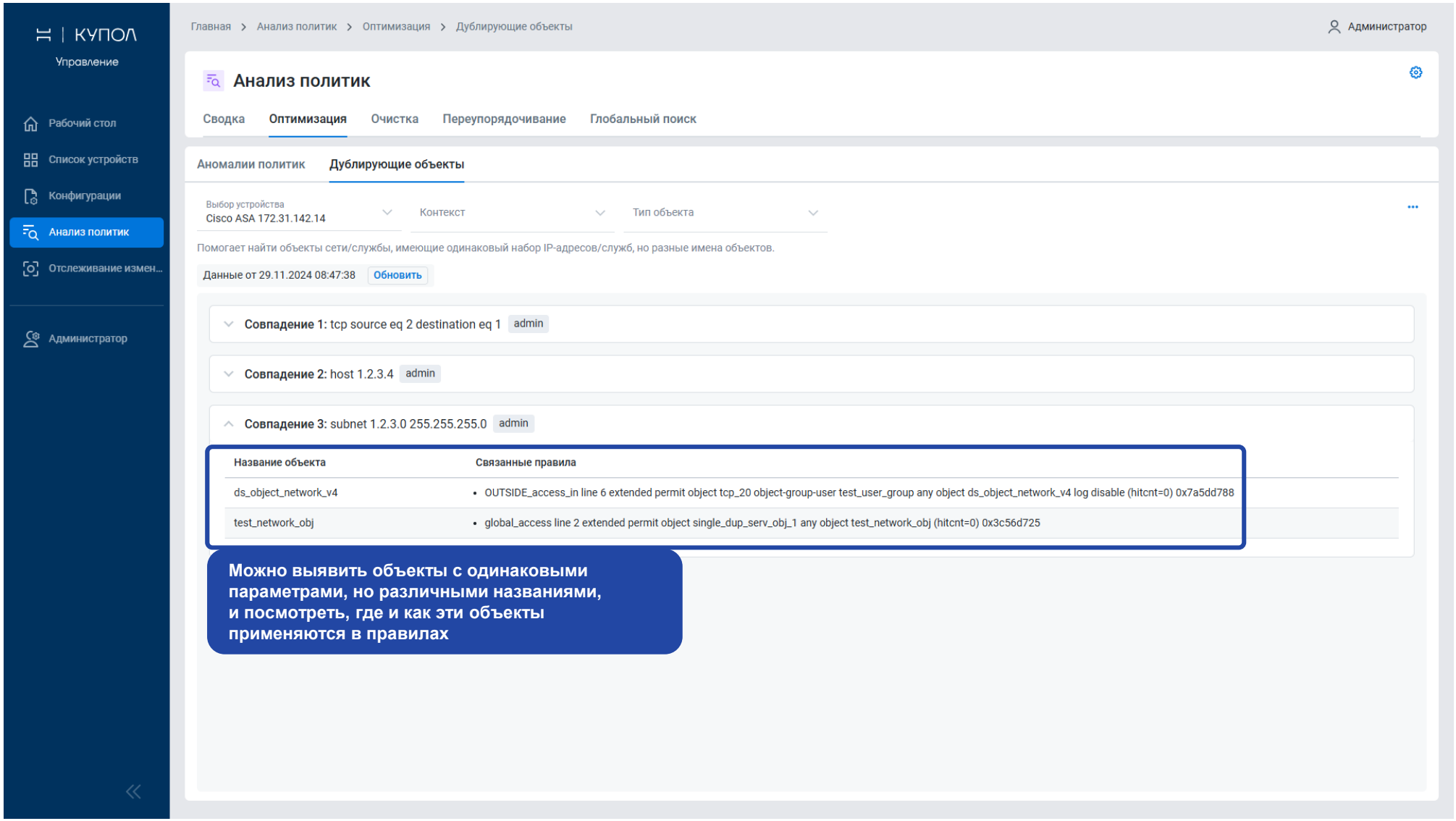
АНАЛИЗ ПОЛИТИК — ДУБЛИРУЮЩИЕ ОБЪЕКТЫ



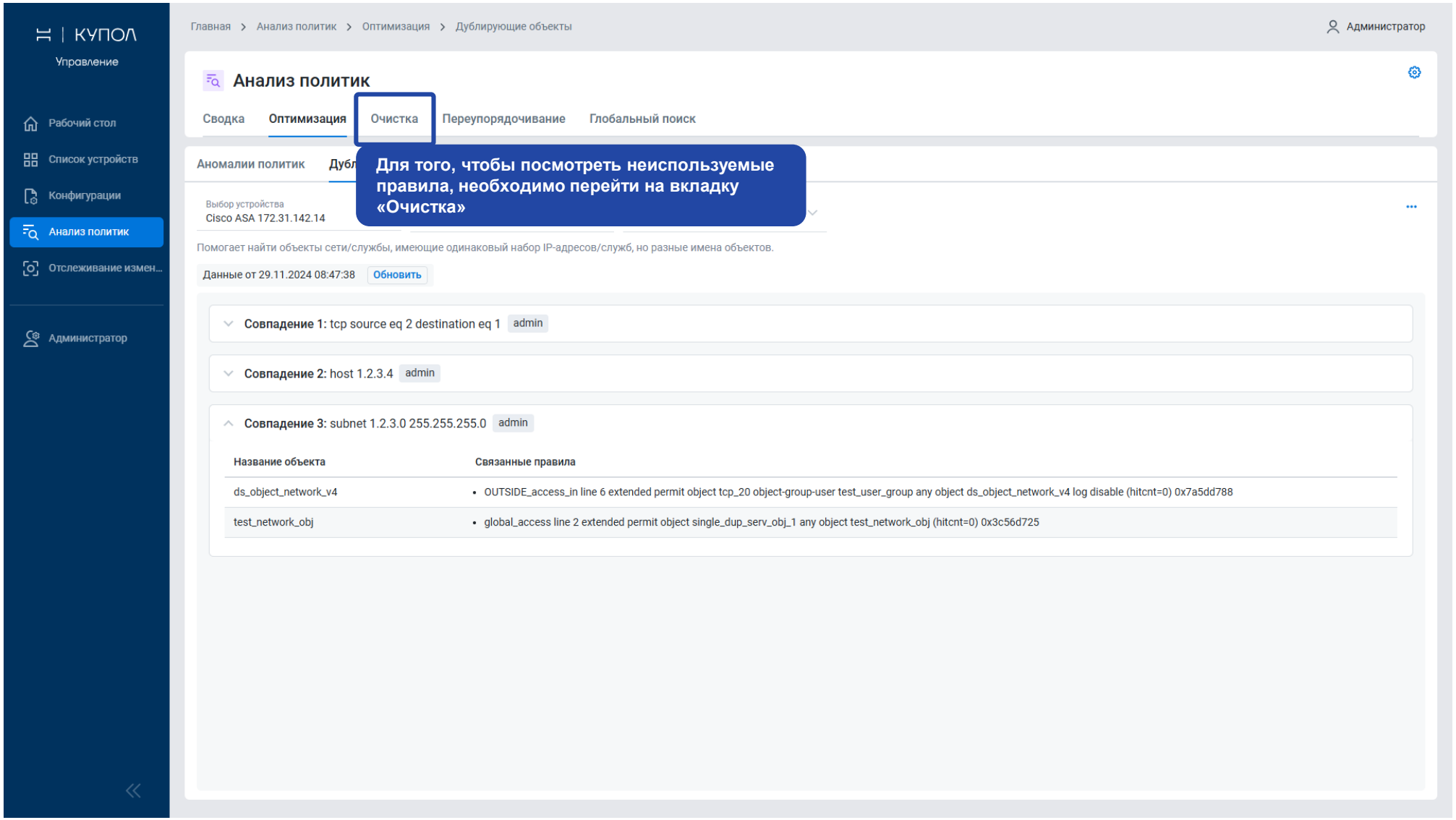
АНАЛИЗ ПОЛИТИК — ДУБЛИРУЮЩИЕ ОБЪЕКТЫ



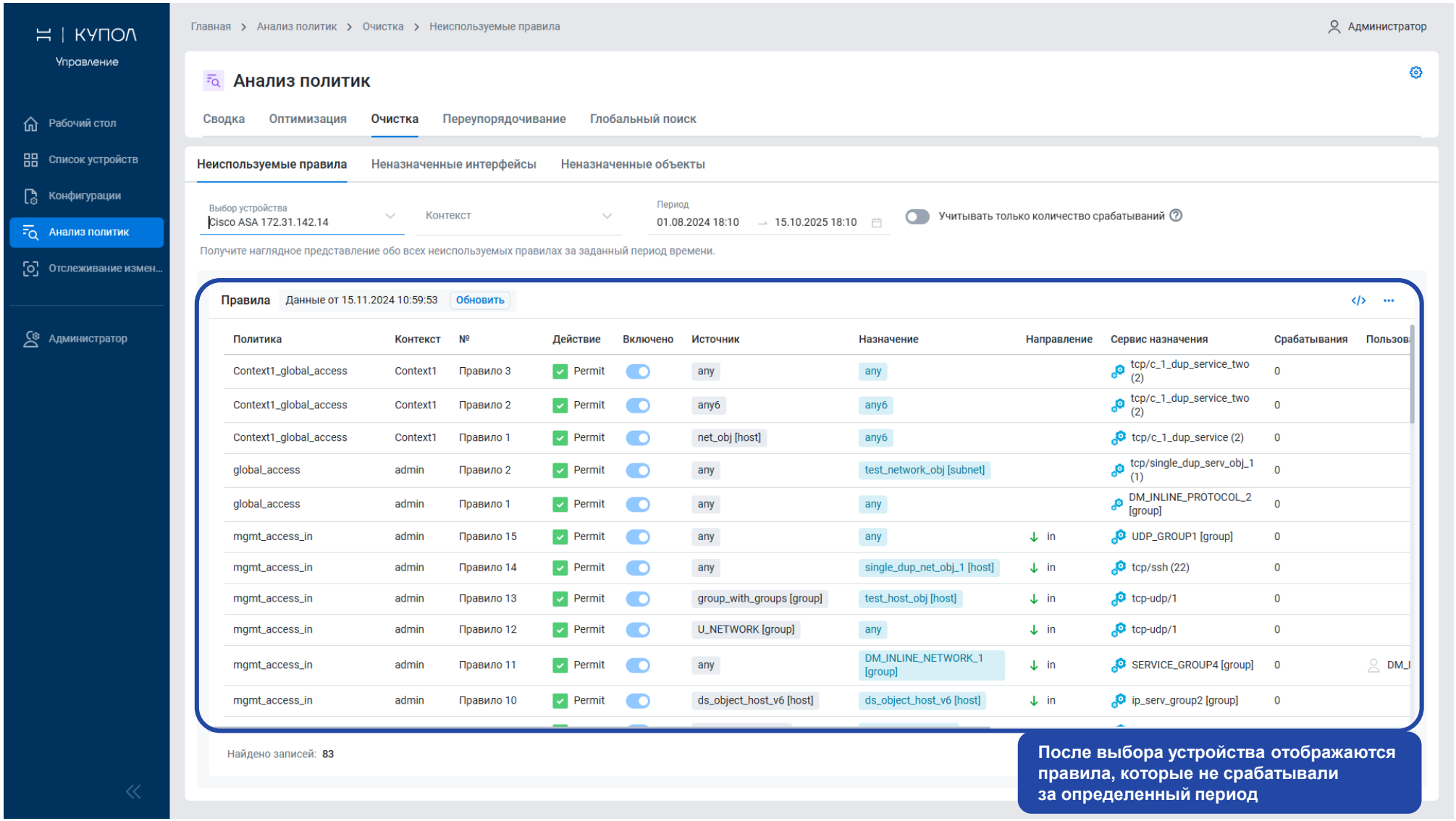
АНАЛИЗ ПОЛИТИК — ДУБЛИРУЮЩИЕ ОБЪЕКТЫ



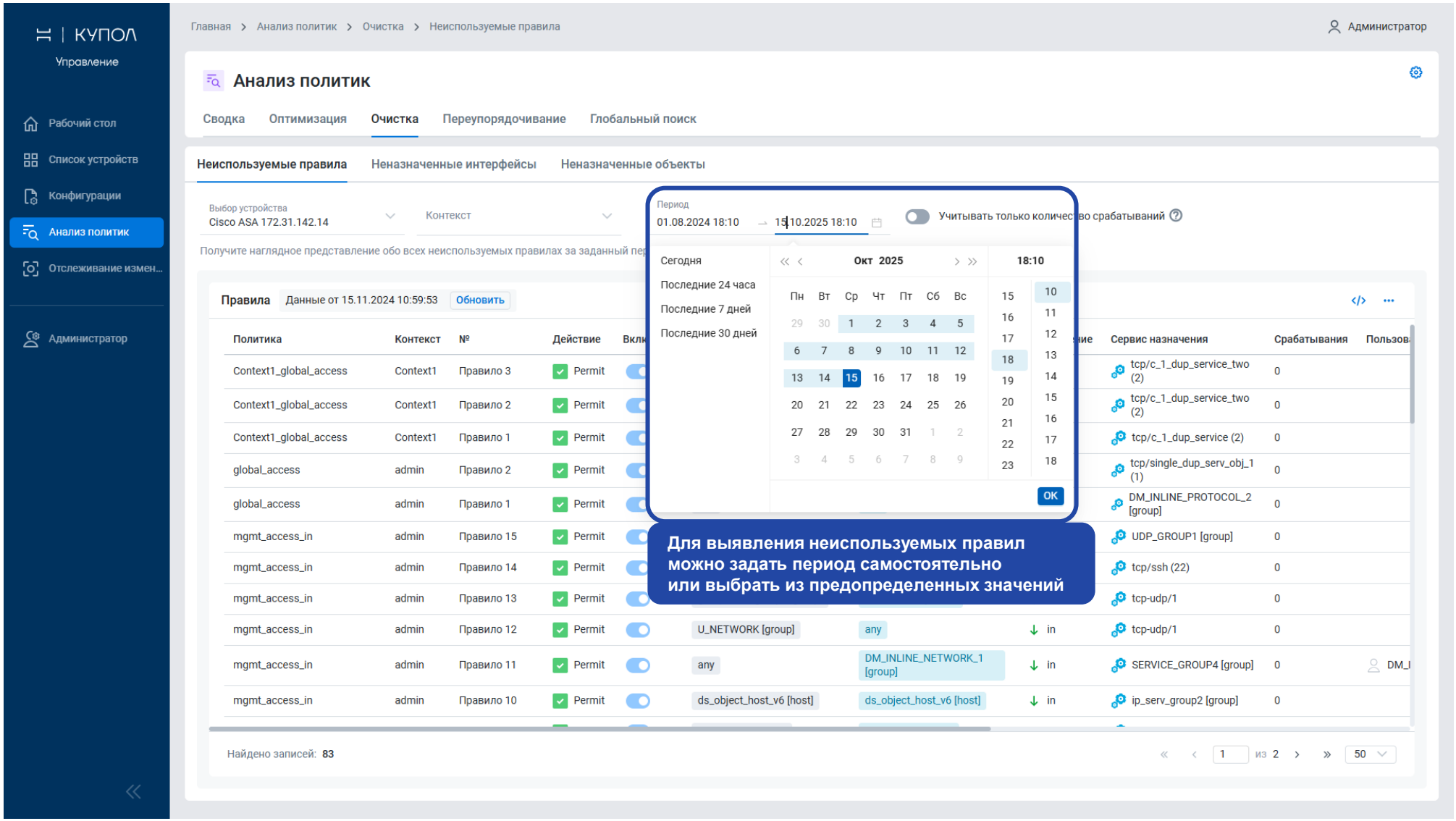
АНАЛИЗ ПОЛИТИК — НЕИСПОЛЬЗУЕМЫЕ ПРАВИЛА



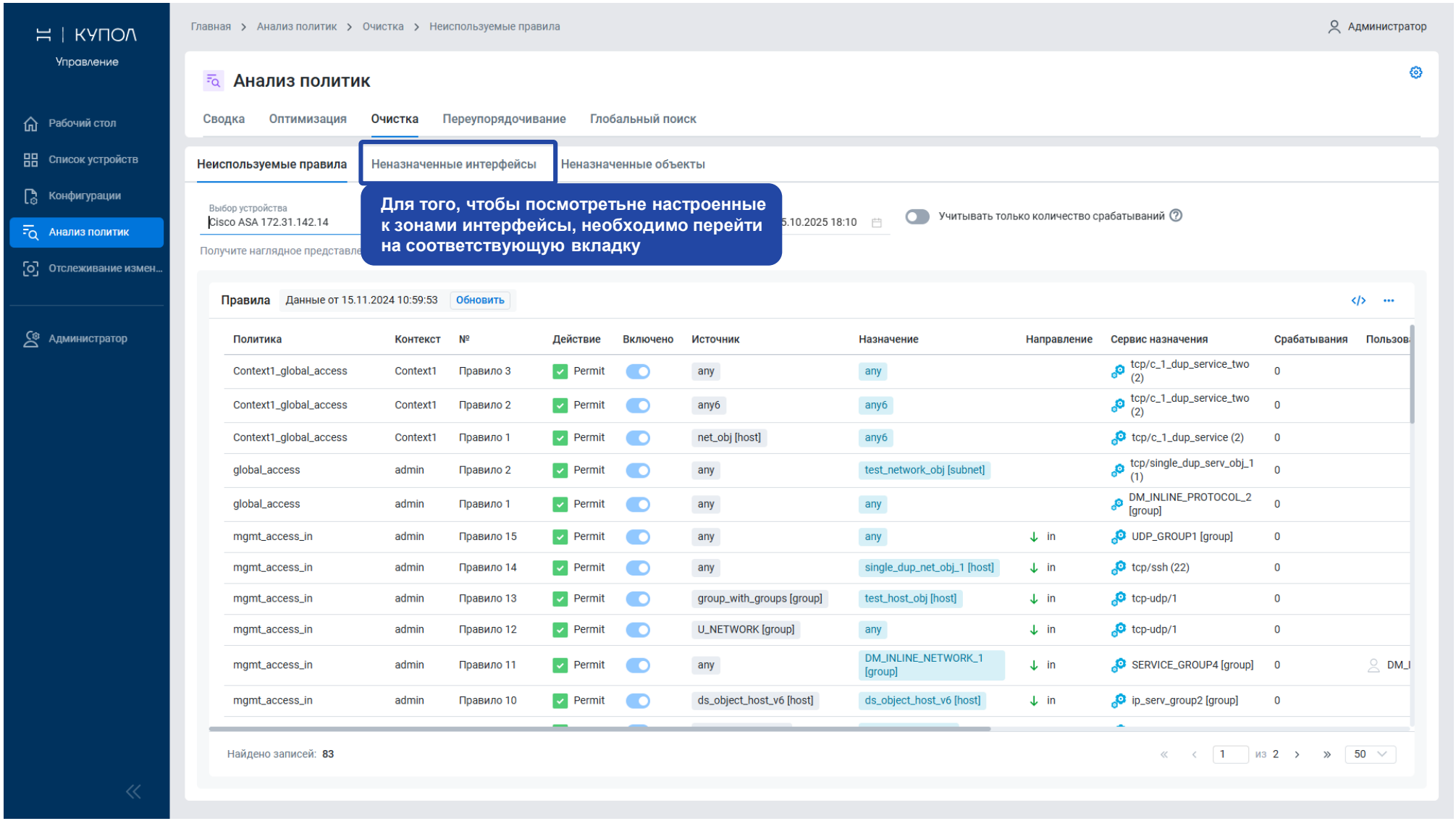
АНАЛИЗ ПОЛИТИК — НЕИСПОЛЬЗУЕМЫЕ ПРАВИЛА



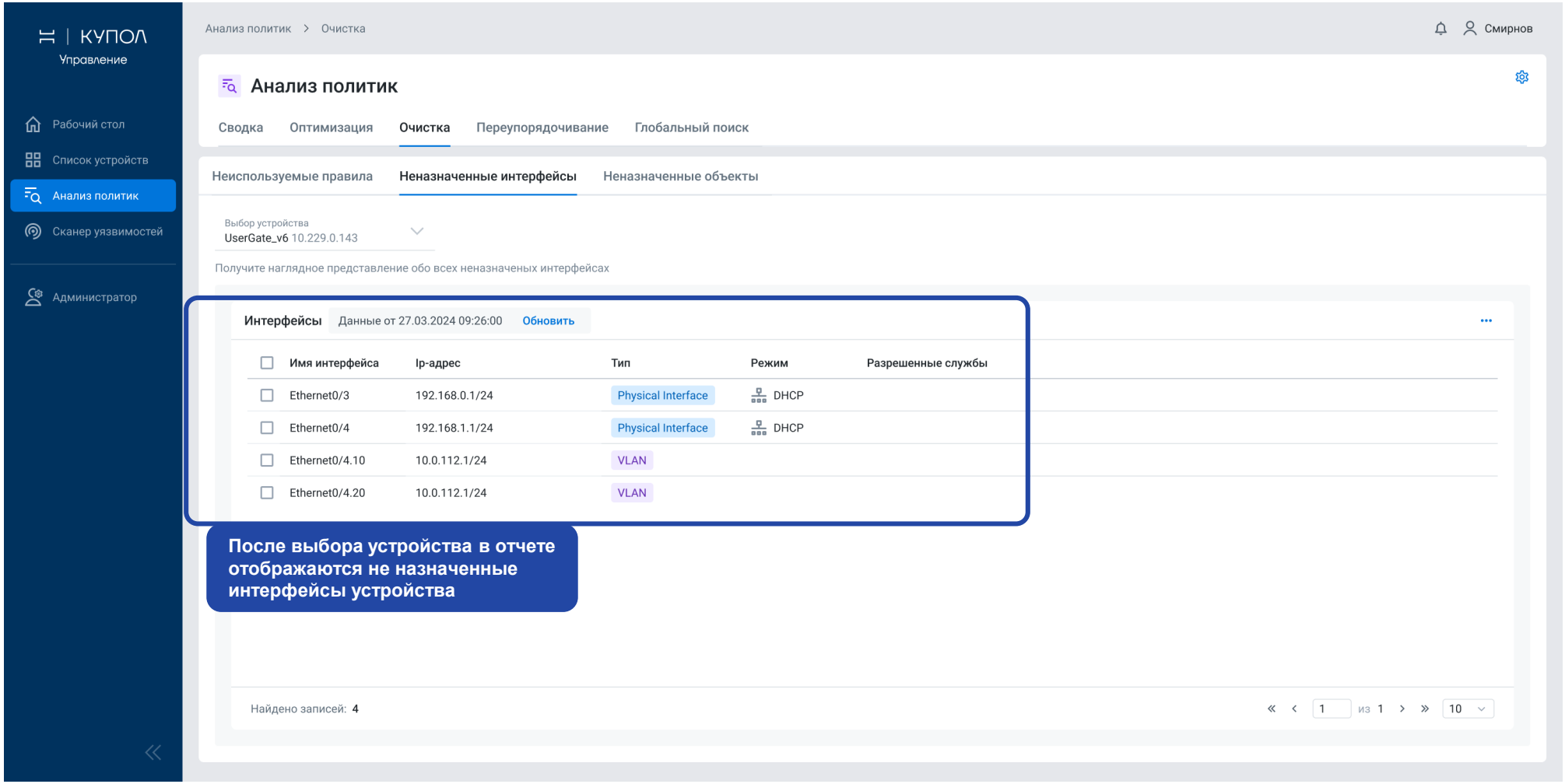
АНАЛИЗ ПОЛИТИК — НЕИСПОЛЬЗУЕМЫЕ ПРАВИЛА



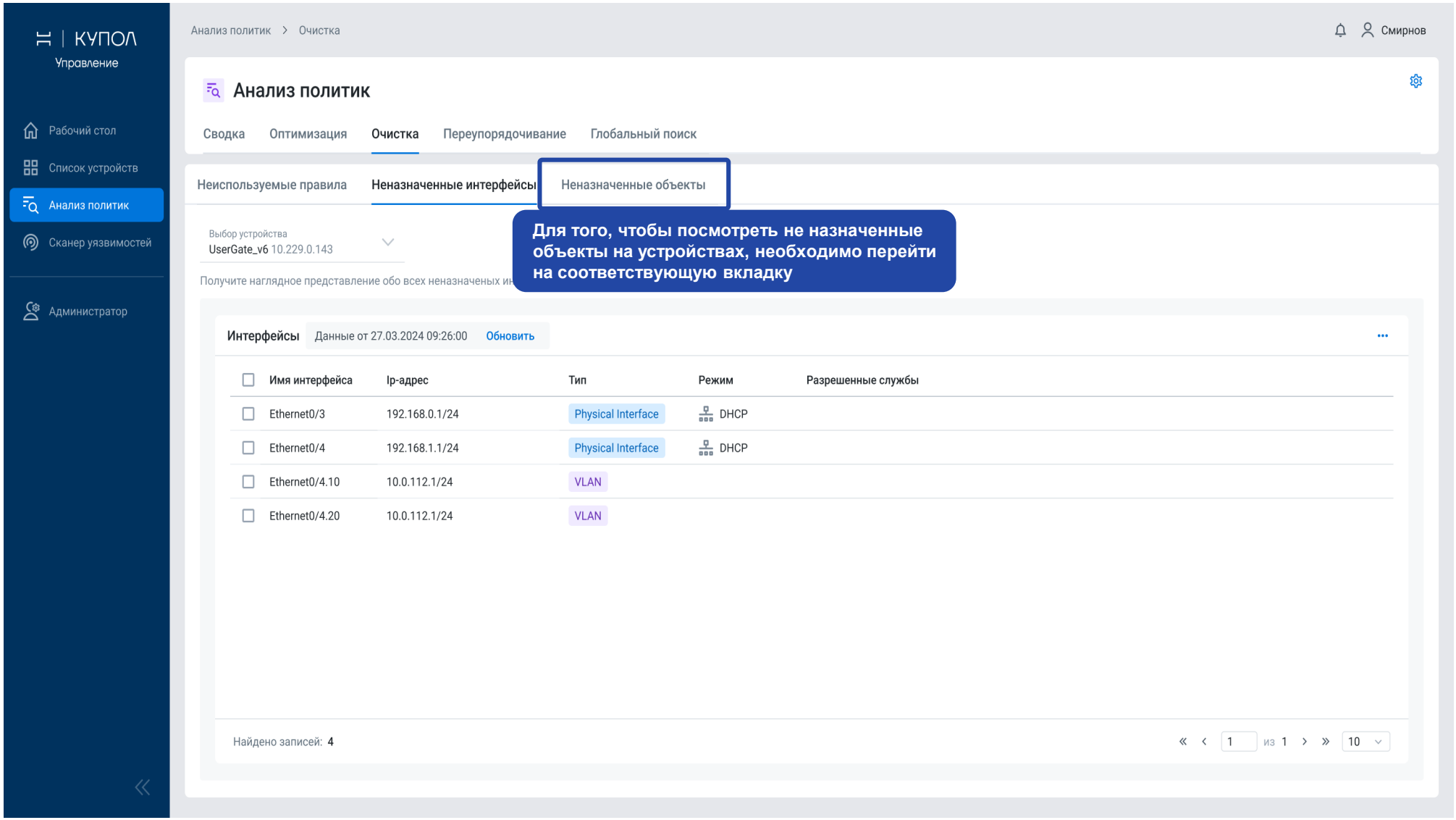
АНАЛИЗ ПОЛИТИК — НЕНАЗНАЧЕННЫЕ ИНТЕРФЕЙСЫ



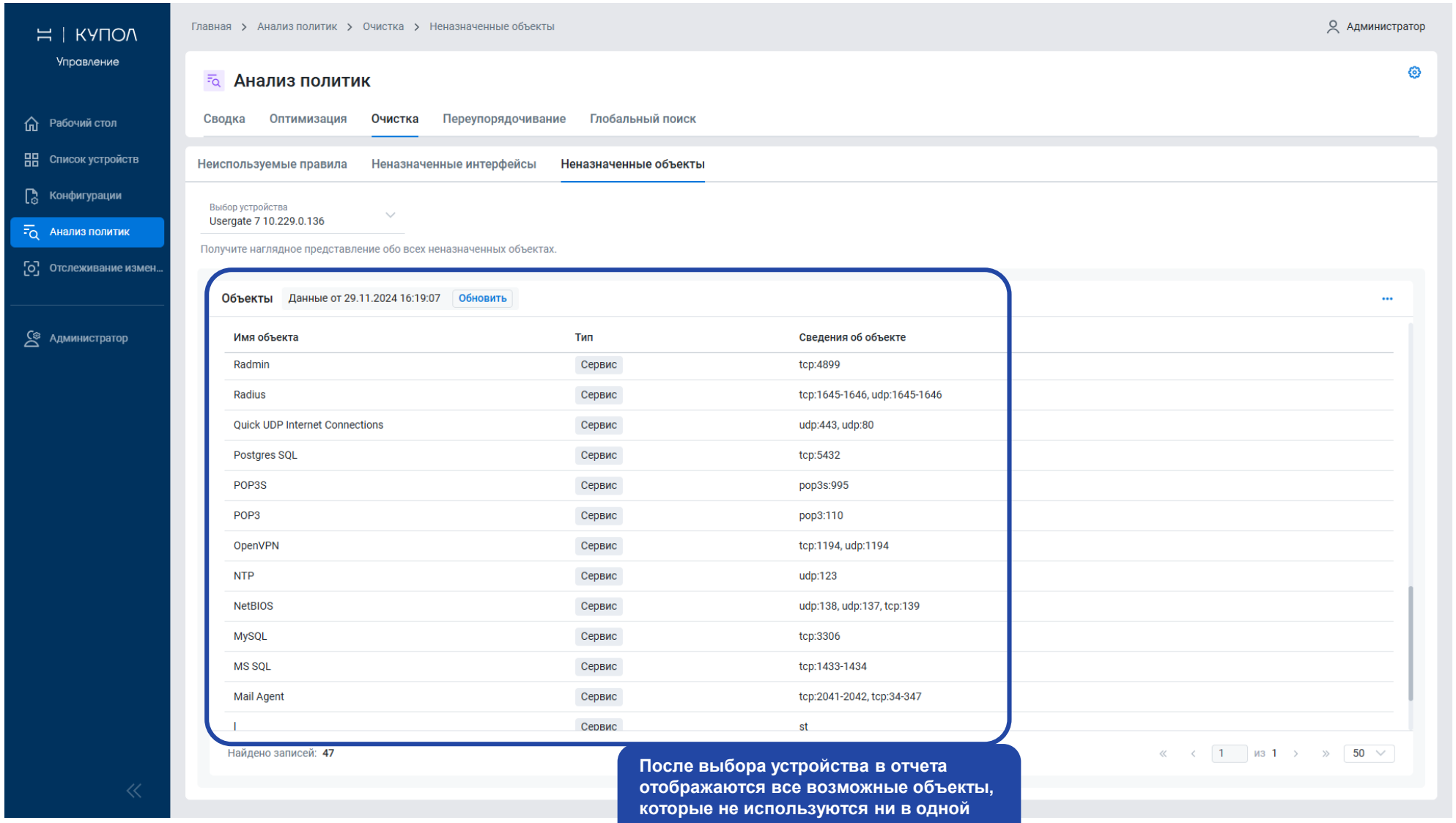
АНАЛИЗ ПОЛИТИК — НЕНАЗНАЧЕННЫЕ ИНТЕРФЕЙСЫ



АНАЛИЗ ПОЛИТИК — НЕНАЗНАЧЕННЫЕ ОБЪЕКТЫ

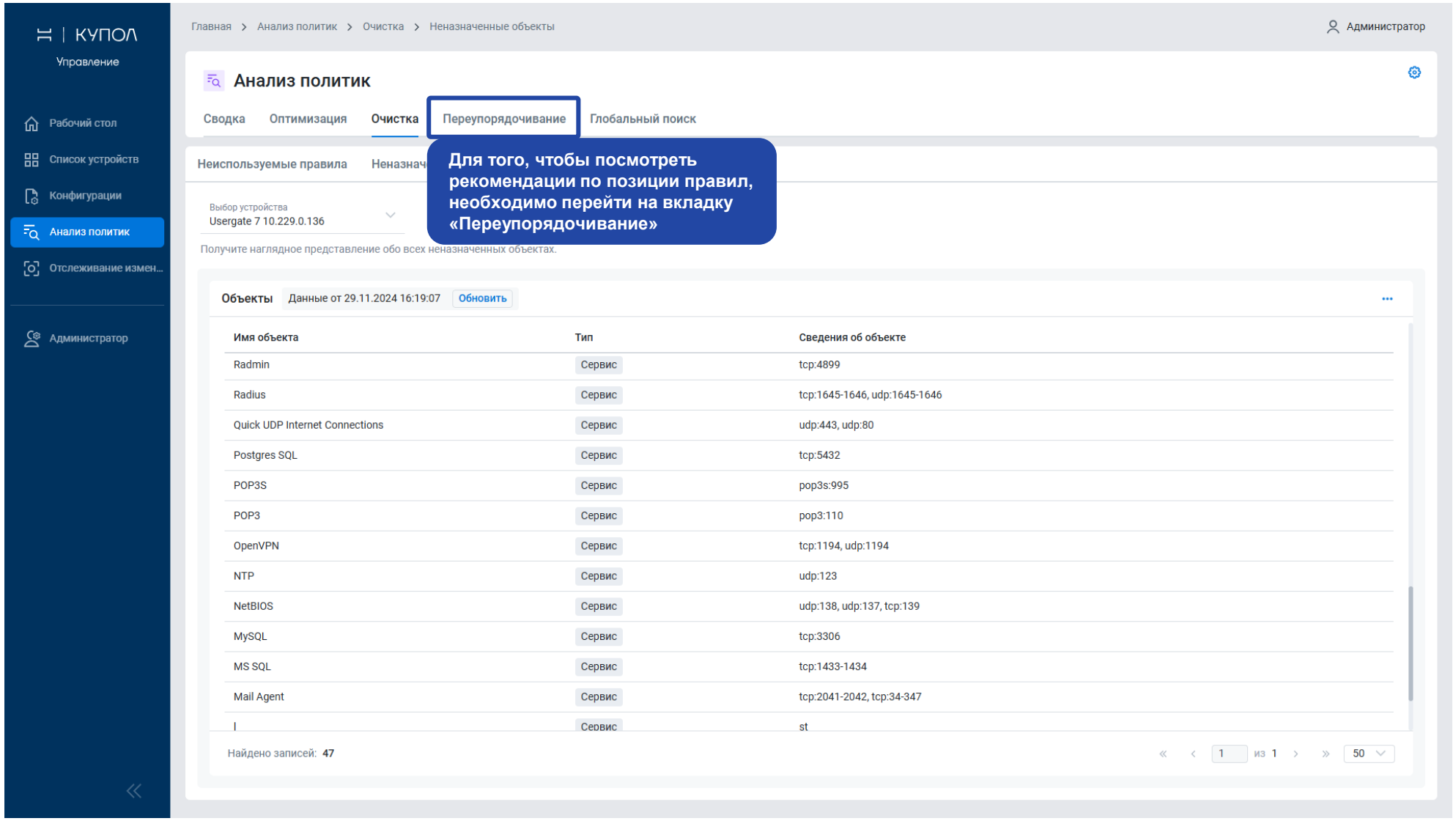


АНАЛИЗ ПОЛИТИК — НЕНАЗНАЧЕННЫЕ ОБЪЕКТЫ

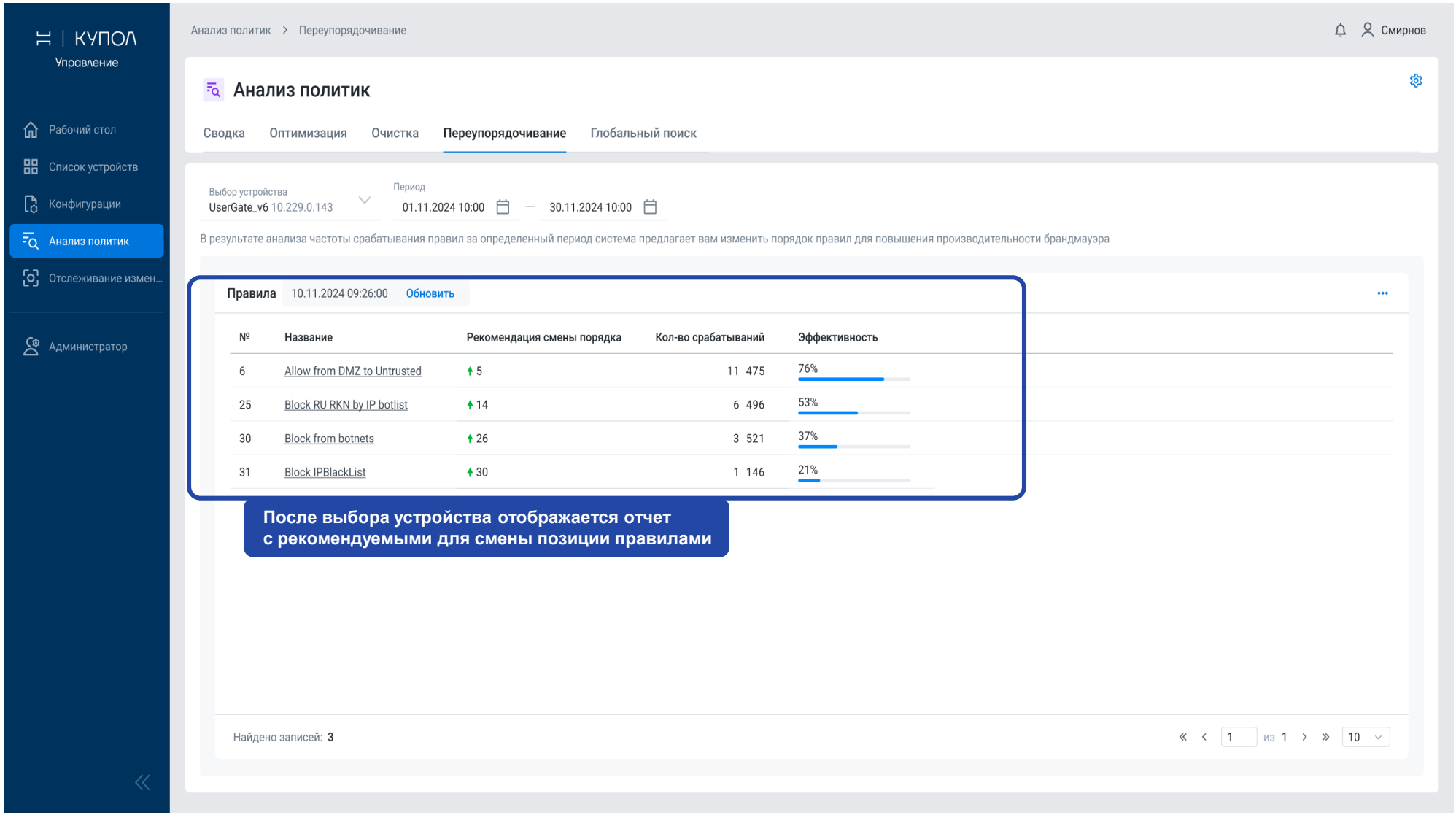


После выбора устройства в отчета отображаются все возможные объекты, которые не используются ни в одной политике

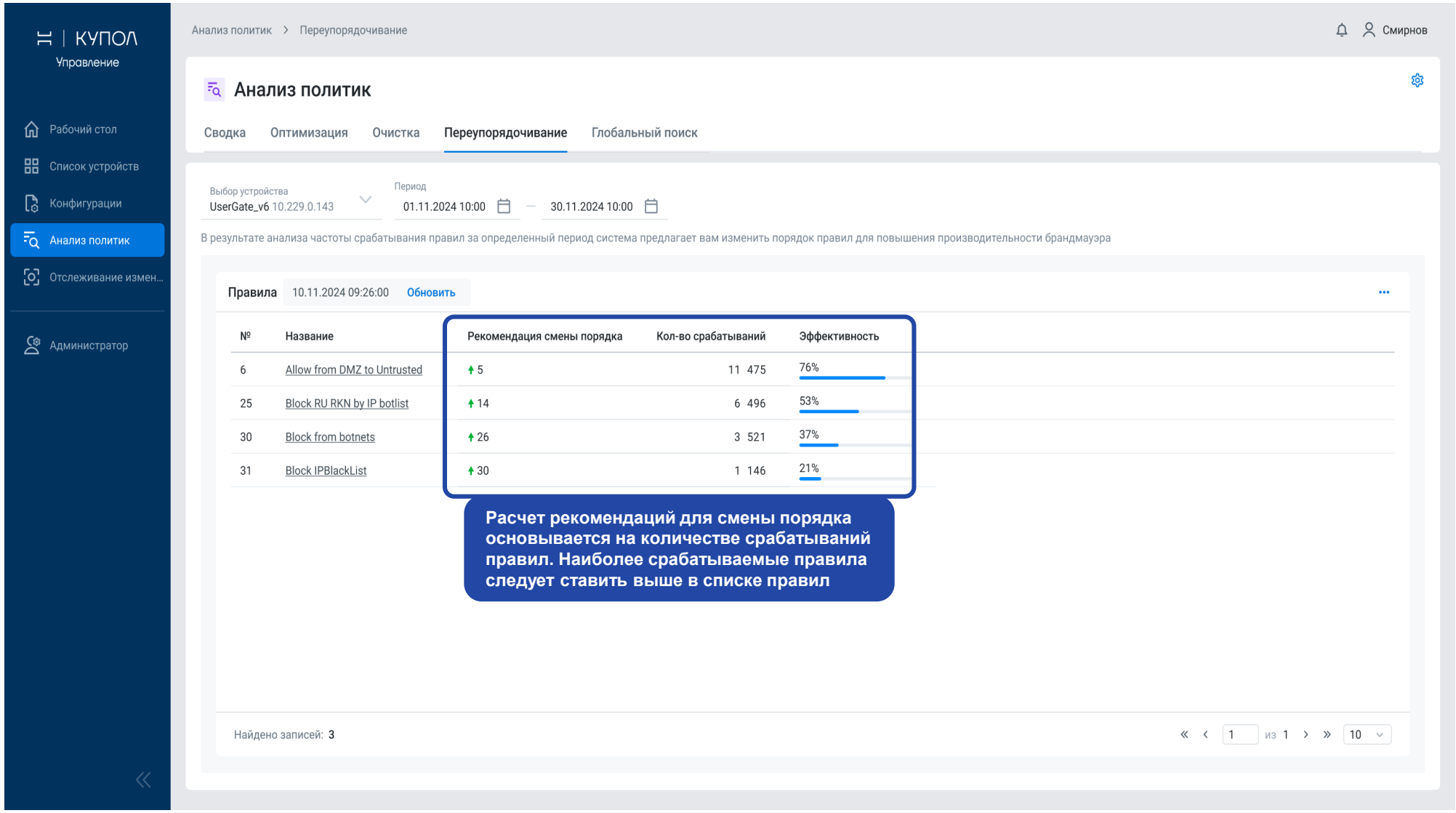
АНАЛИЗ ПОЛИТИК — ПЕРЕУПОРЯДОЧИВАНИЕ



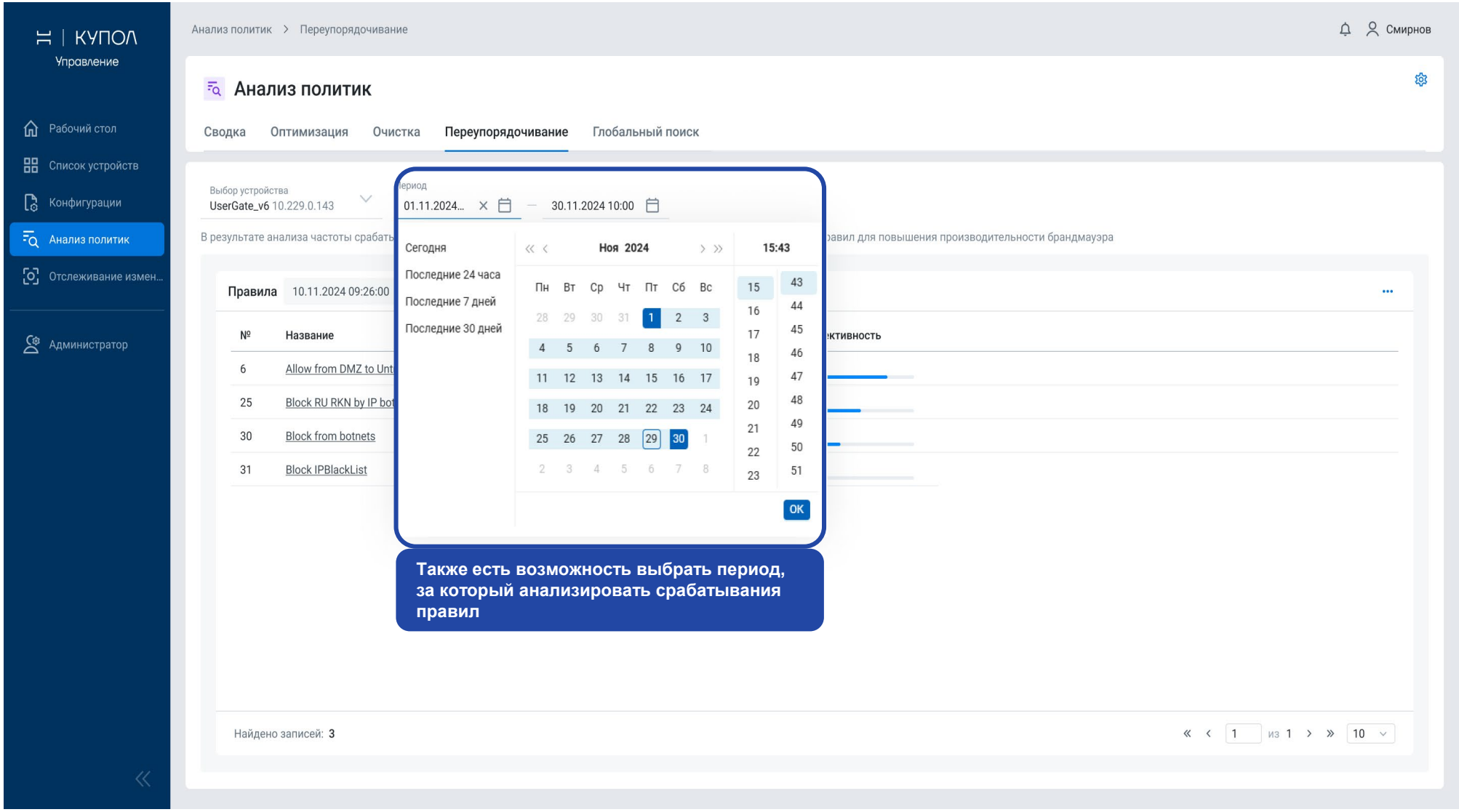
АНАЛИЗ ПОЛИТИК — ПЕРЕУПОРЯДОЧИВАНИЕ



АНАЛИЗ ПОЛИТИК — ПЕРЕУПОРЯДОЧИВАНИЕ

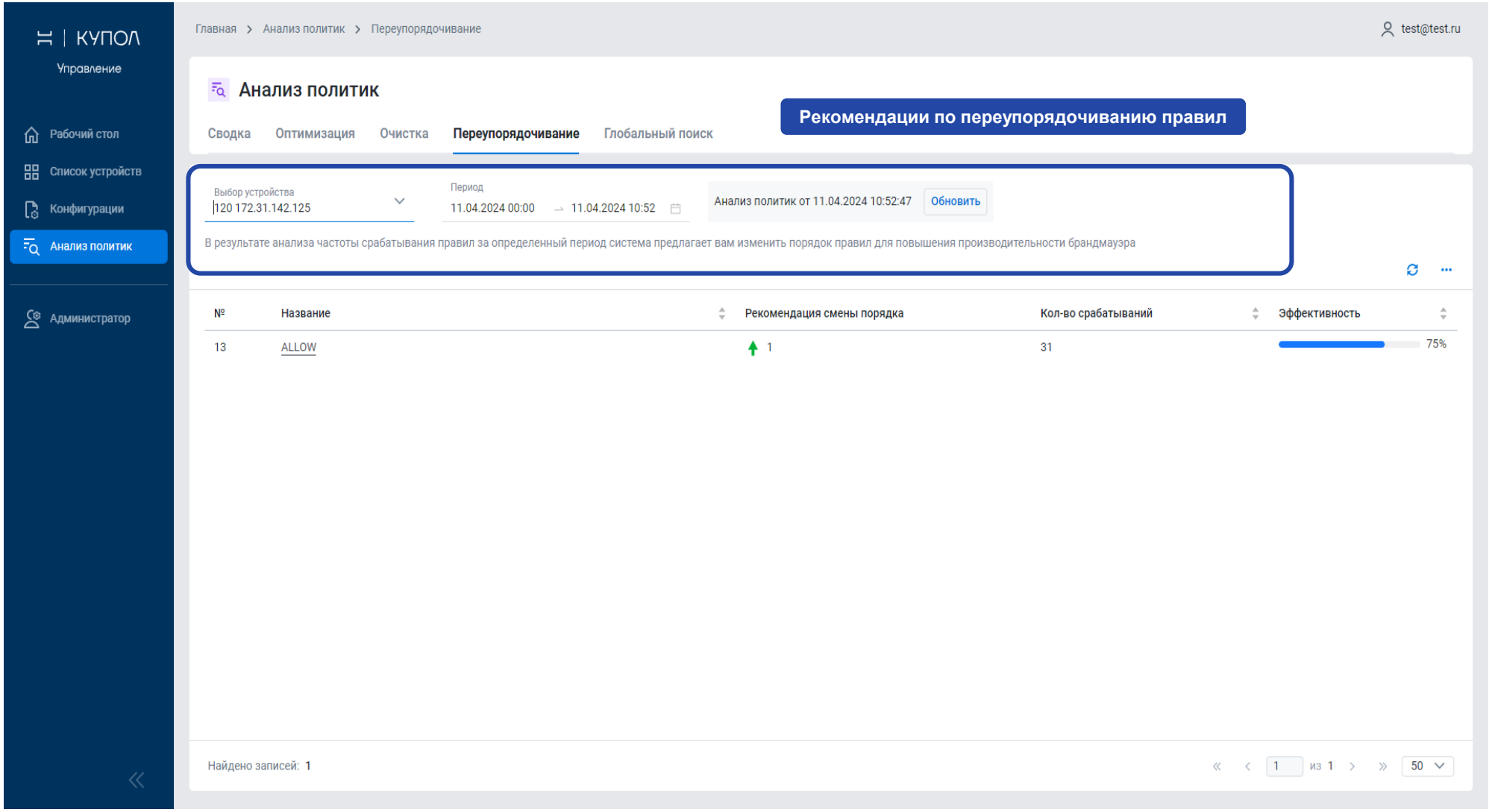


АНАЛИЗ ПОЛИТИК — ПЕРЕУПОРЯДОЧИВАНИЕ



АНАЛИЗ ПОЛИТИК БЕЗОПАСНОСТИ

НСТС | КУПОЛ

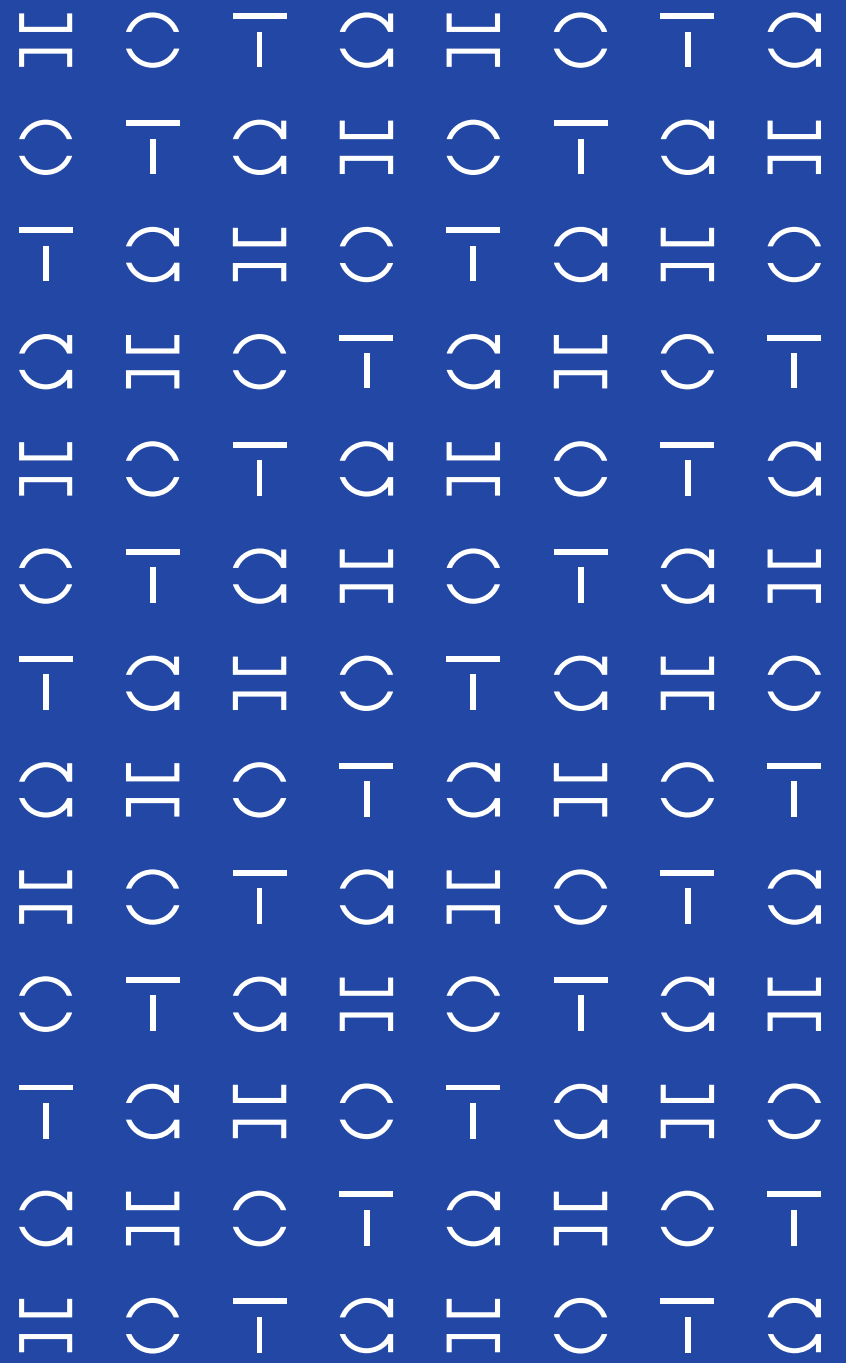


ГЛОБАЛЬНЫЙ ПОИСК

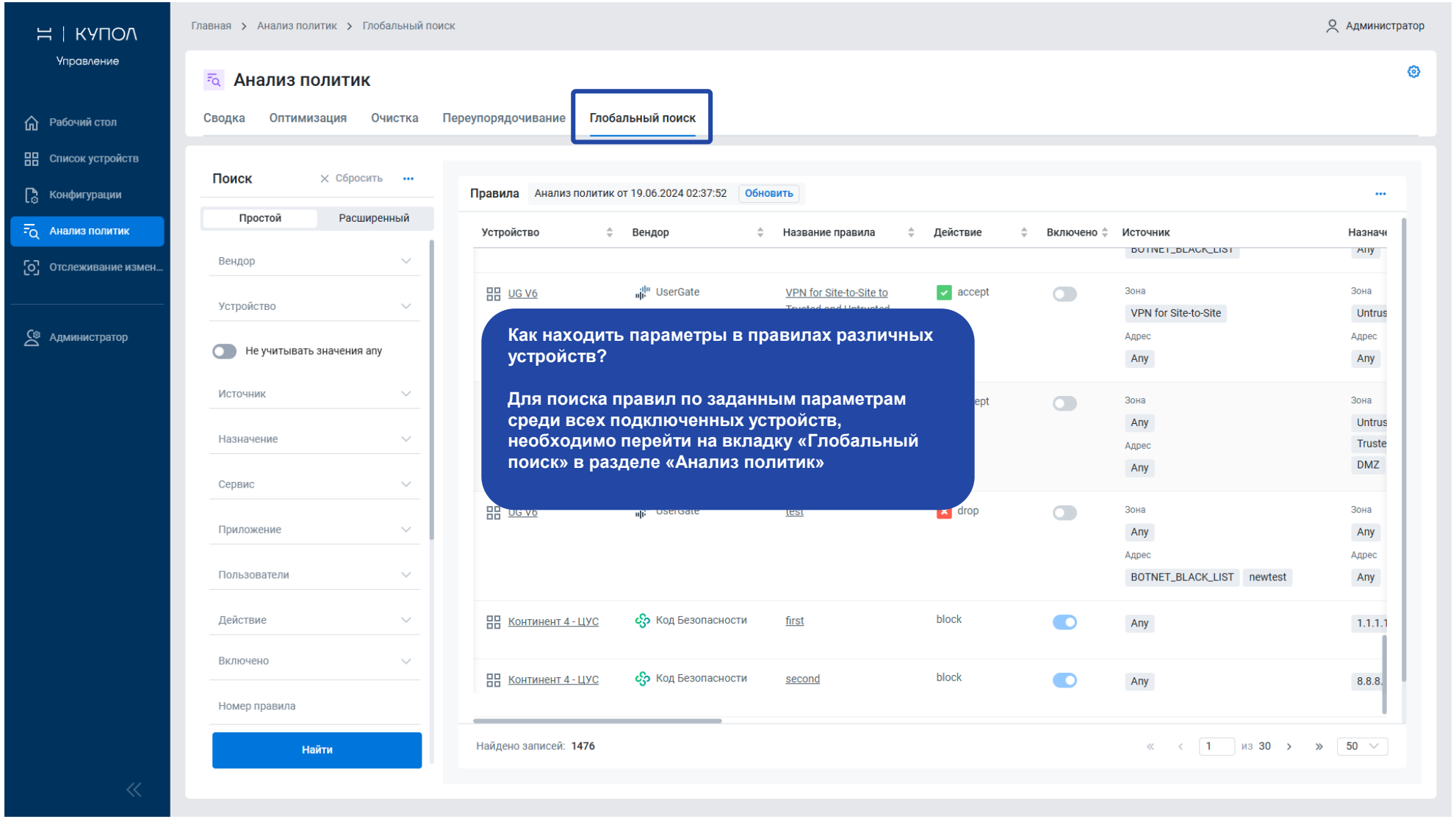
Задача: быстрый поиск всех правил на всех устройствах по нашим критериям запроса.

***Кейс*:** быстро отозвать доступ у субподрядчика к инфраструктуре, которому он был временно представлен.

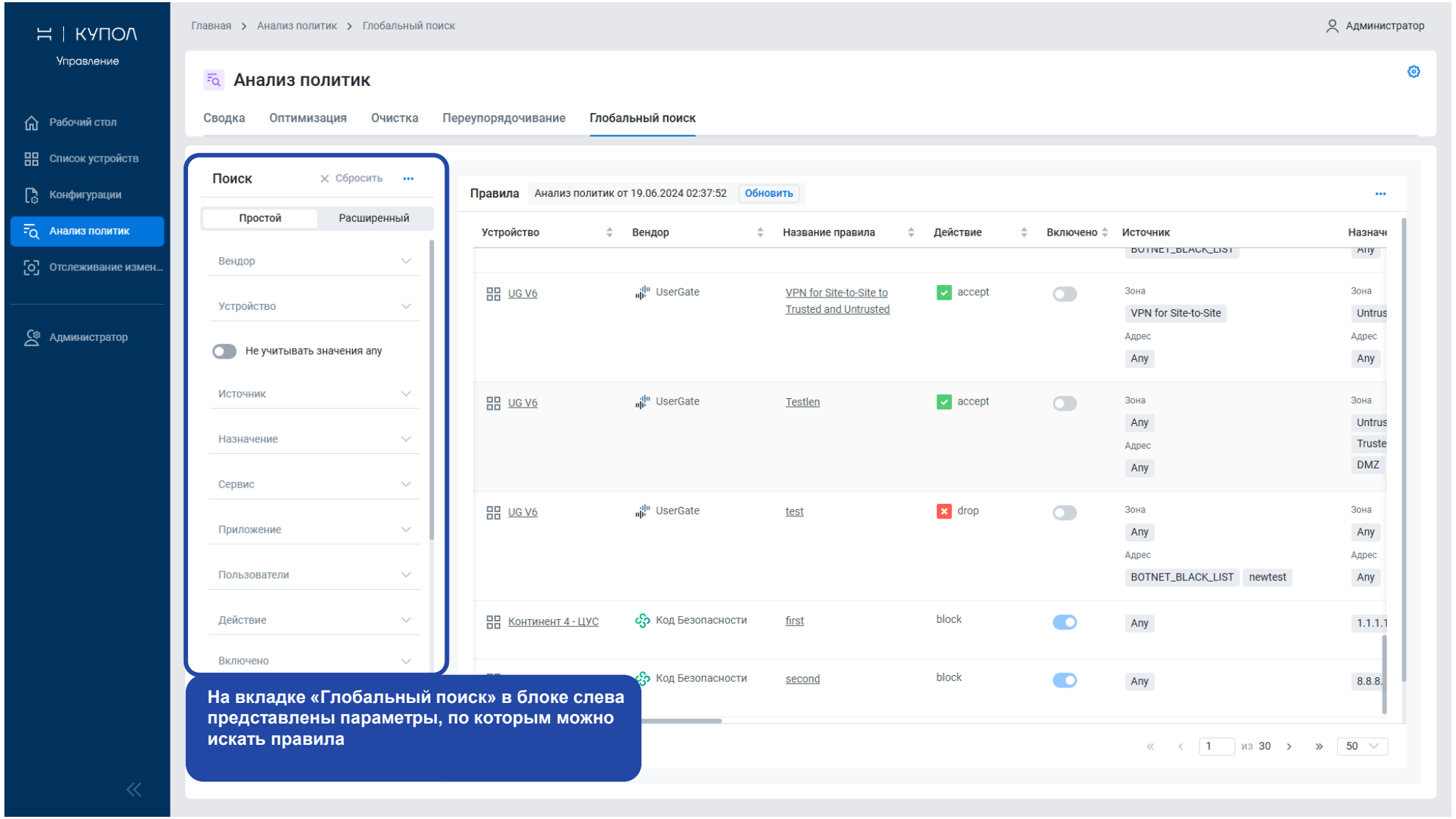
Для этого необходимо найти все правила *на всех устройствах*, по которым был представлен доступ этому субподрядчику.



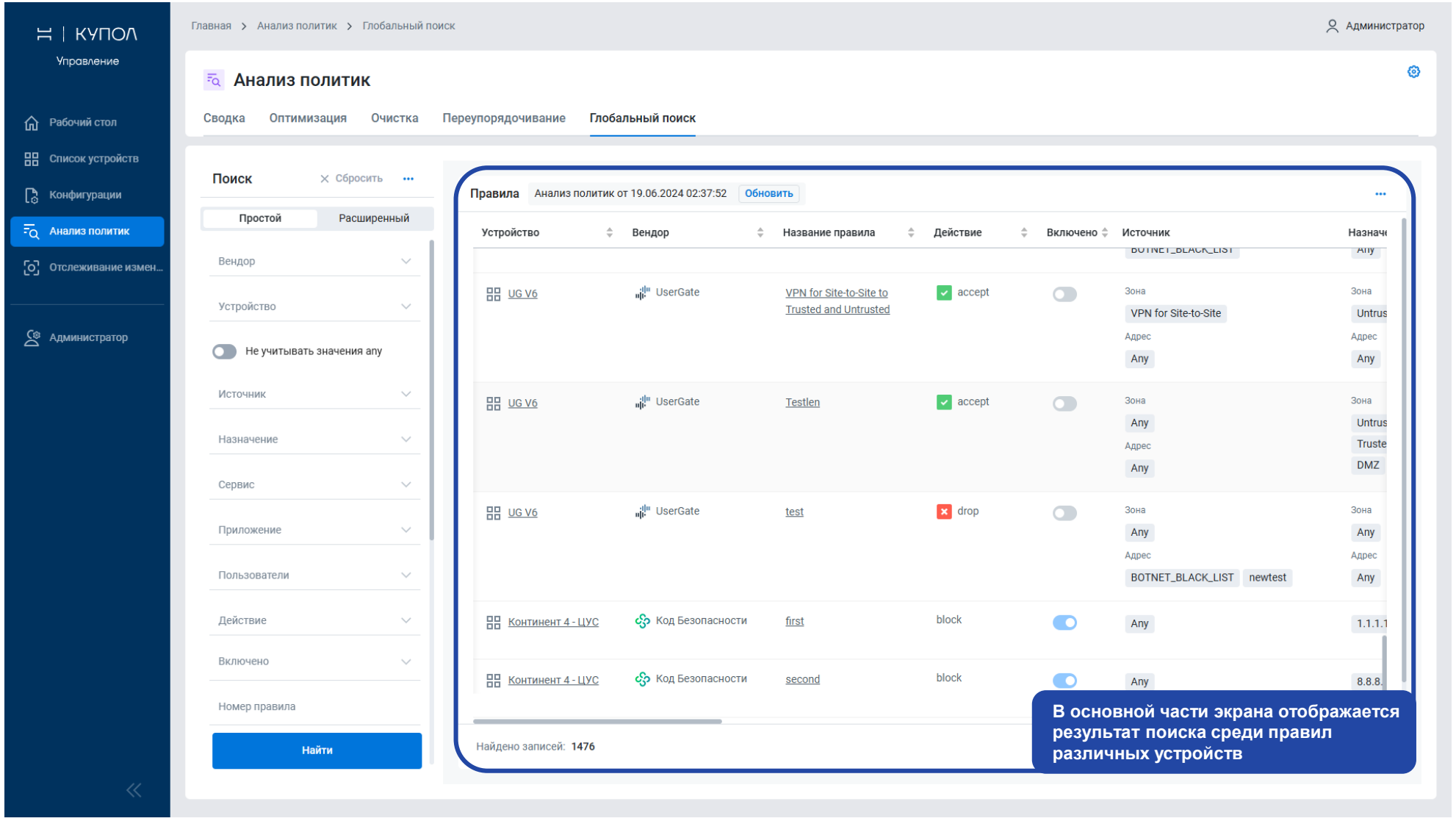
ГЛОБАЛЬНЫЙ ПОИСК



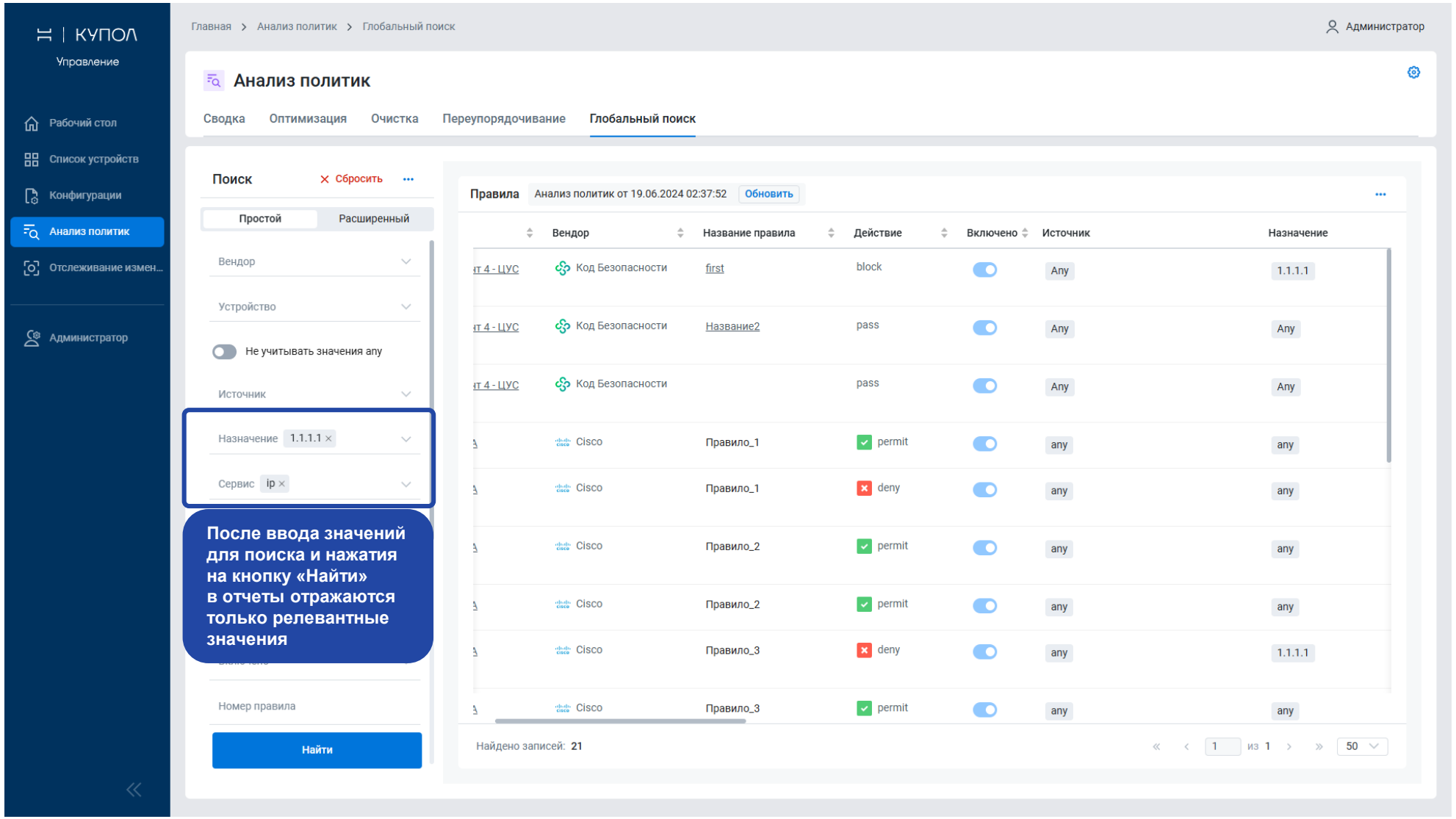
ГЛОБАЛЬНЫЙ ПОИСК



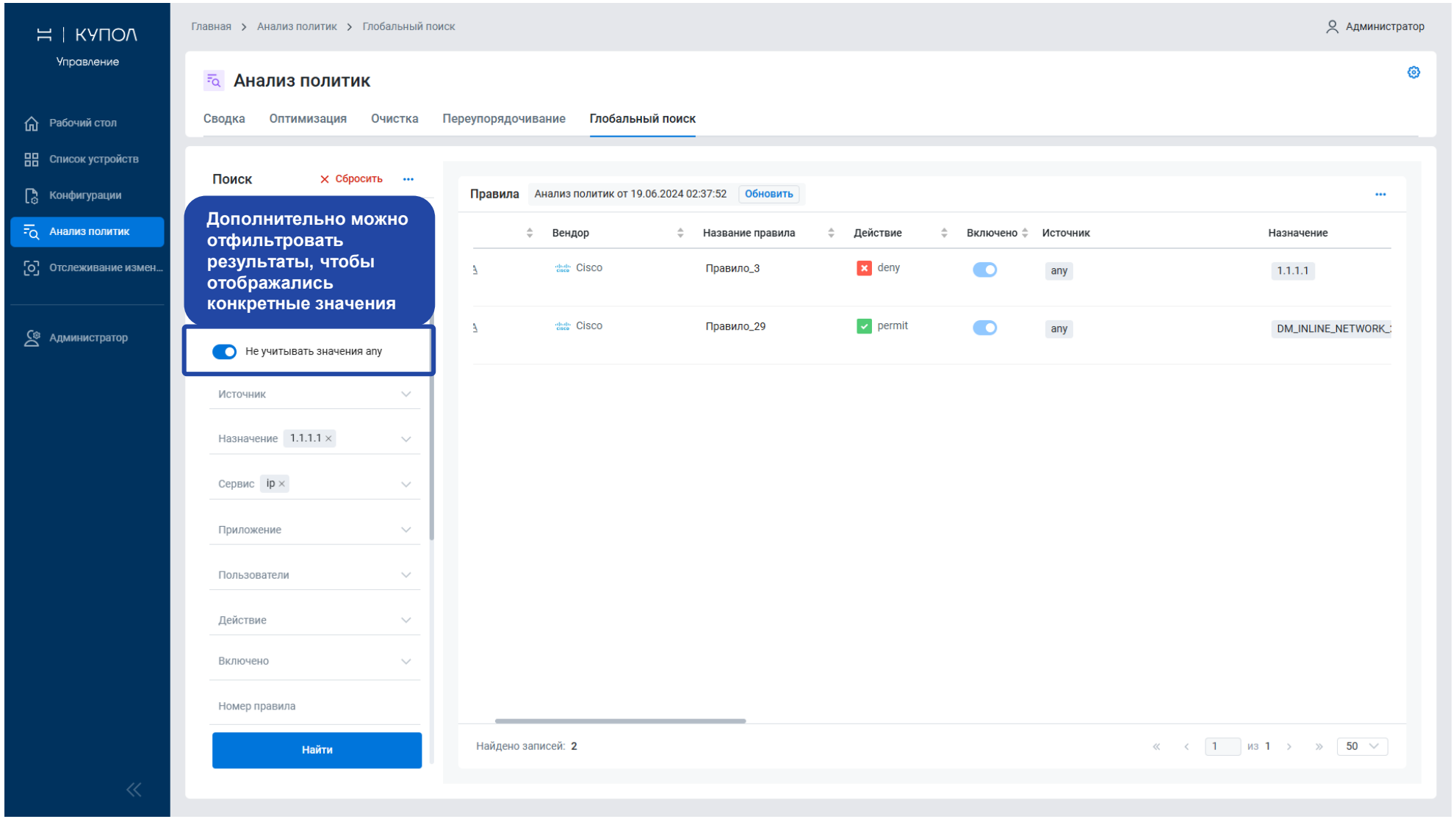
ГЛОБАЛЬНЫЙ ПОИСК



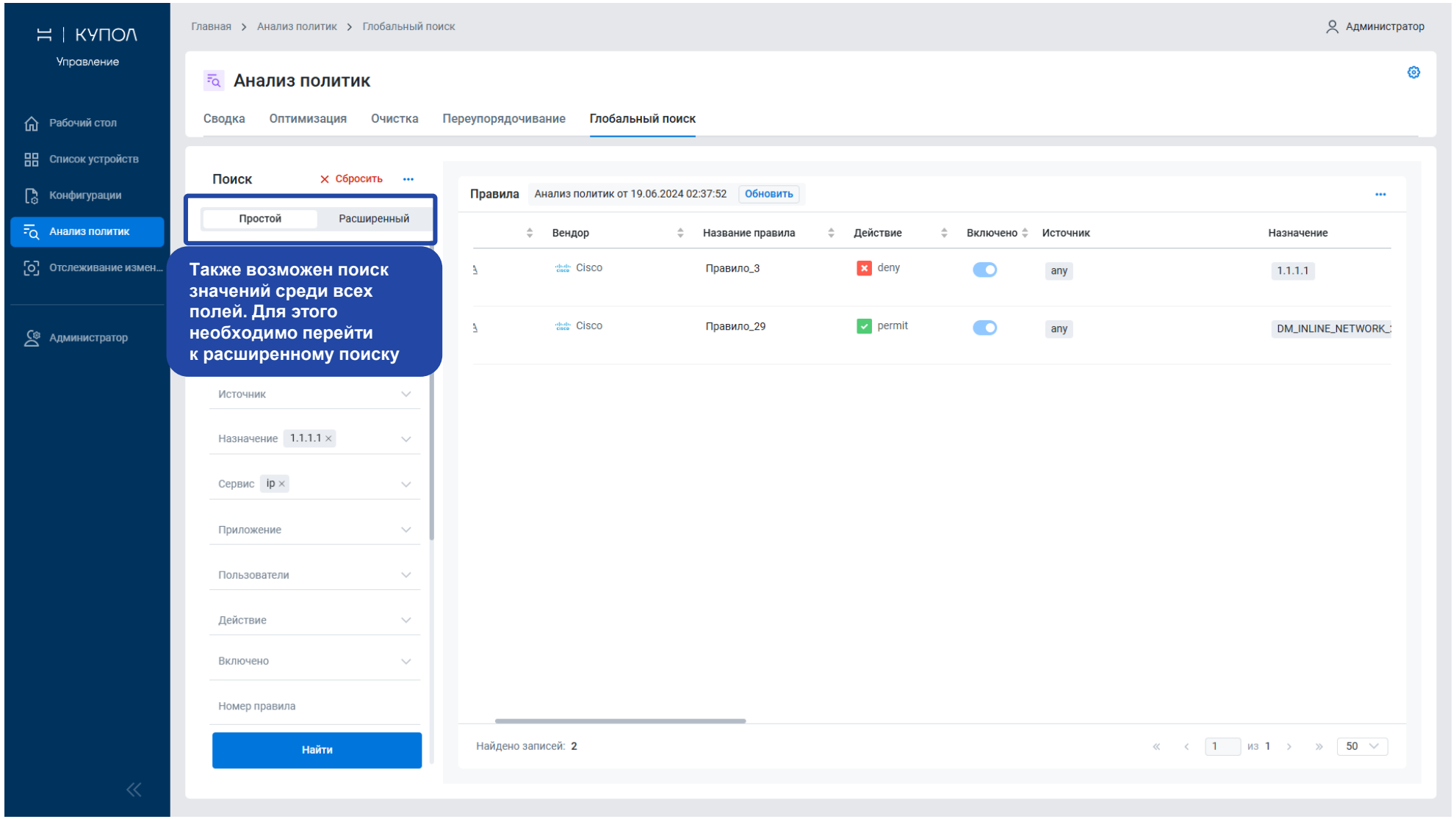
ГЛОБАЛЬНЫЙ ПОИСК



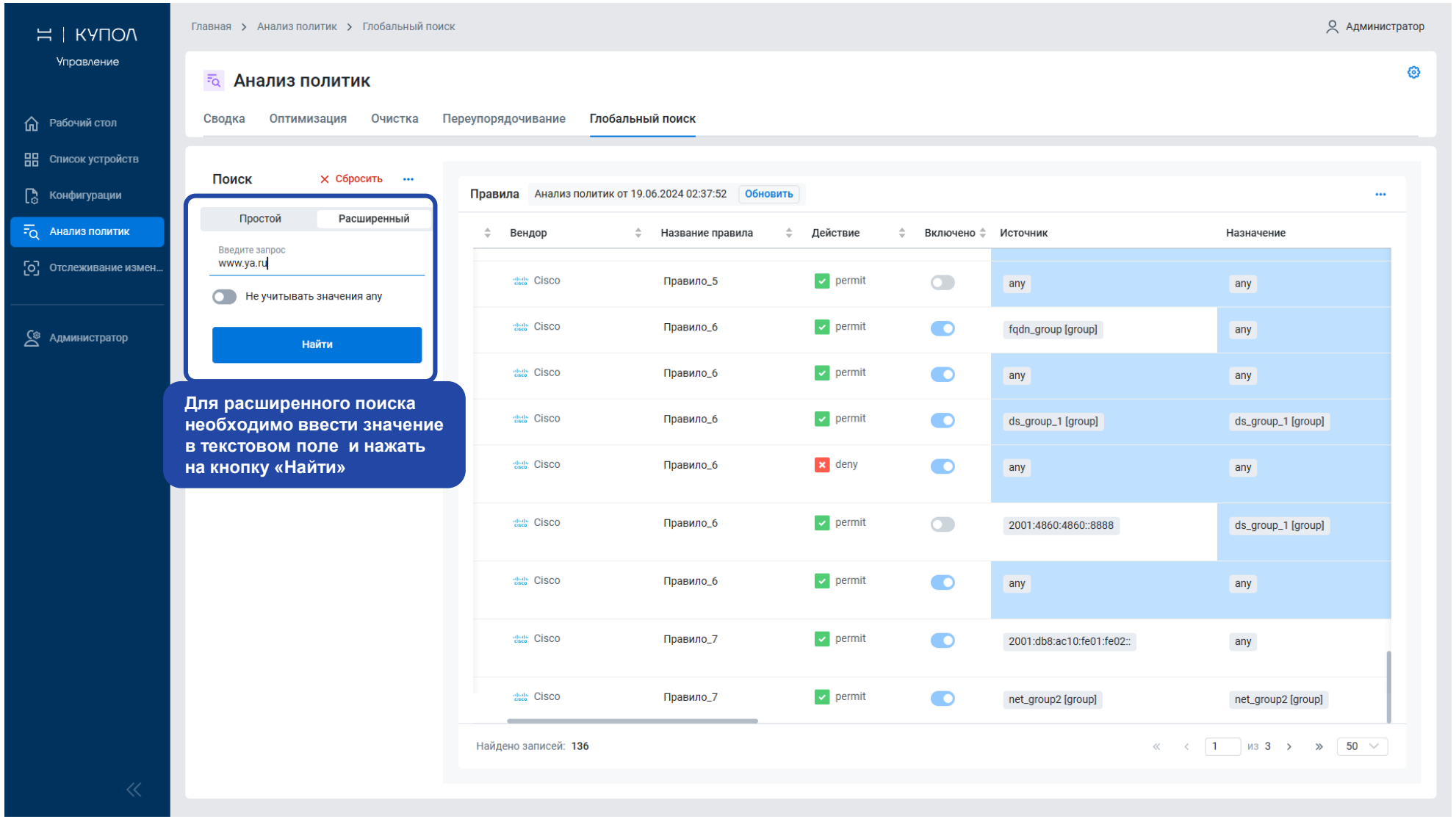
ГЛОБАЛЬНЫЙ ПОИСК



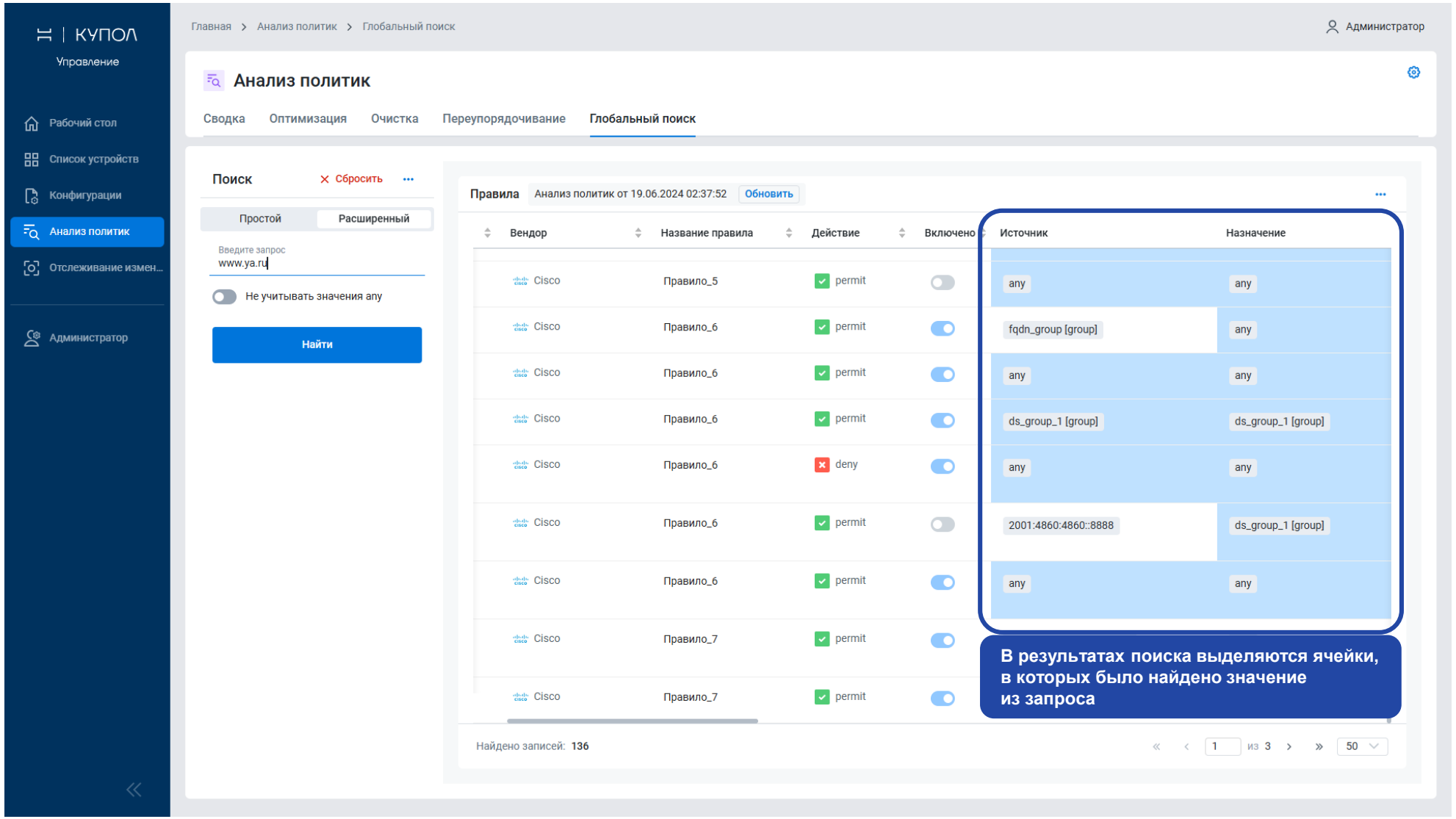
ГЛОБАЛЬНЫЙ ПОИСК



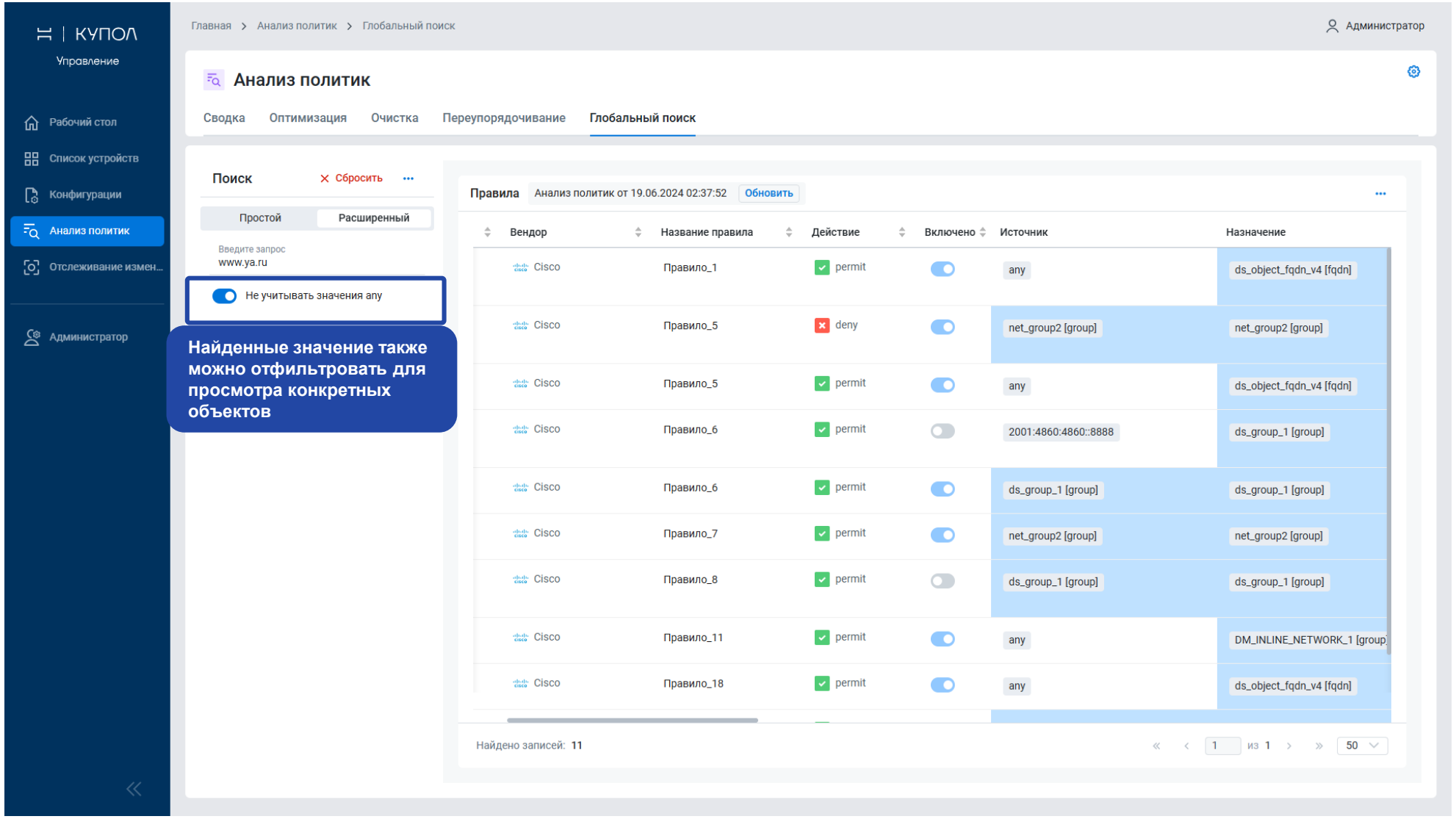
ГЛОБАЛЬНЫЙ ПОИСК



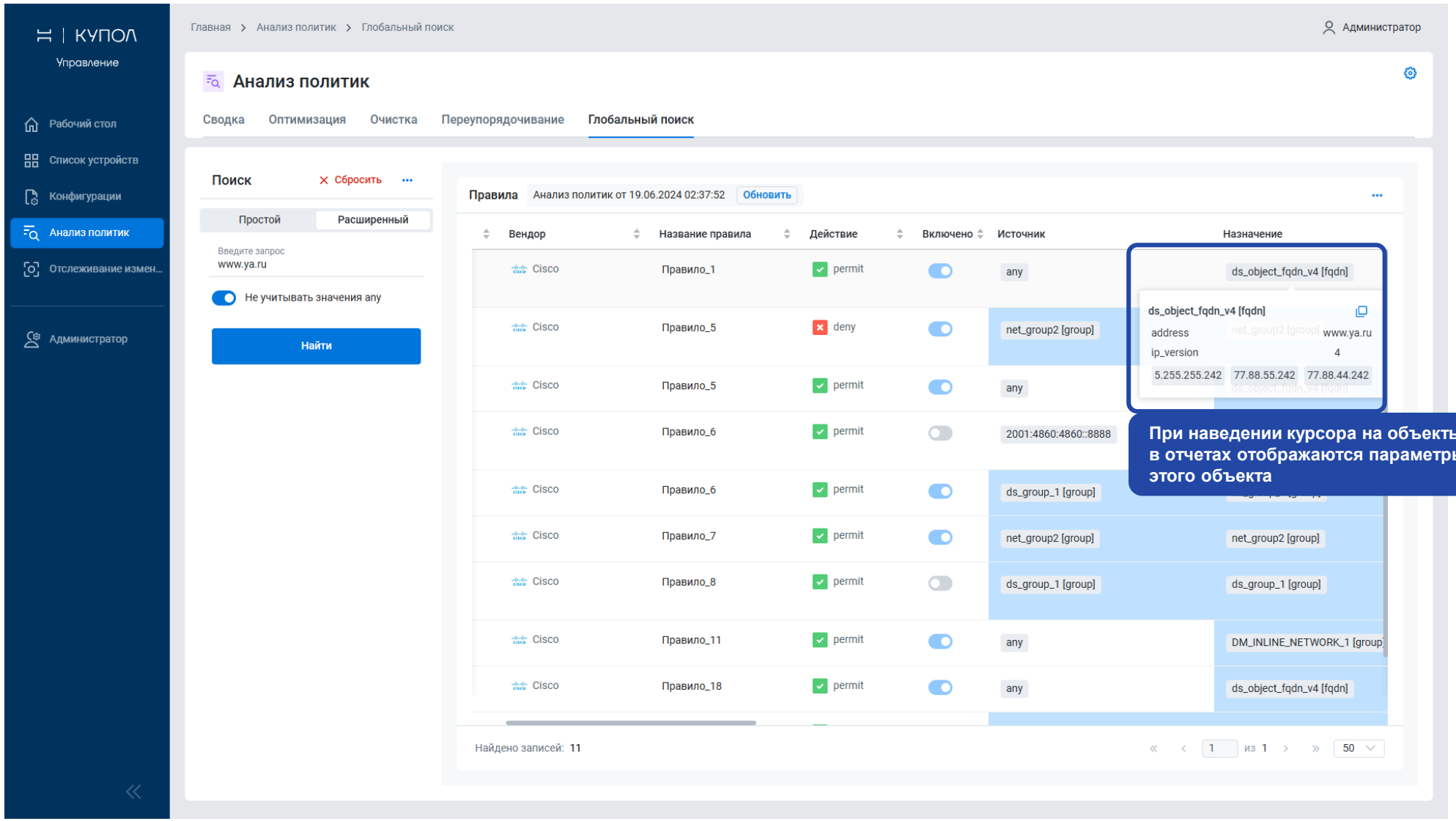
ГЛОБАЛЬНЫЙ ПОИСК



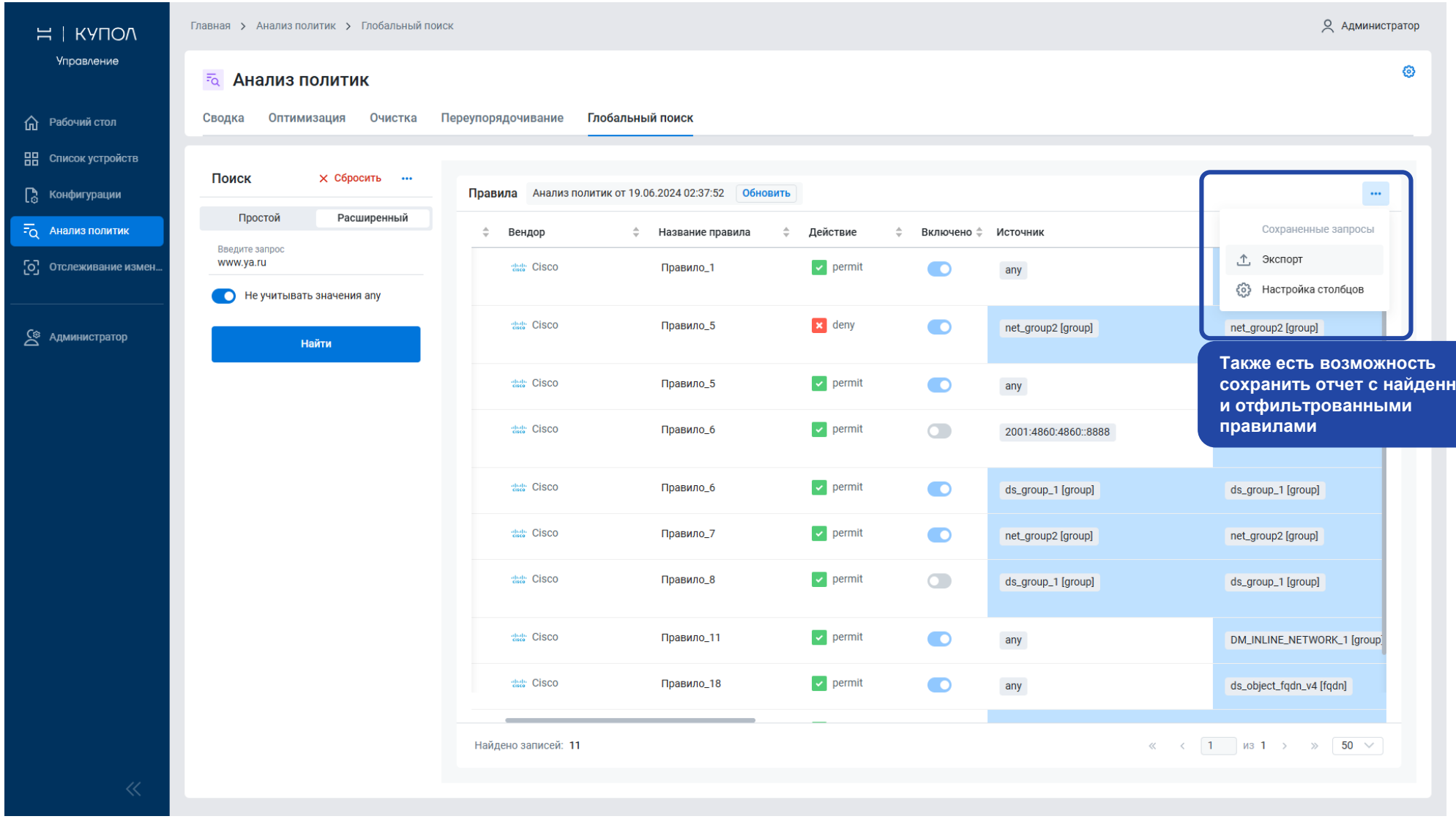
ГЛОБАЛЬНЫЙ ПОИСК



ГЛОБАЛЬНЫЙ ПОИСК

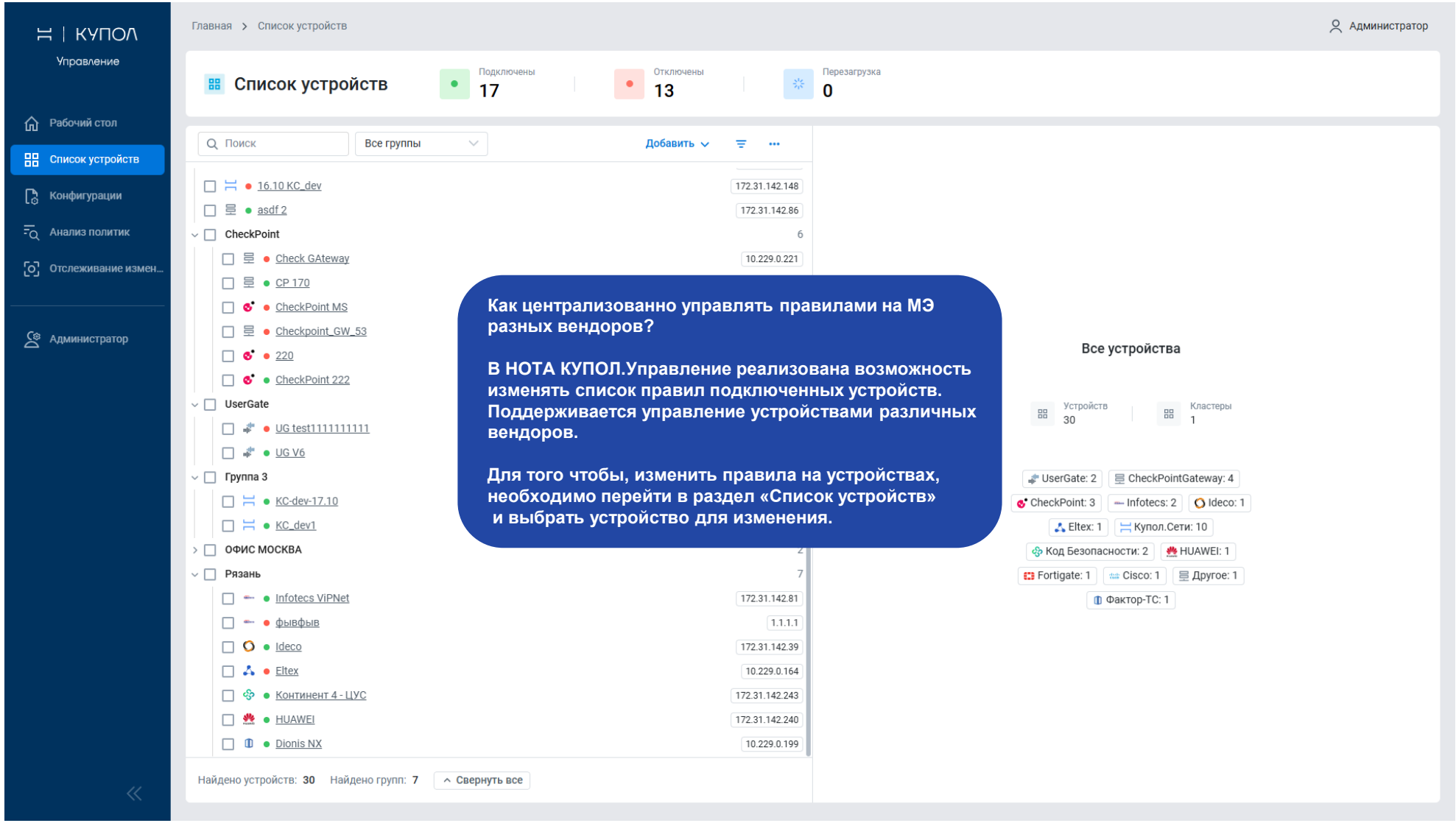


ГЛОБАЛЬНЫЙ ПОИСК

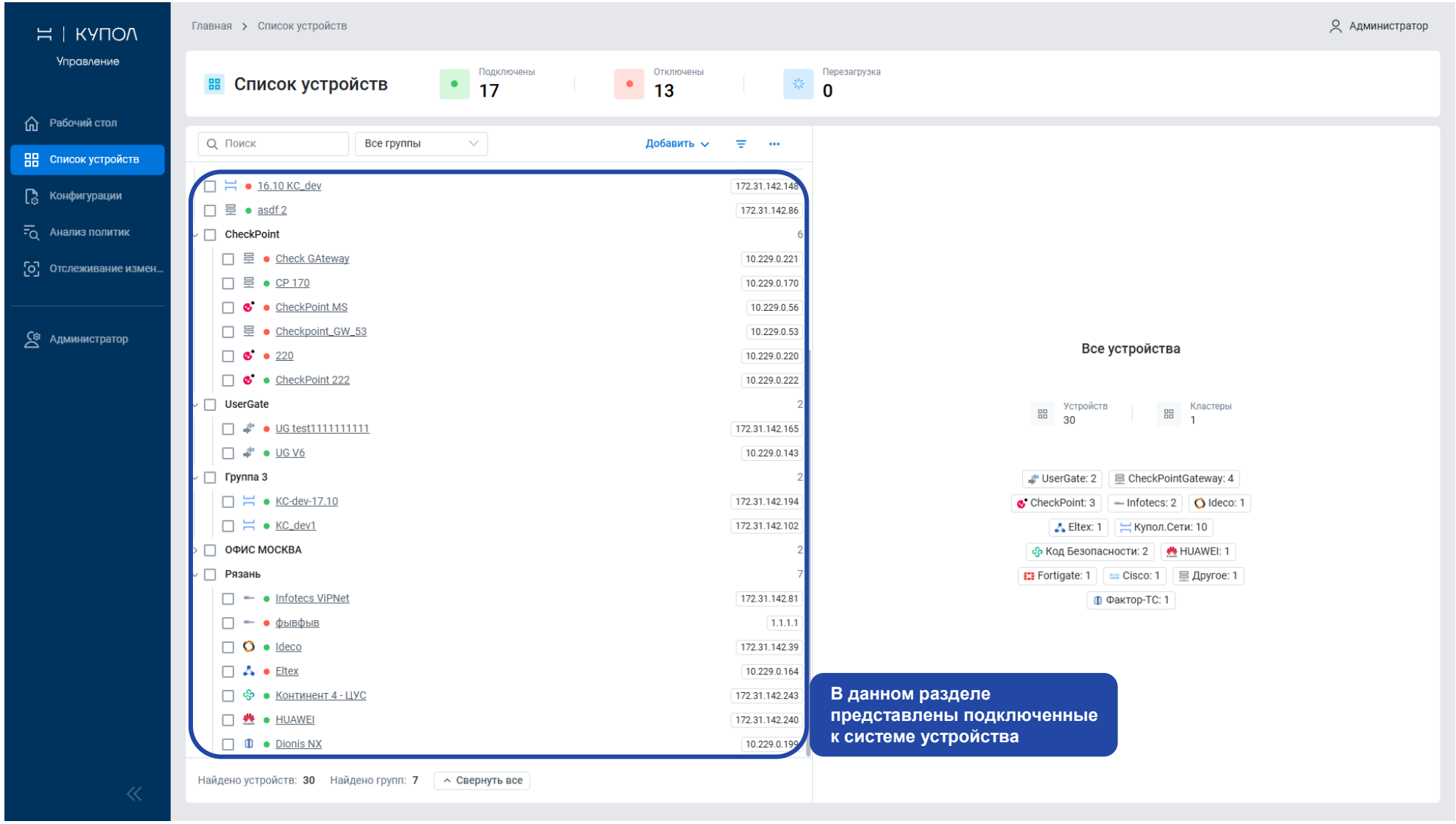


УПРАВЛЕНИЕ ПРАВИЛАМИ

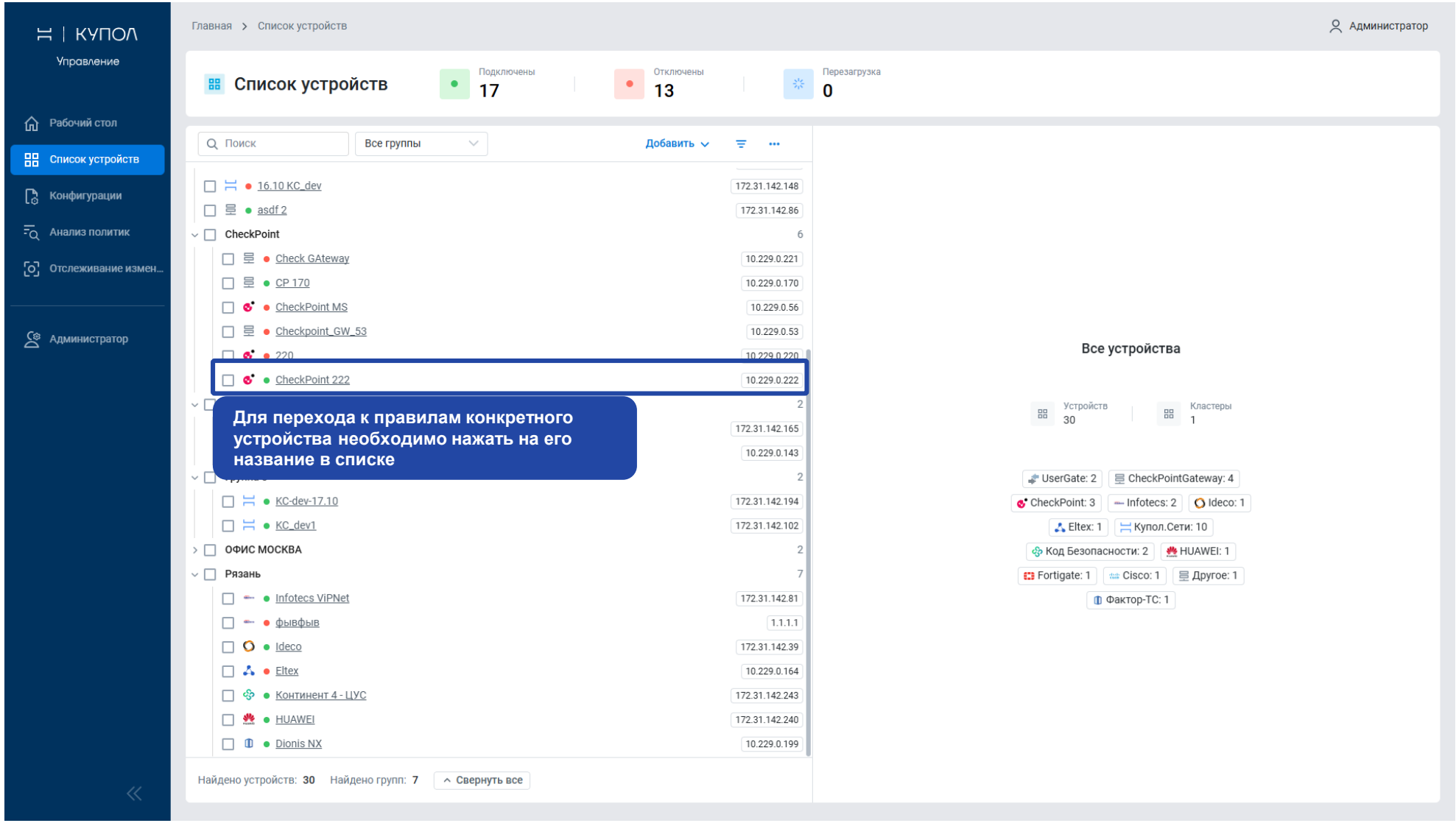
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



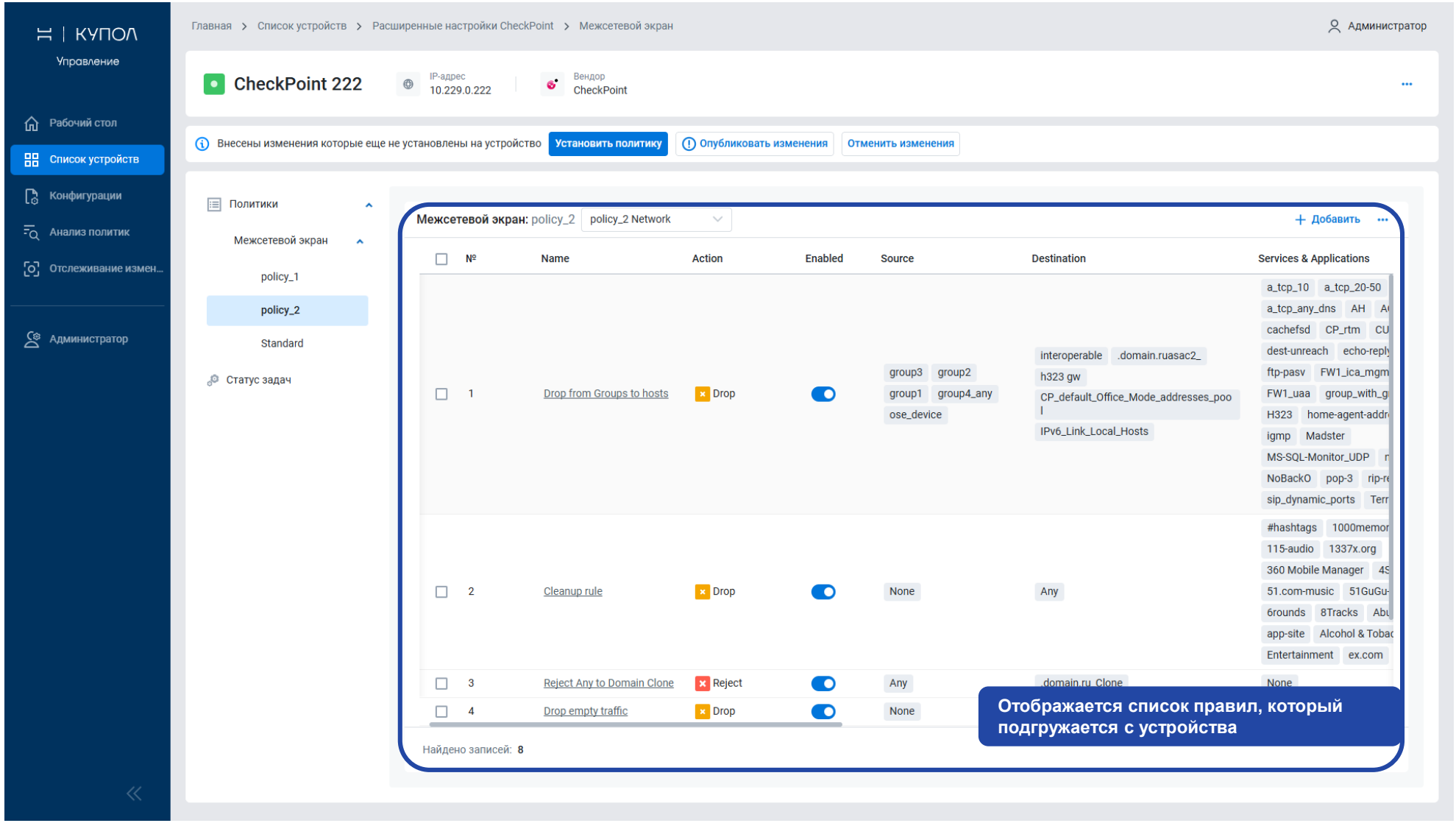
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



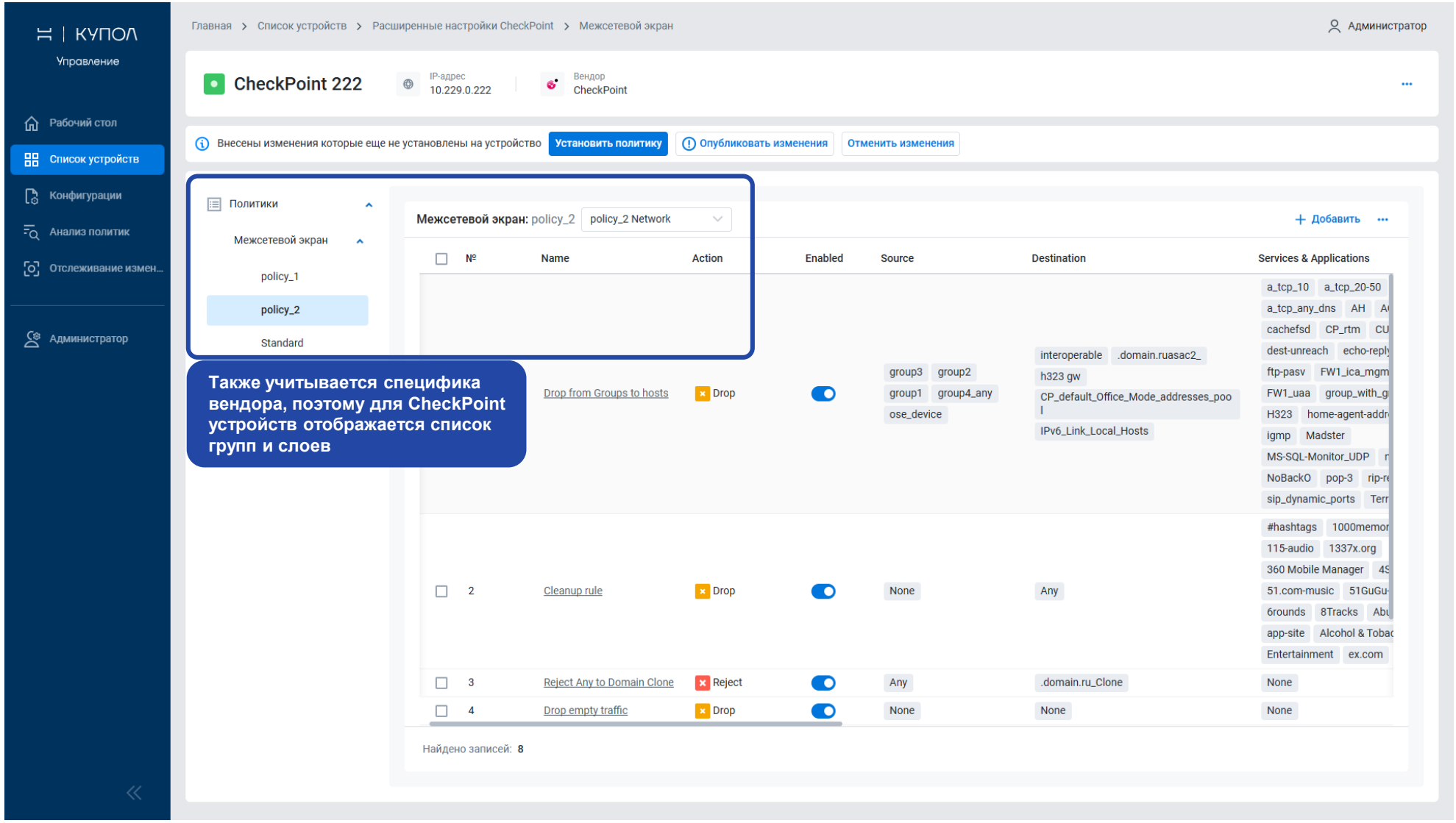
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



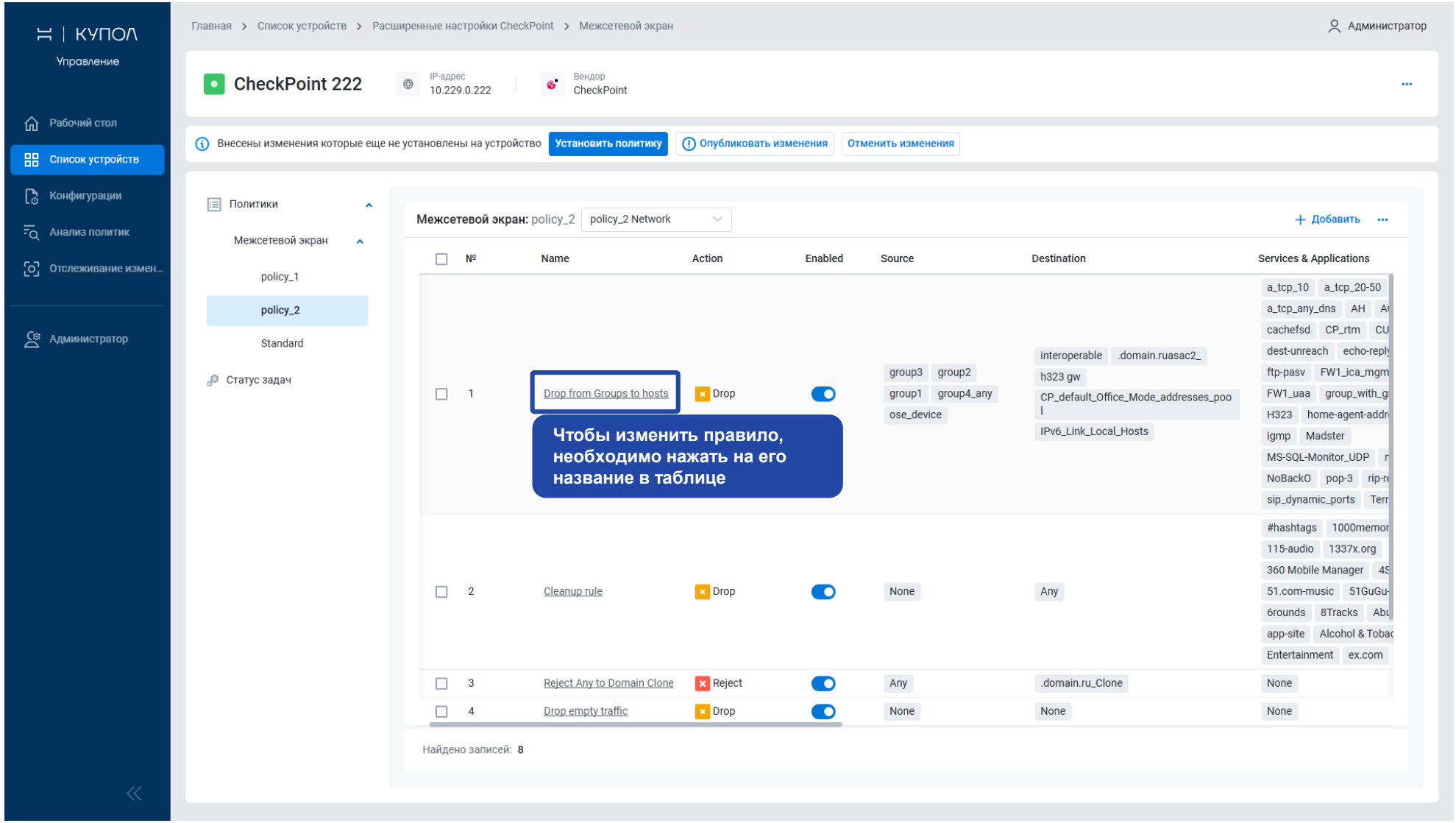
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



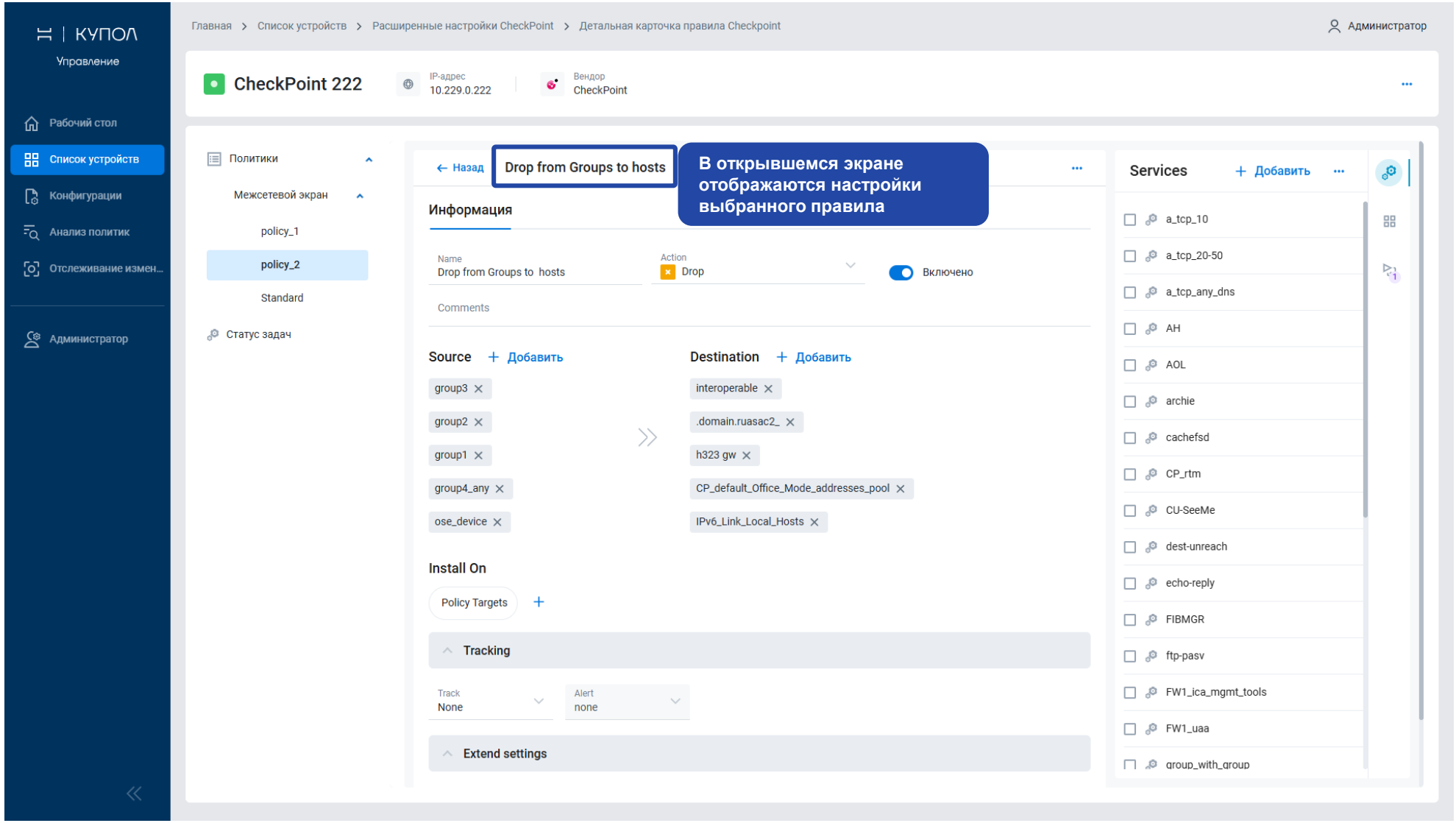
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



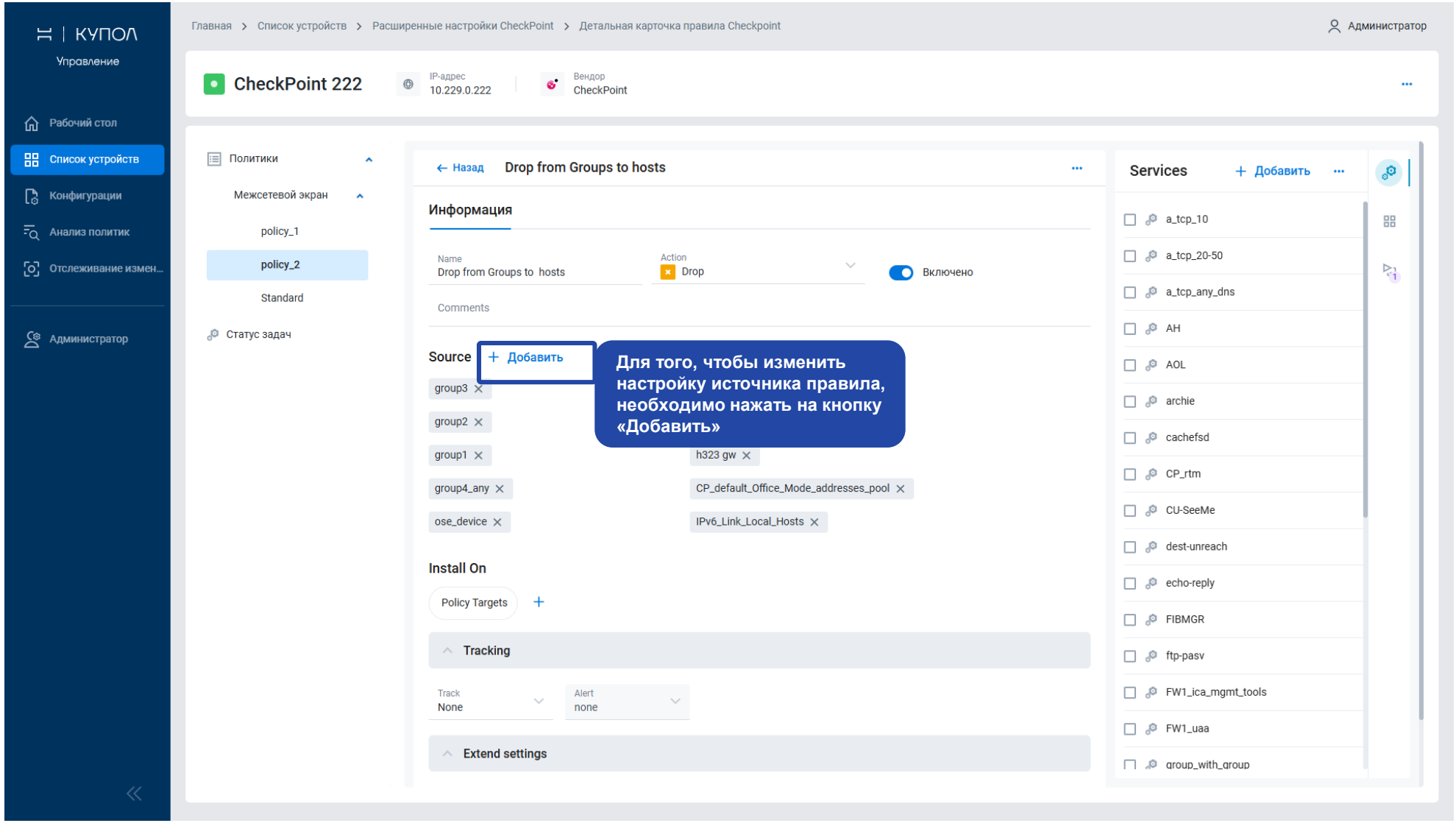
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



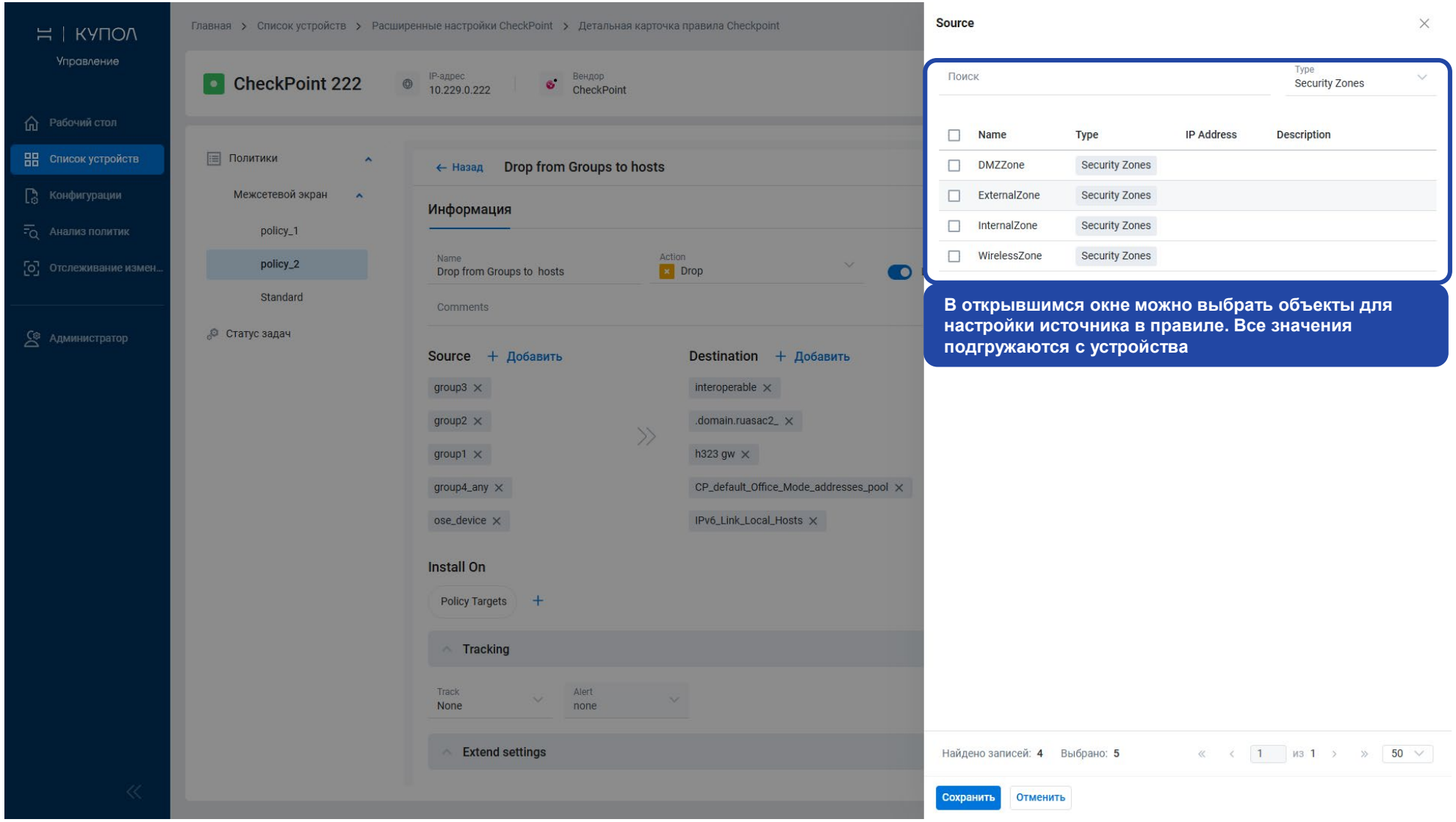
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



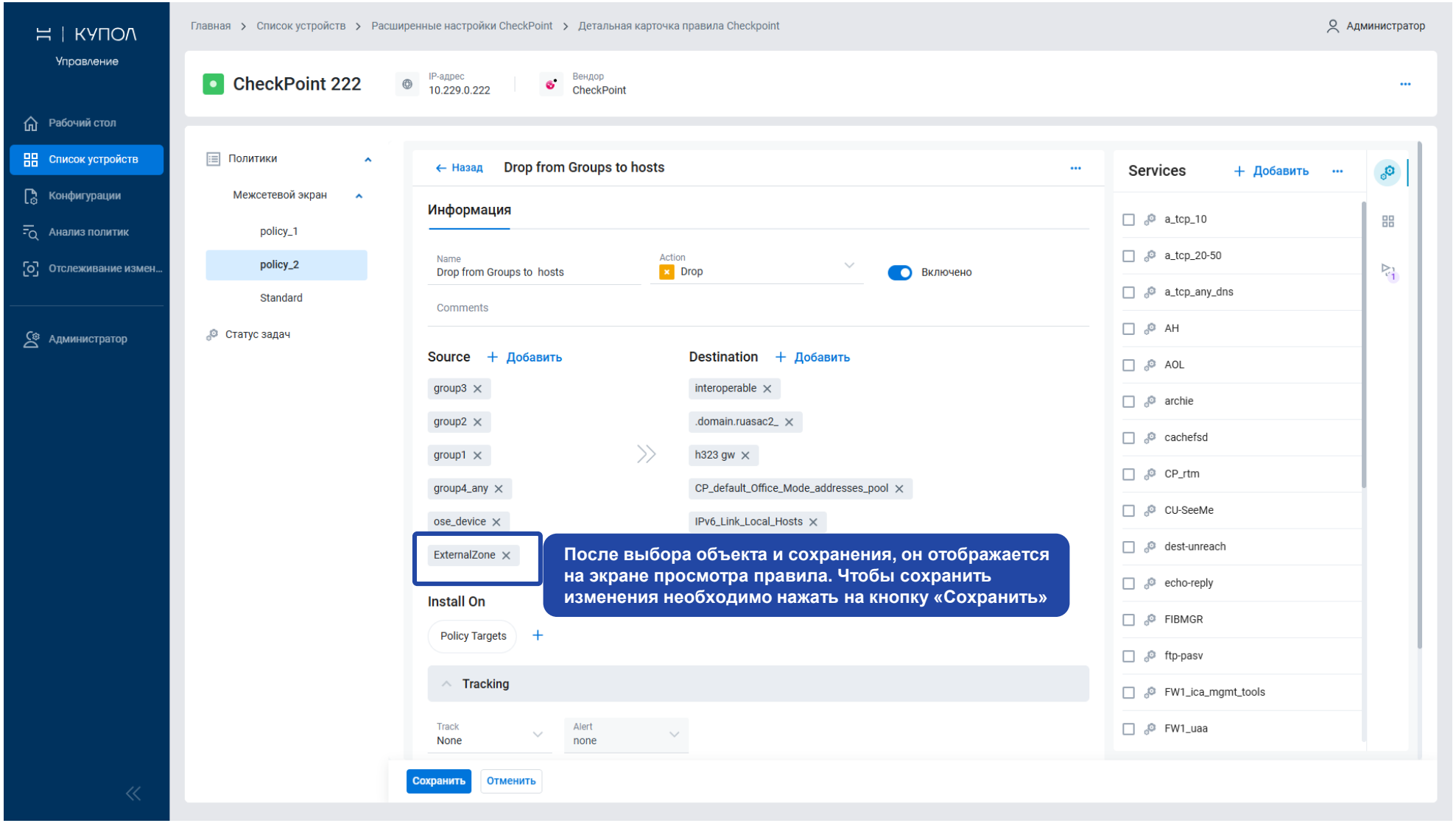
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



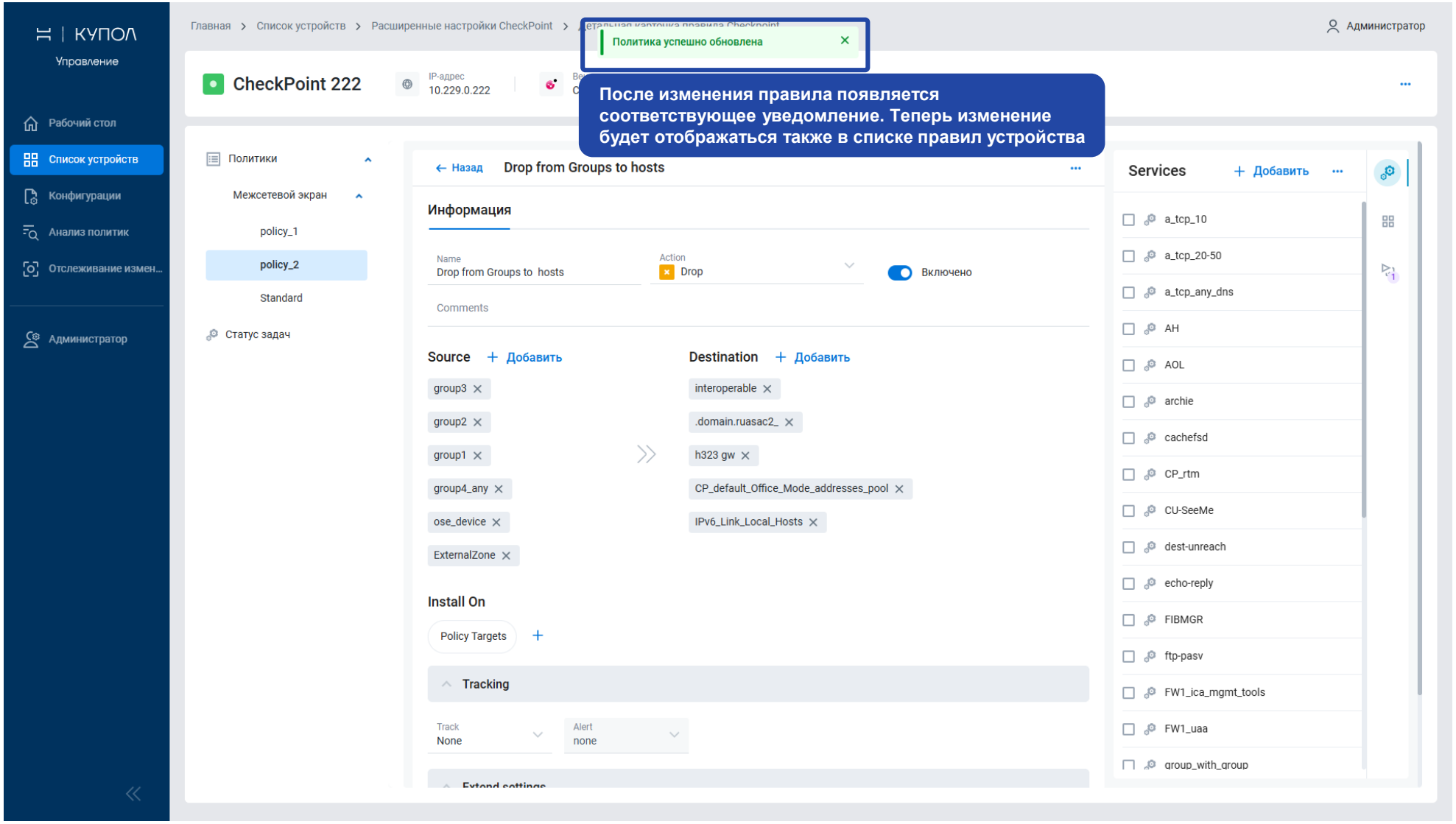
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



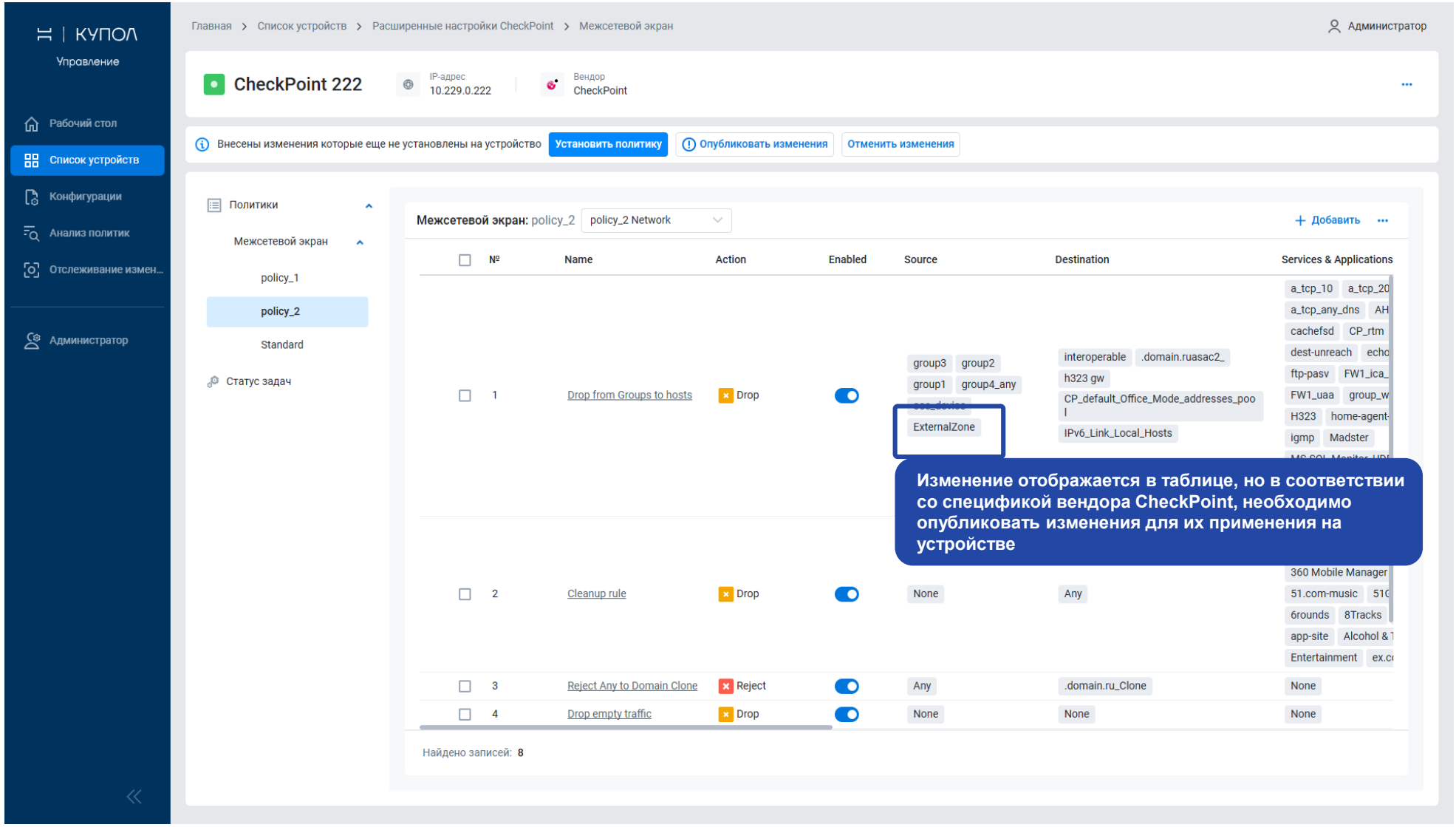
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



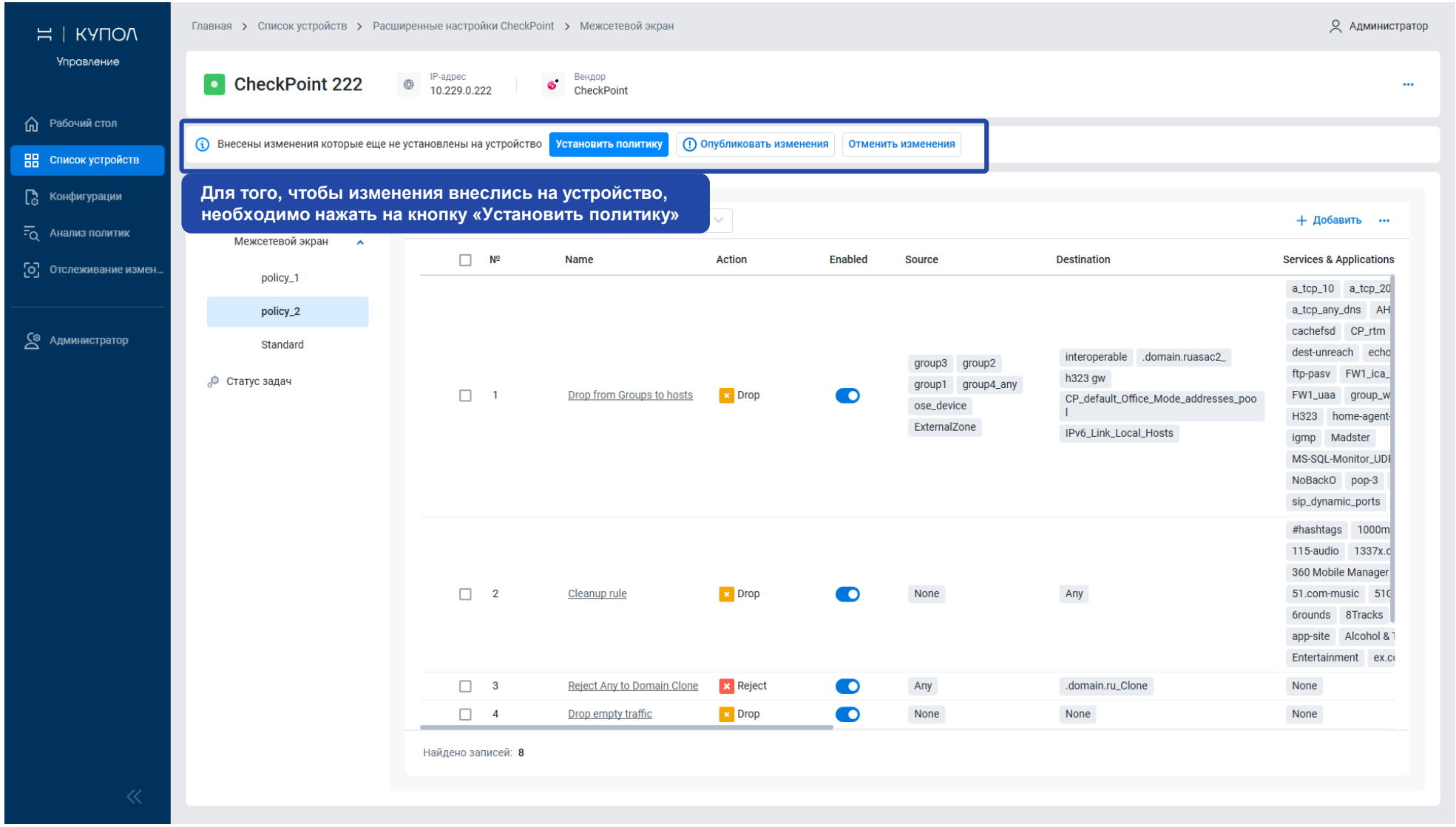
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



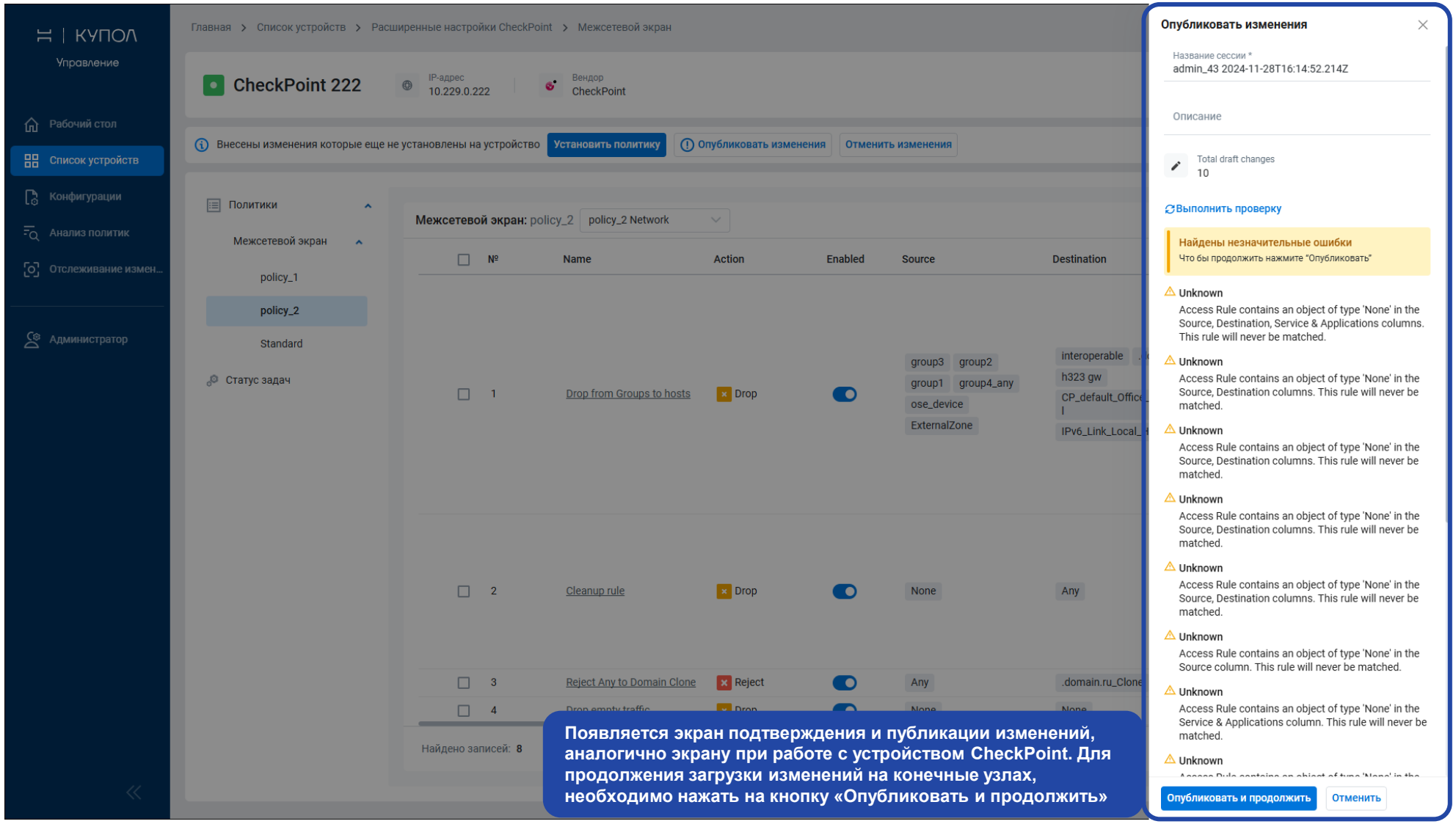
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



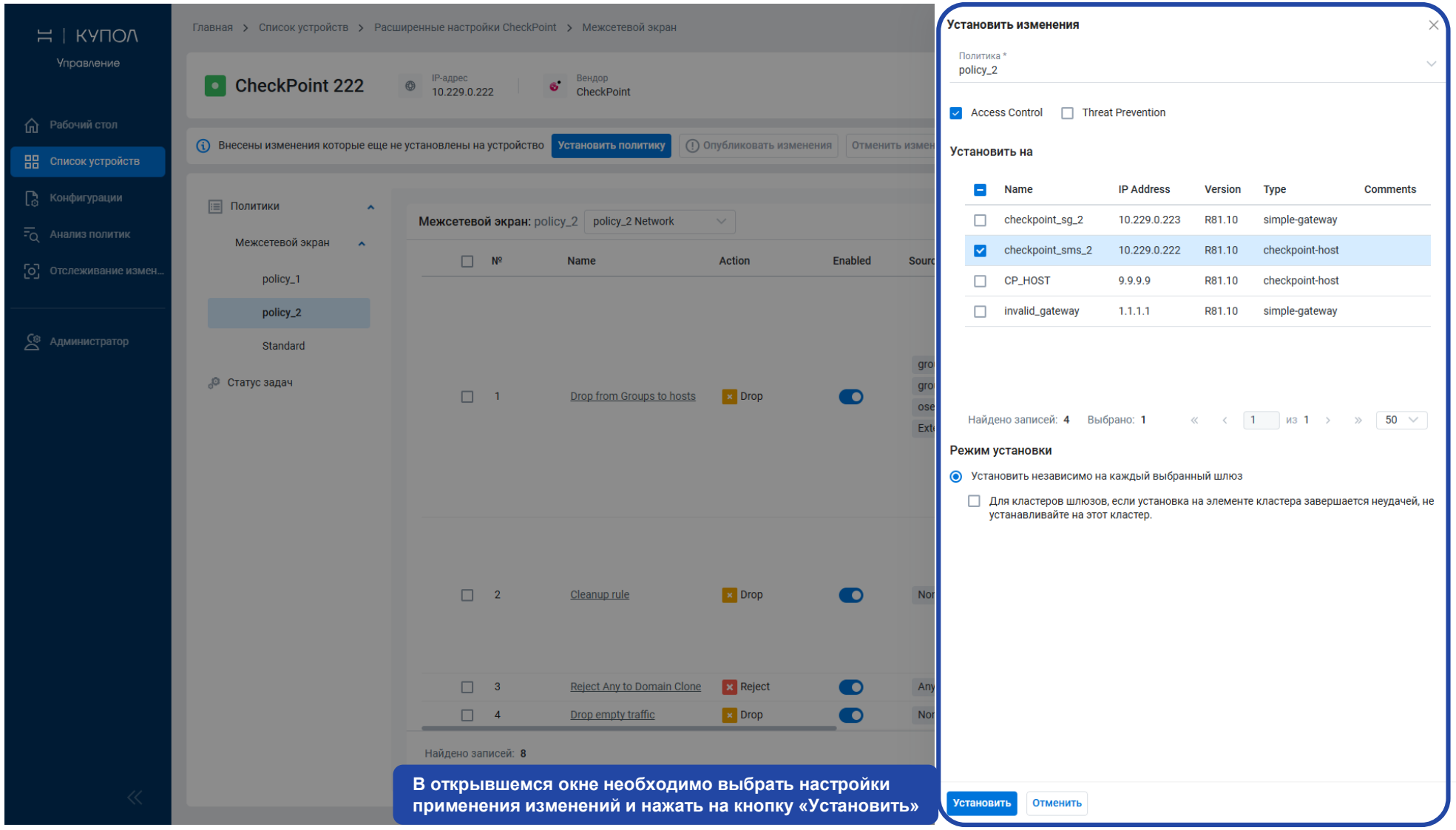
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ

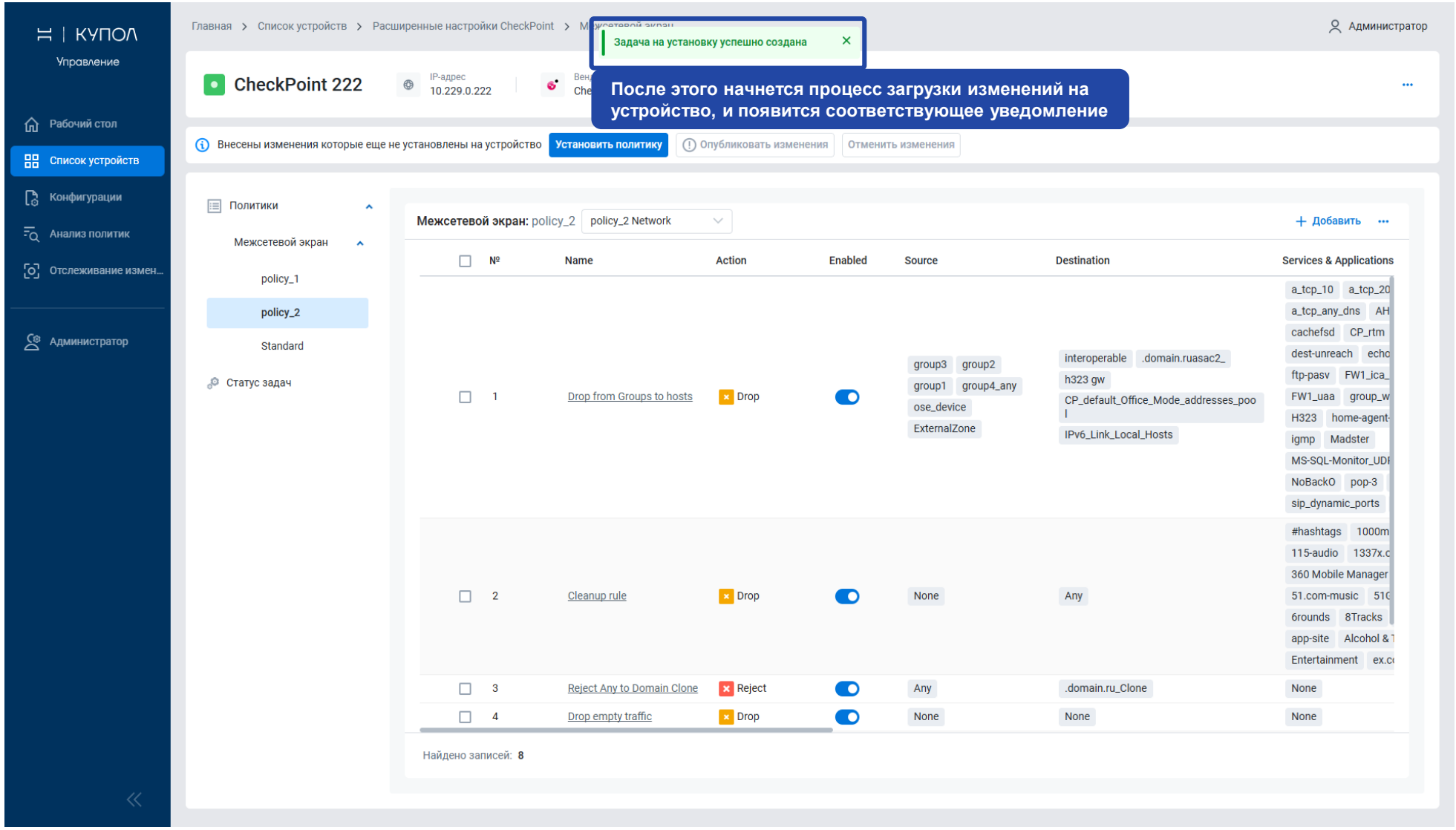


УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ

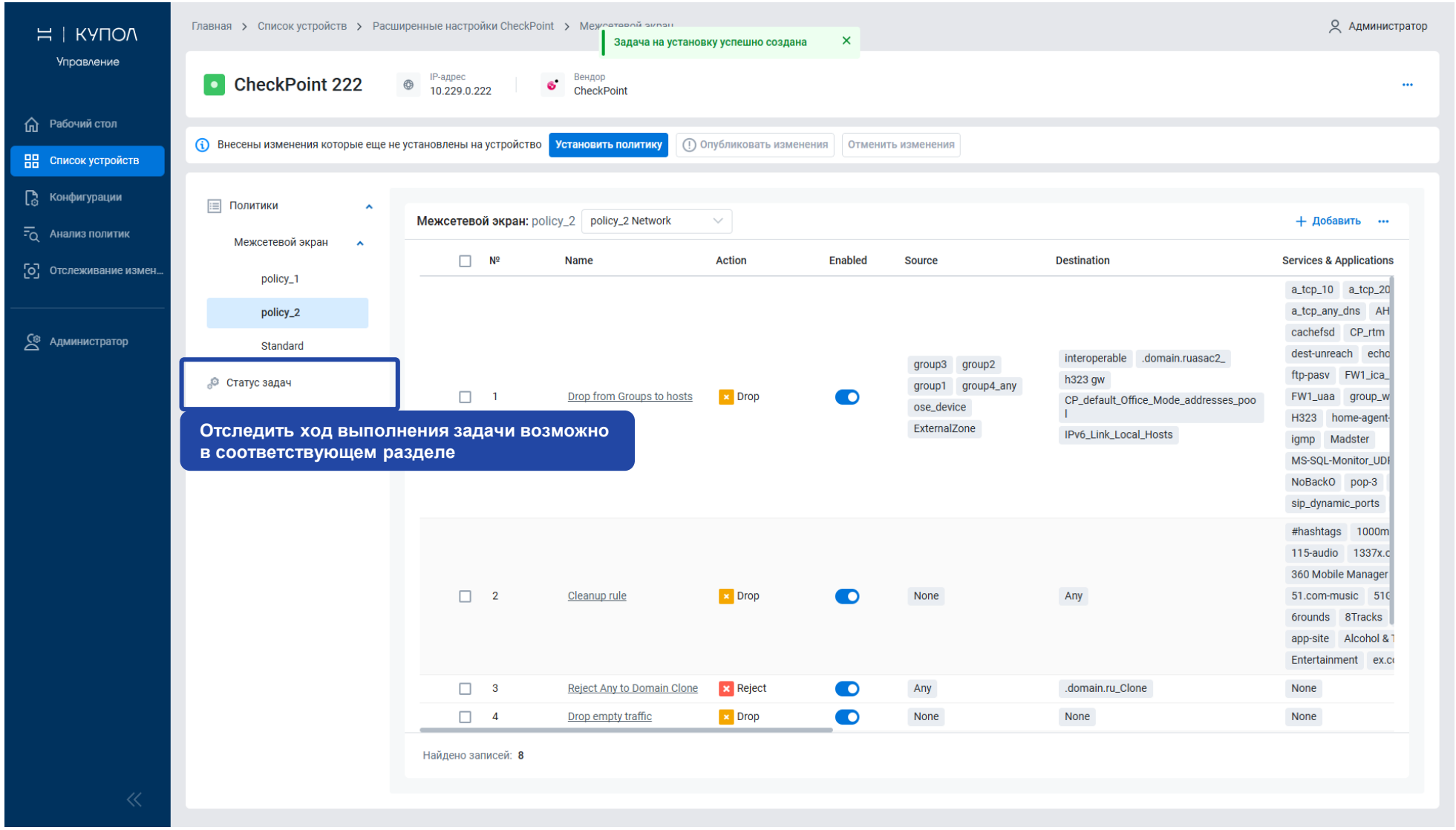


В открывшемся окне необходимо выбрать настройки применения изменений и нажать на кнопку «Установить»

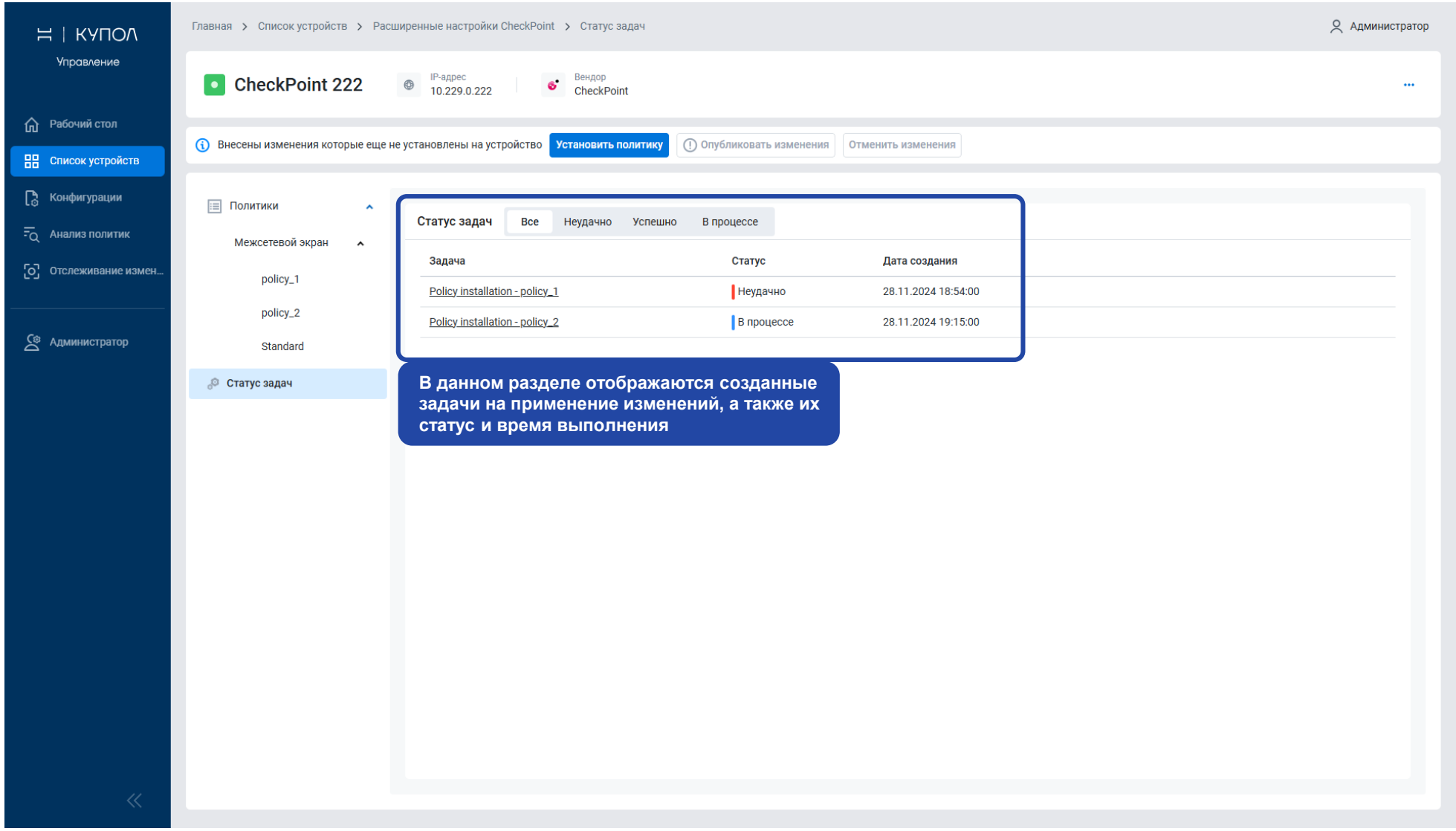
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



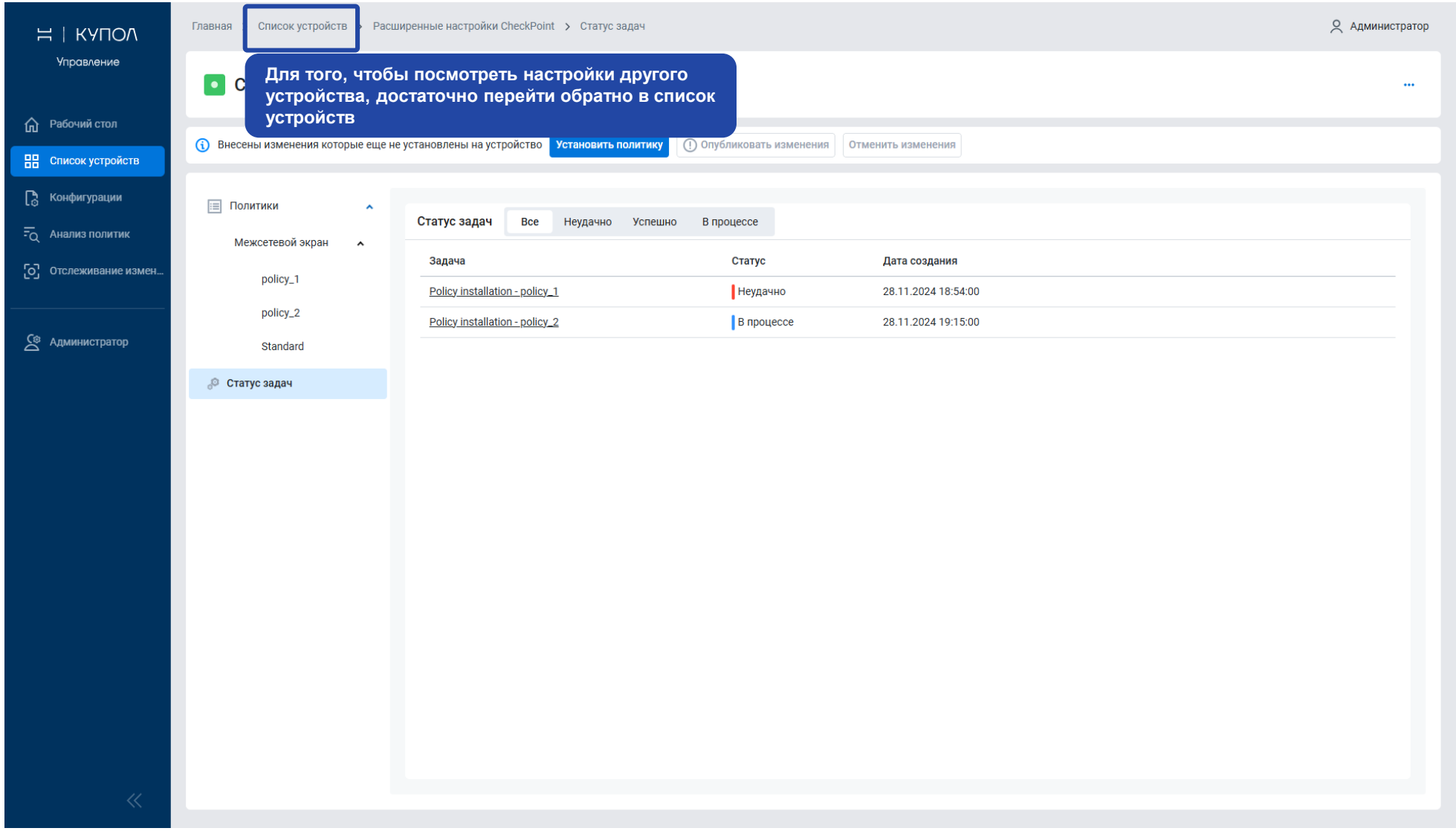
УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ



УПРАВЛЕНИЕ ПРАВИЛАМИ МЭ

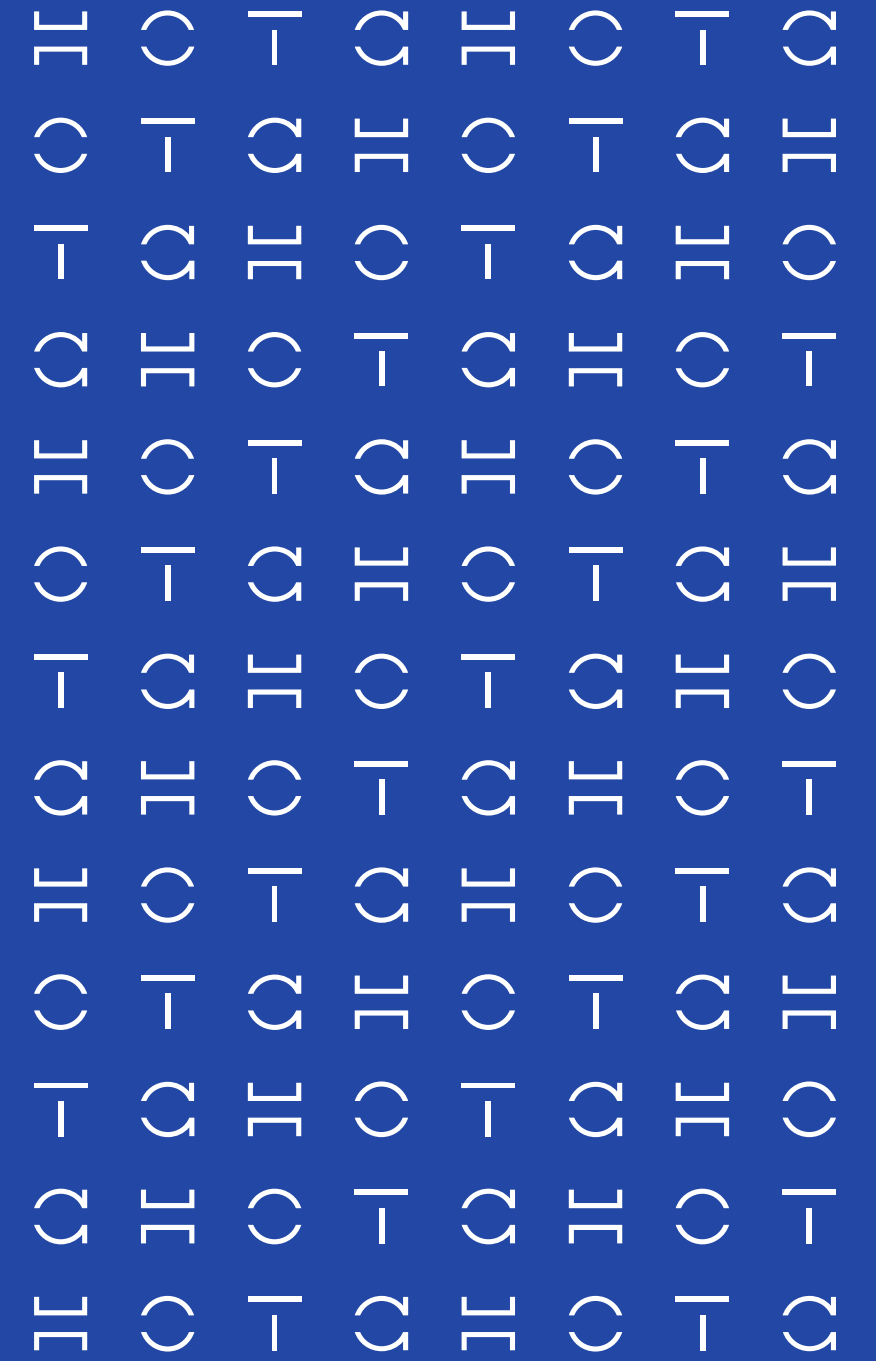


ЗОНАЛЬНЫЙ АНАЛИЗ

Установка глобальной политики межсетевого взаимодействия.

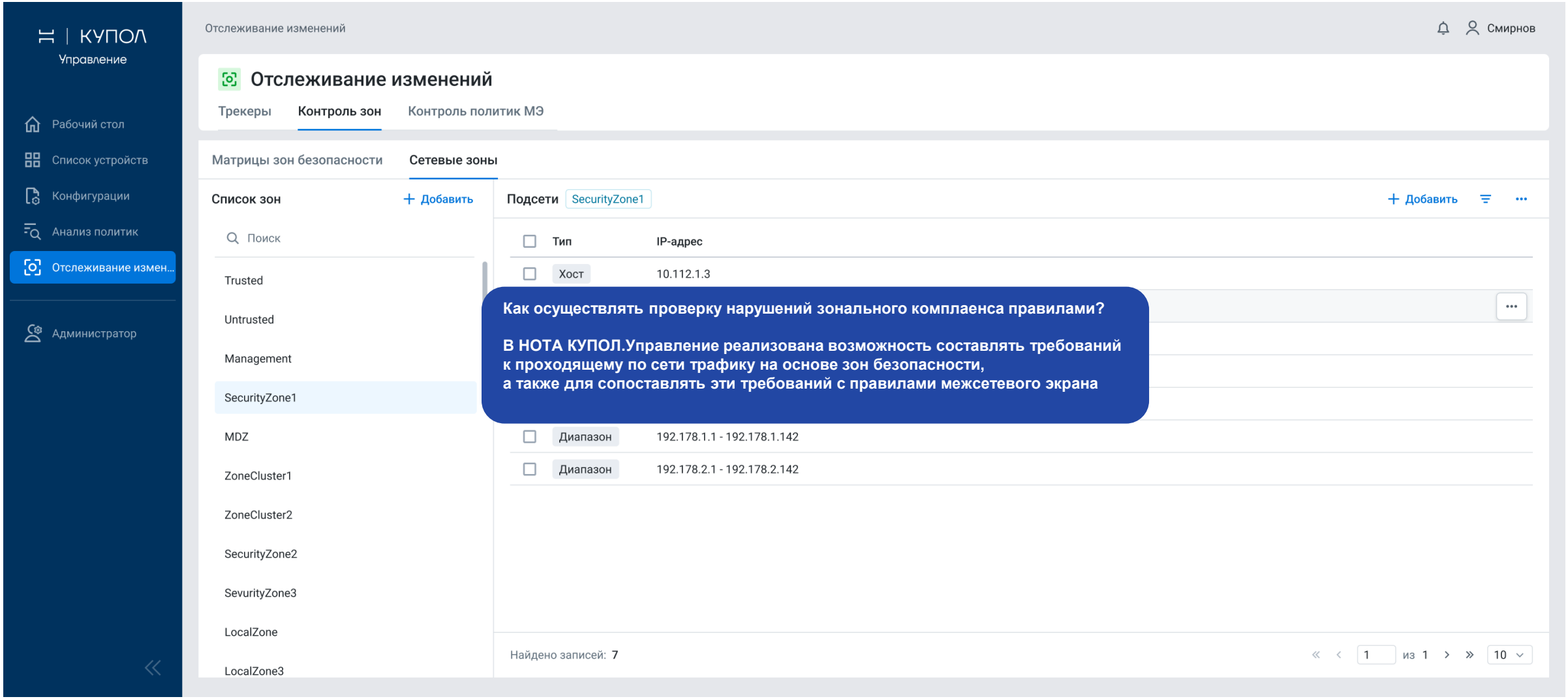
Кейс 1: мы хотим запретить доступ из публичной зоны в DMZ и обратно. Если где-то появится политика, противоречащая этой глобальной политике, то мы хотим об этом узнать и получить рекомендации по устранению.

Кейс 2: мы хотим контролировать отсутствие «дыр» в политиках, которые могут позволить проникнуть в инфраструктуру. Для этого нам нужно обязательно понимать контекст всех устройств.

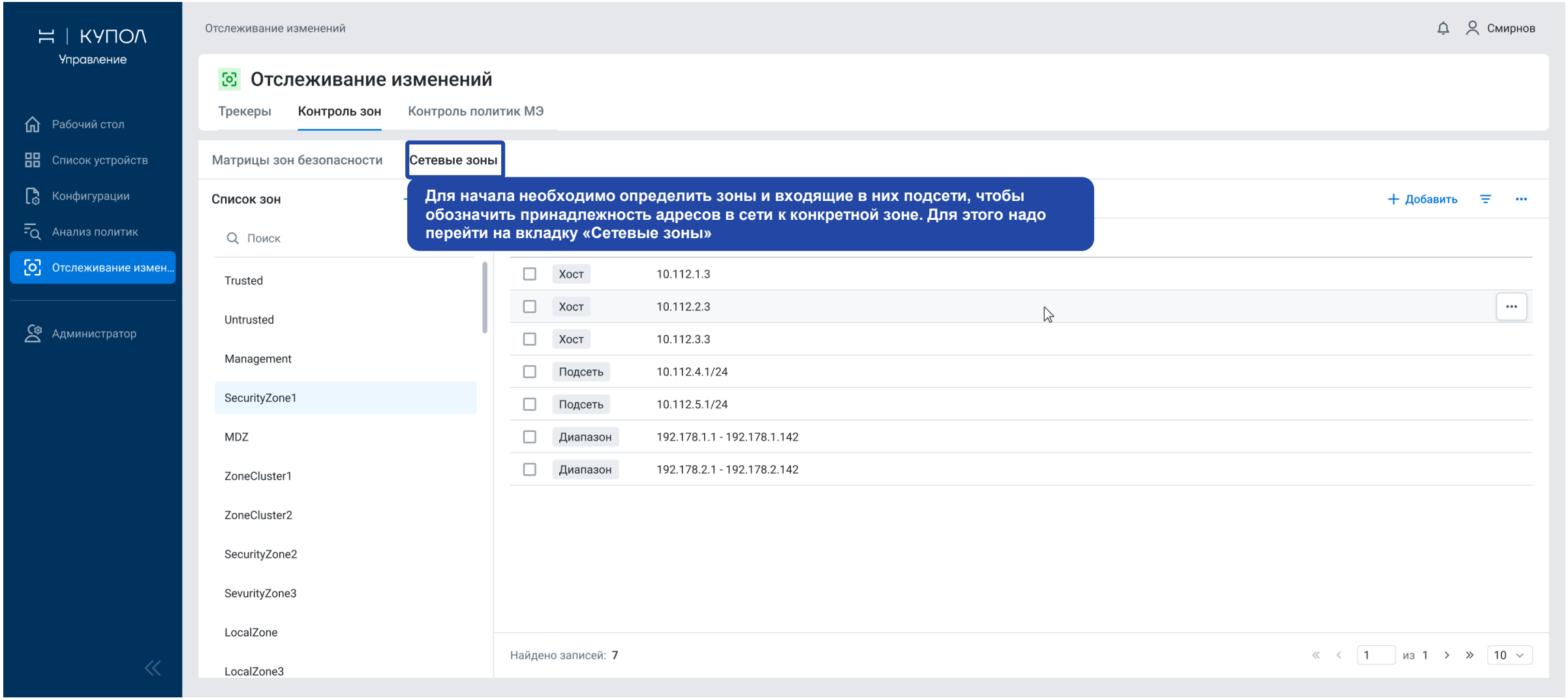


ЗОНАЛЬНЫЙ АНАЛИЗ

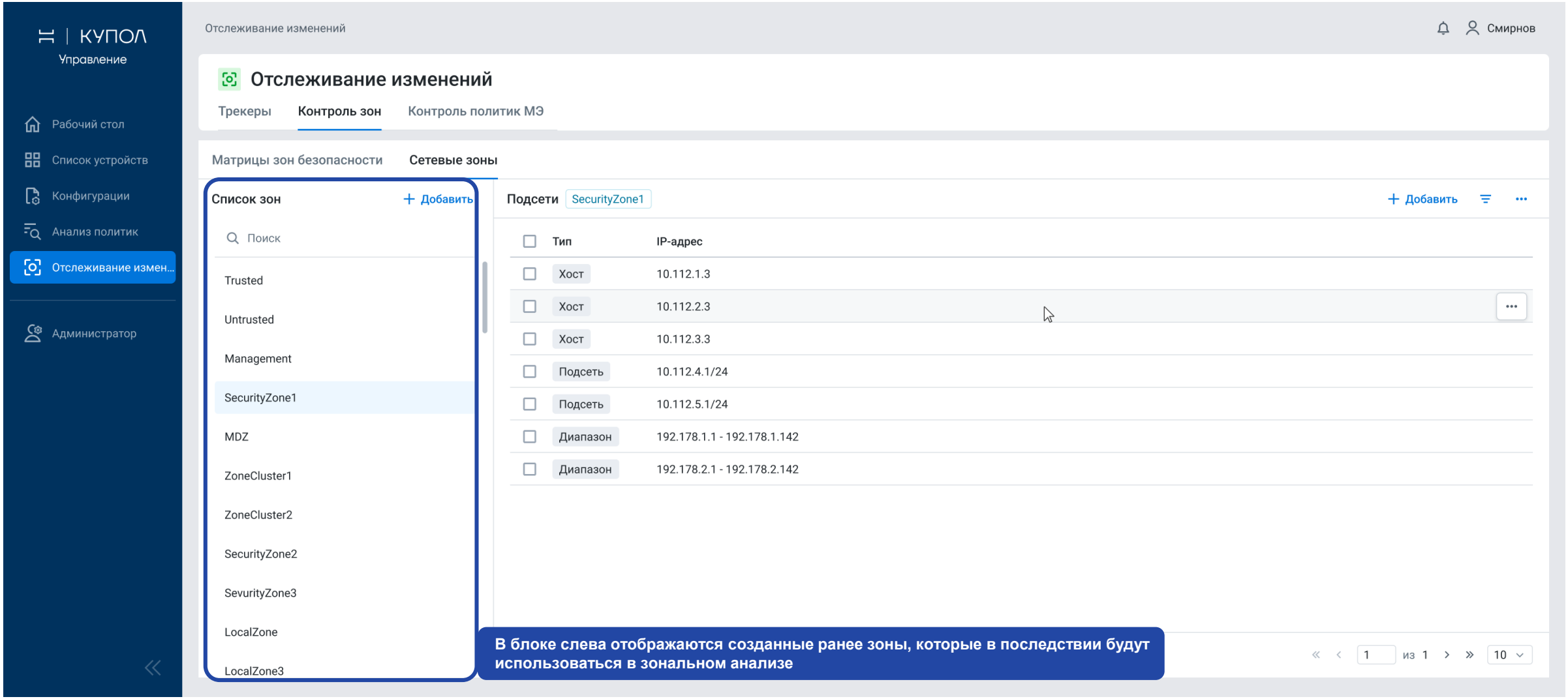
НОТА | КУПОЛ



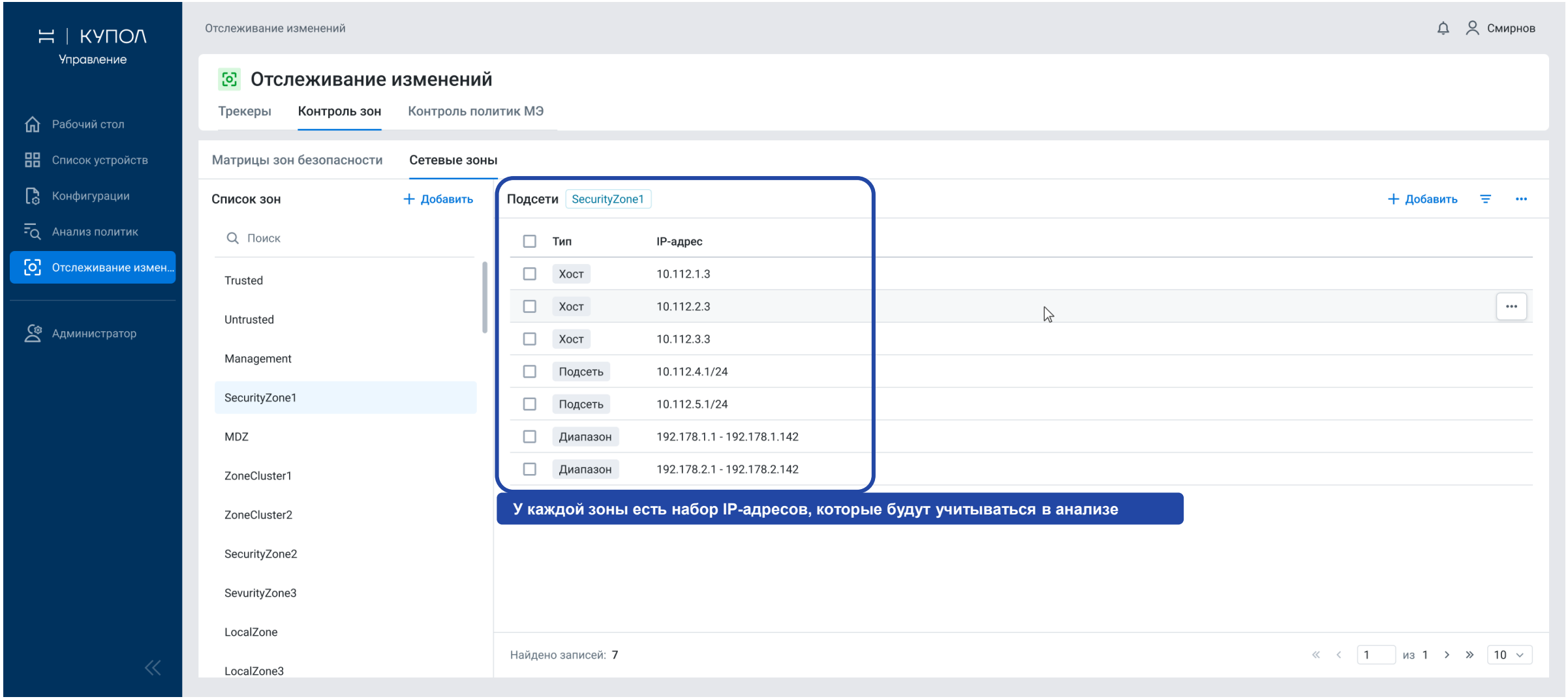
ЗОНАЛЬНЫЙ АНАЛИЗ



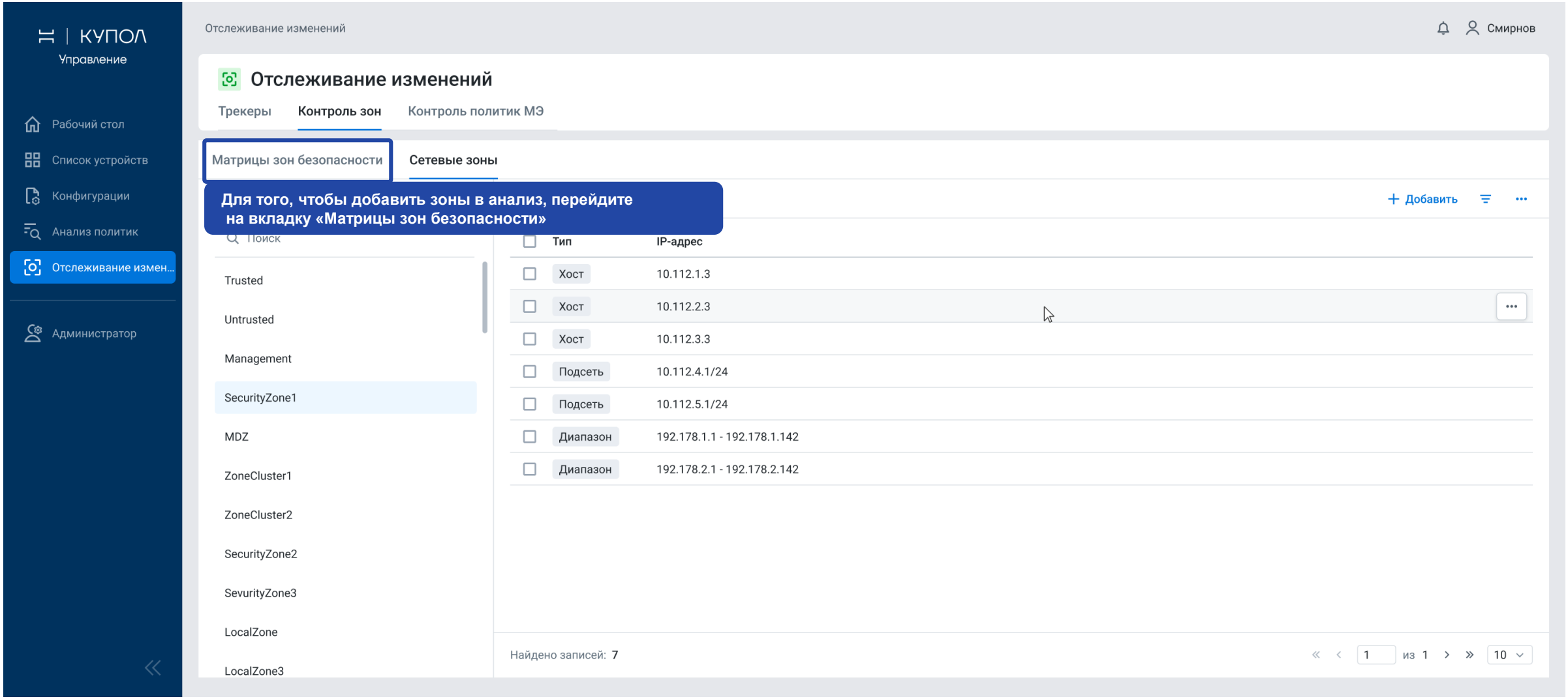
ЗОНАЛЬНЫЙ АНАЛИЗ



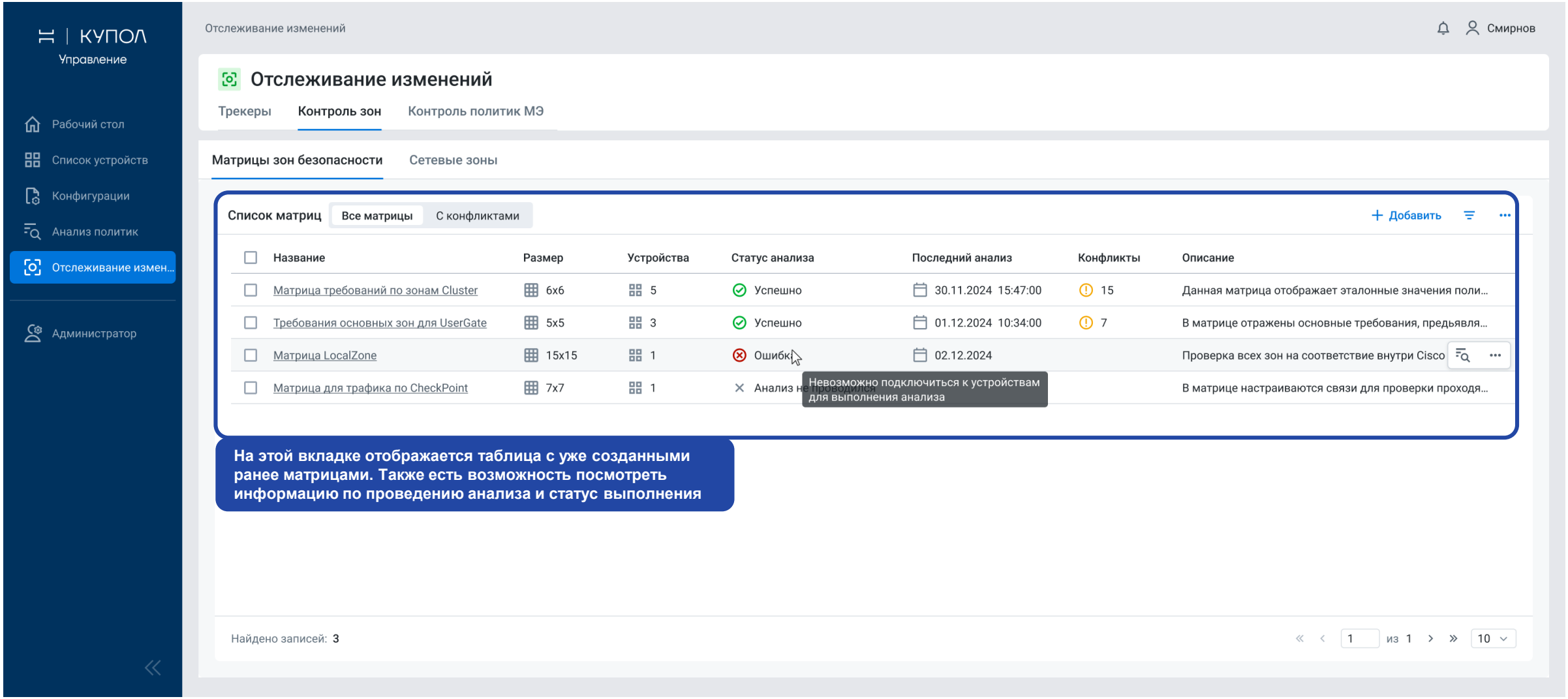
ЗОНАЛЬНЫЙ АНАЛИЗ



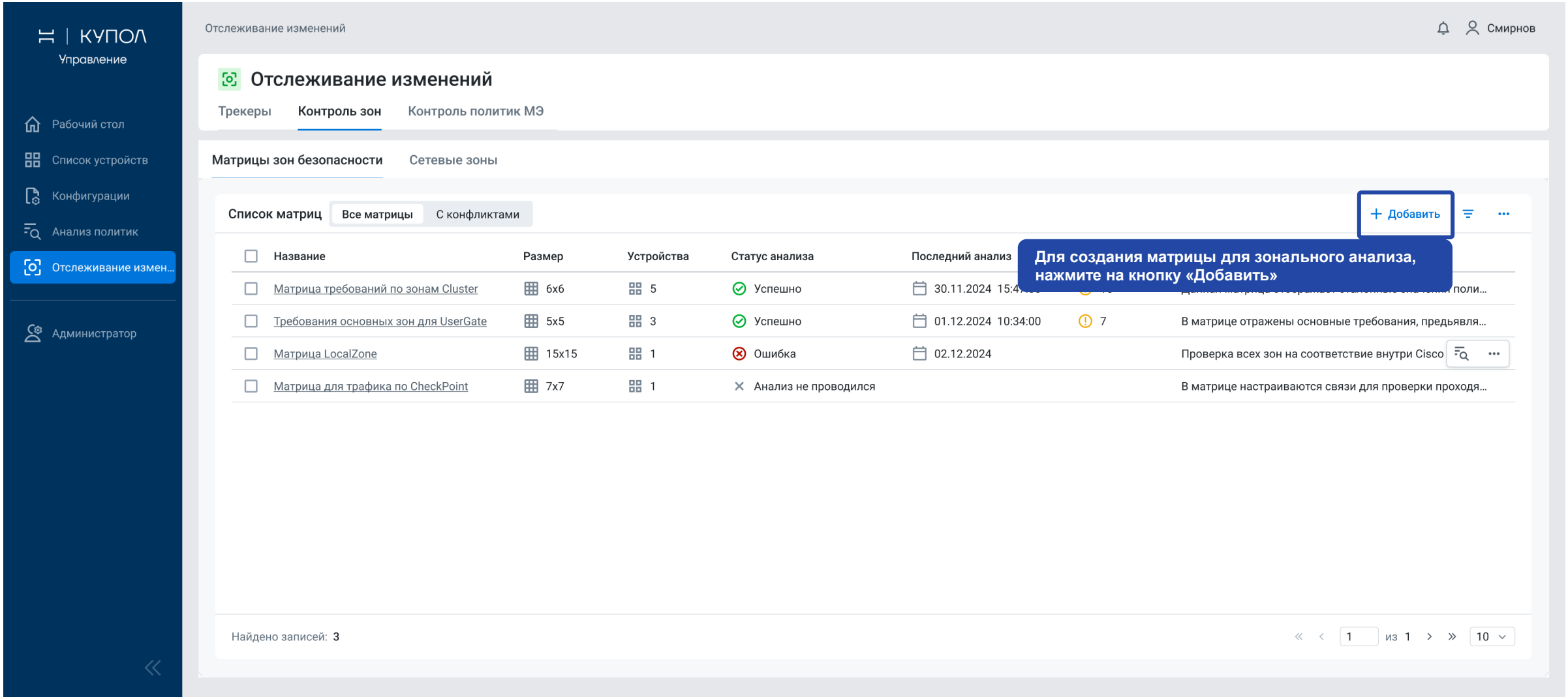
ЗОНАЛЬНЫЙ АНАЛИЗ



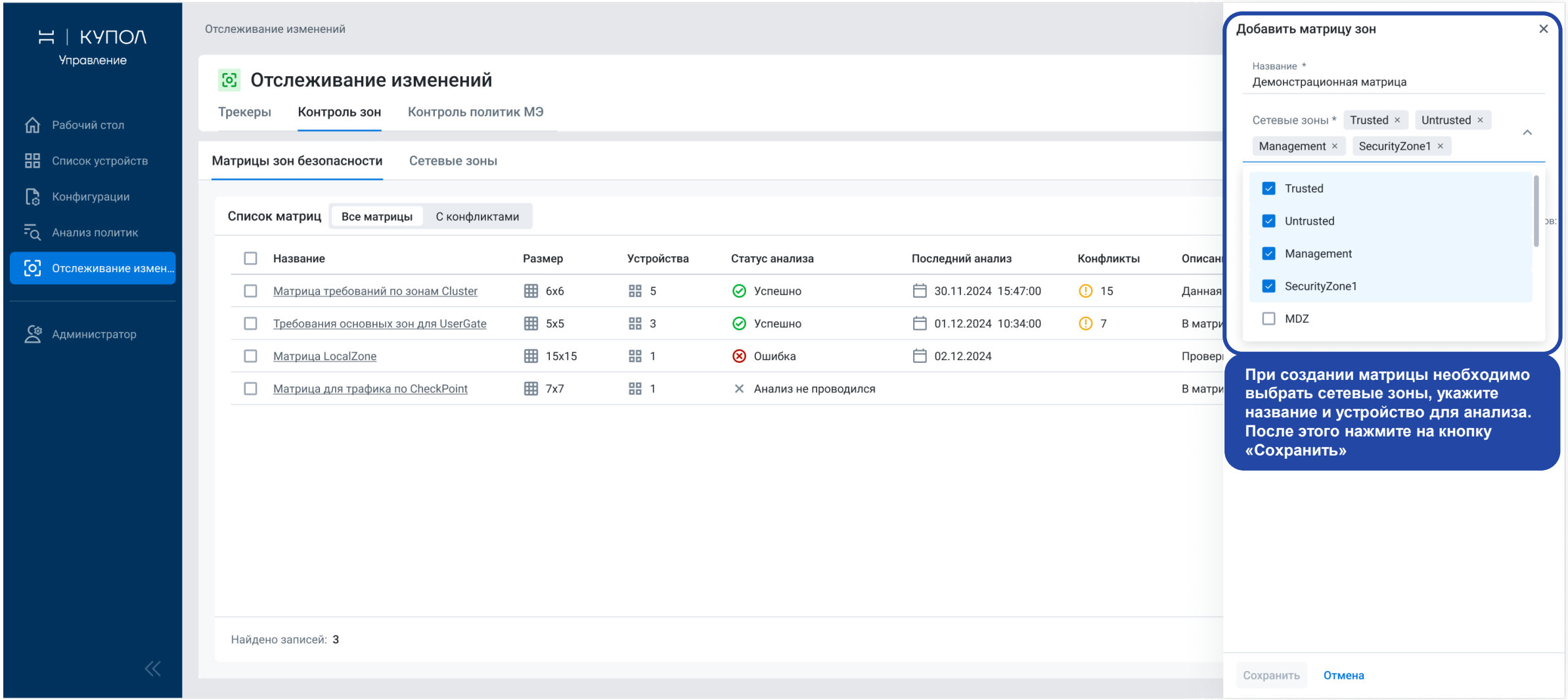
ЗОНАЛЬНЫЙ АНАЛИЗ



ЗОНАЛЬНЫЙ АНАЛИЗ

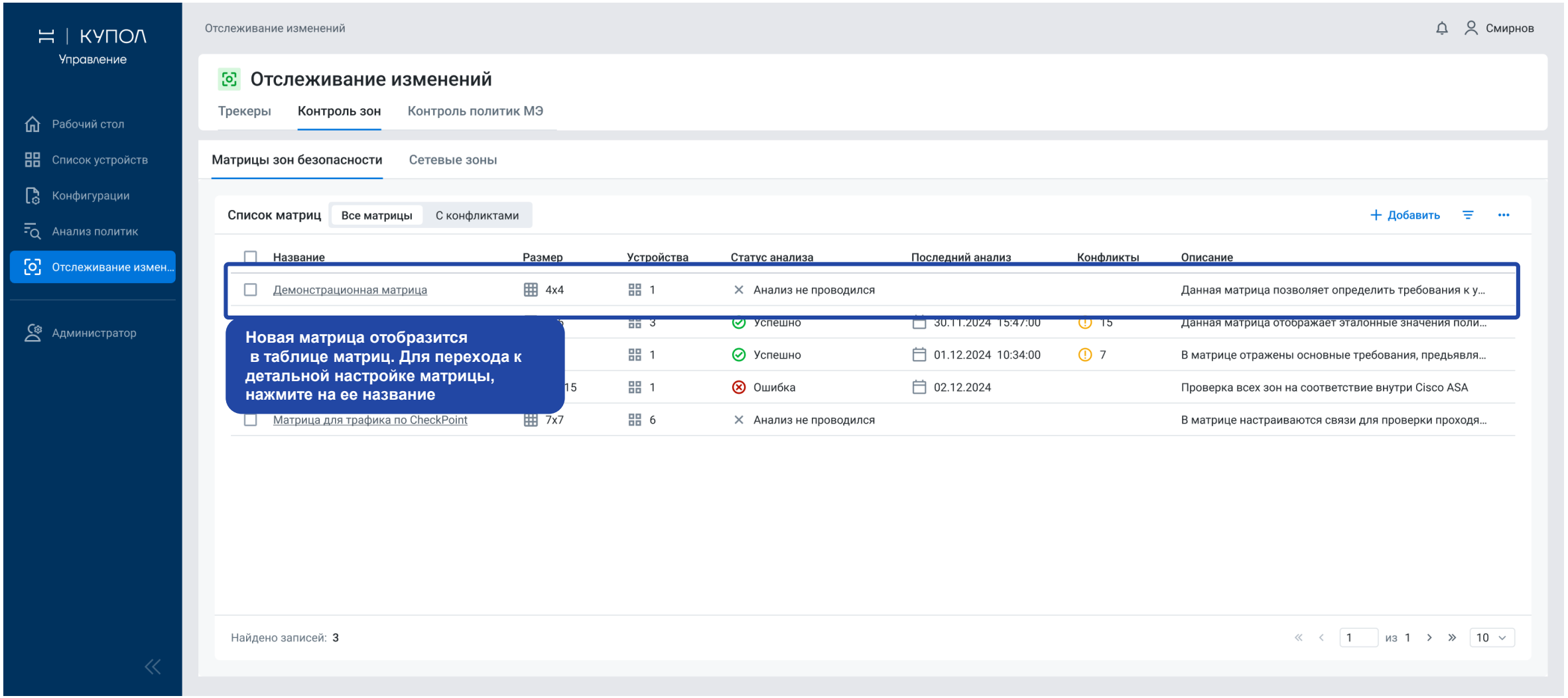


ЗОНАЛЬНЫЙ АНАЛИЗ

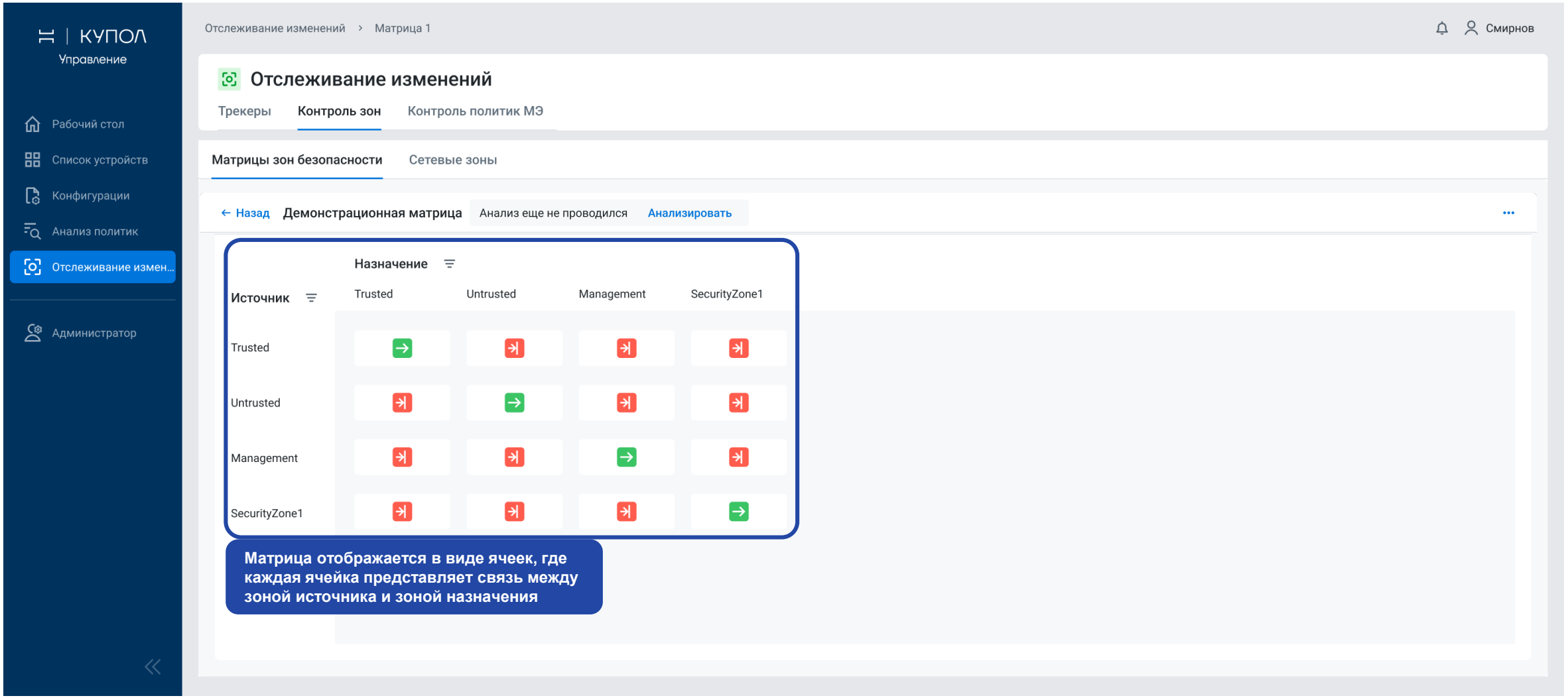


При создании матрицы необходимо выбрать сетевые зоны, укажите название и устройство для анализа. После этого нажмите на кнопку «Сохранить»

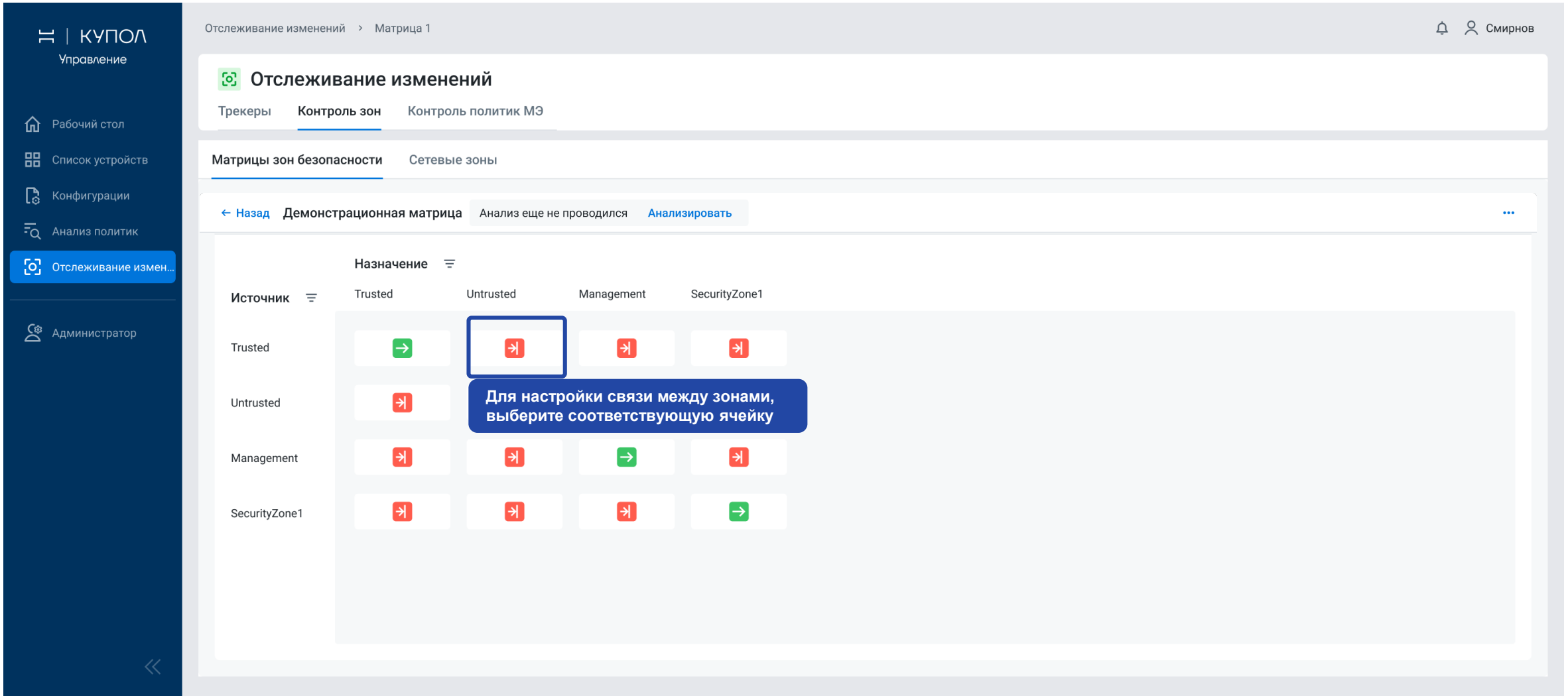
ЗОНАЛЬНЫЙ АНАЛИЗ



ЗОНАЛЬНЫЙ АНАЛИЗ

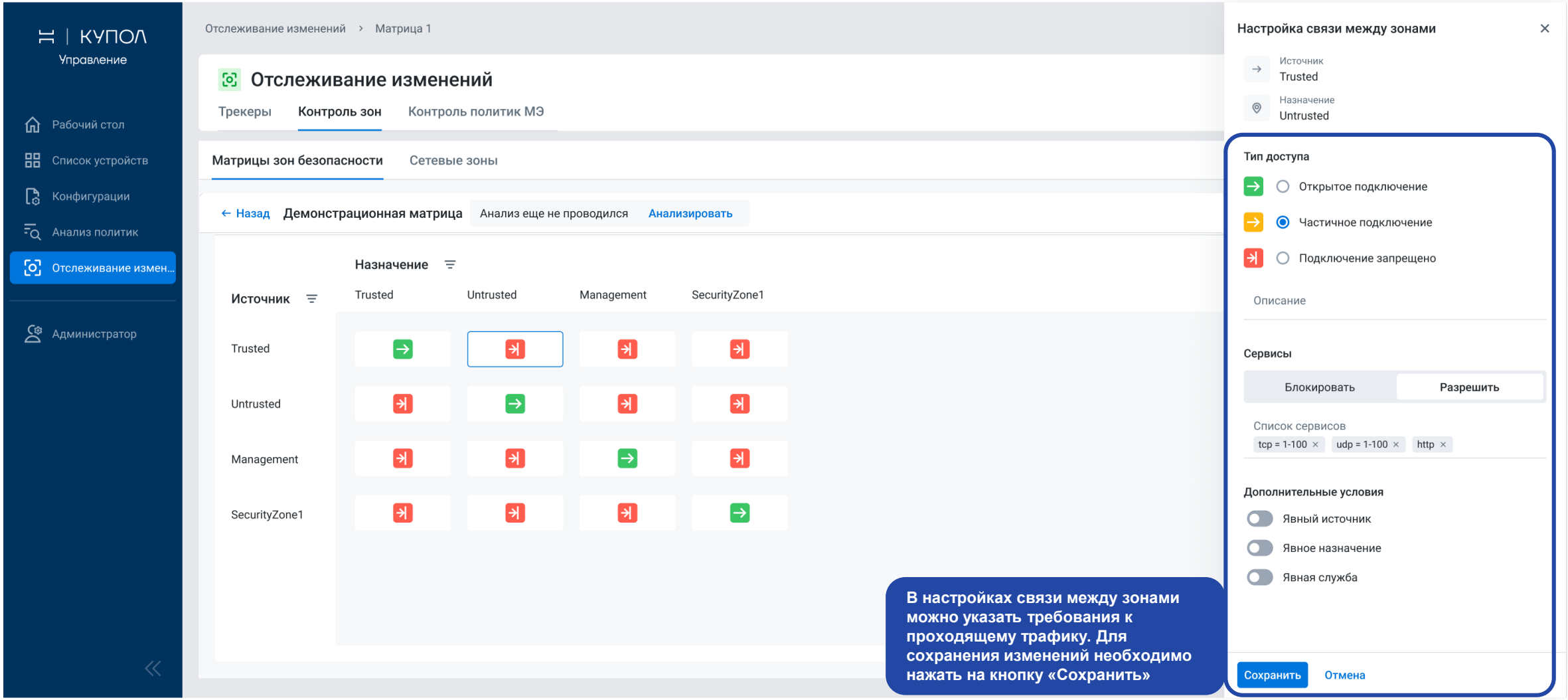


ЗОНАЛЬНЫЙ АНАЛИЗ

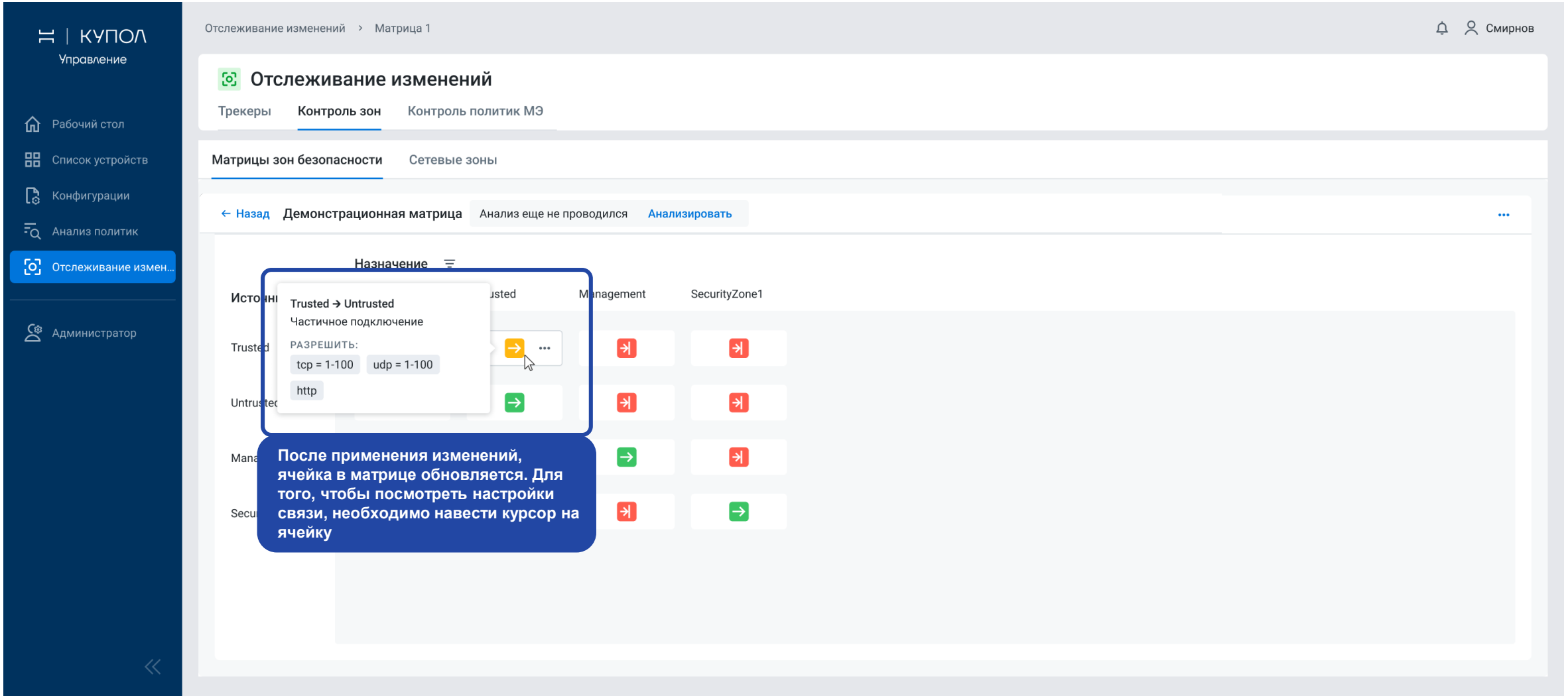


ЗОНАЛЬНЫЙ АНАЛИЗ

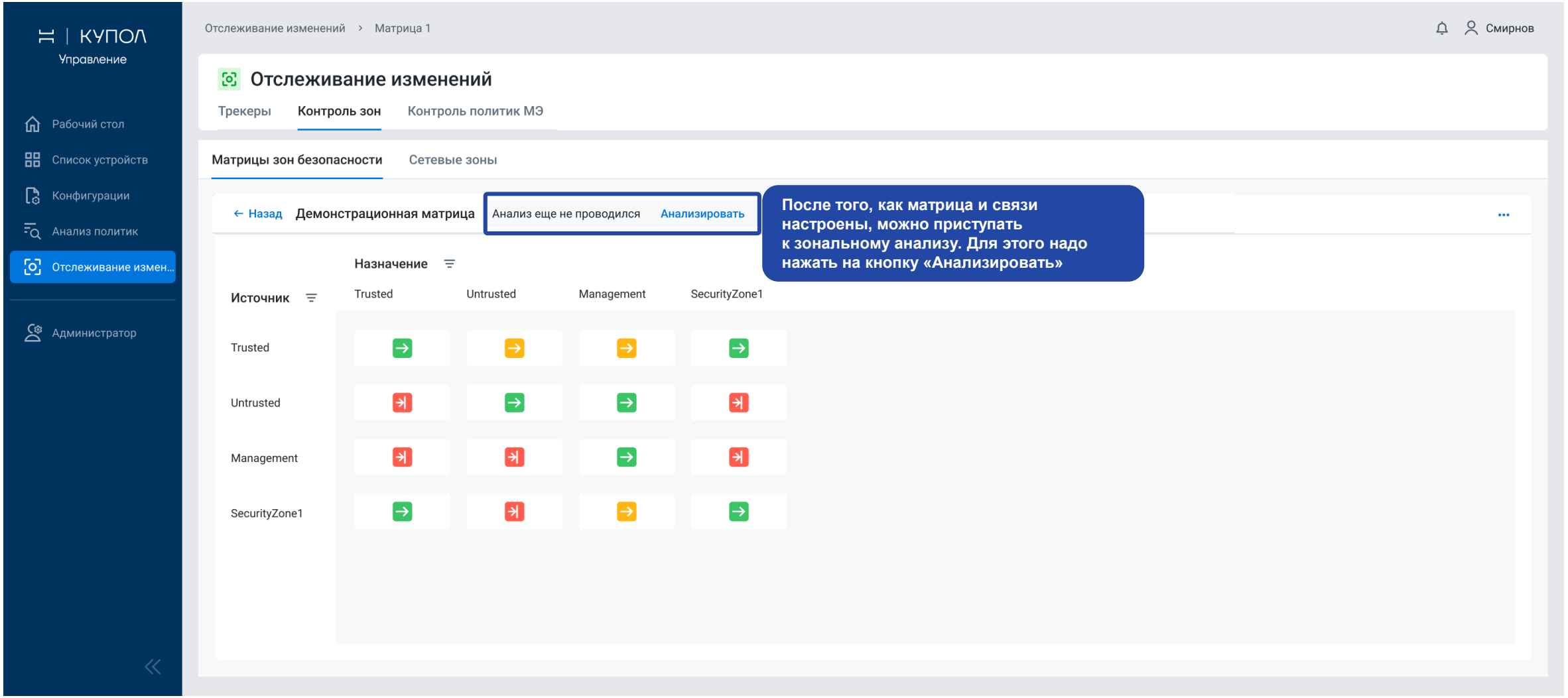
НОТА | КУПОЛ



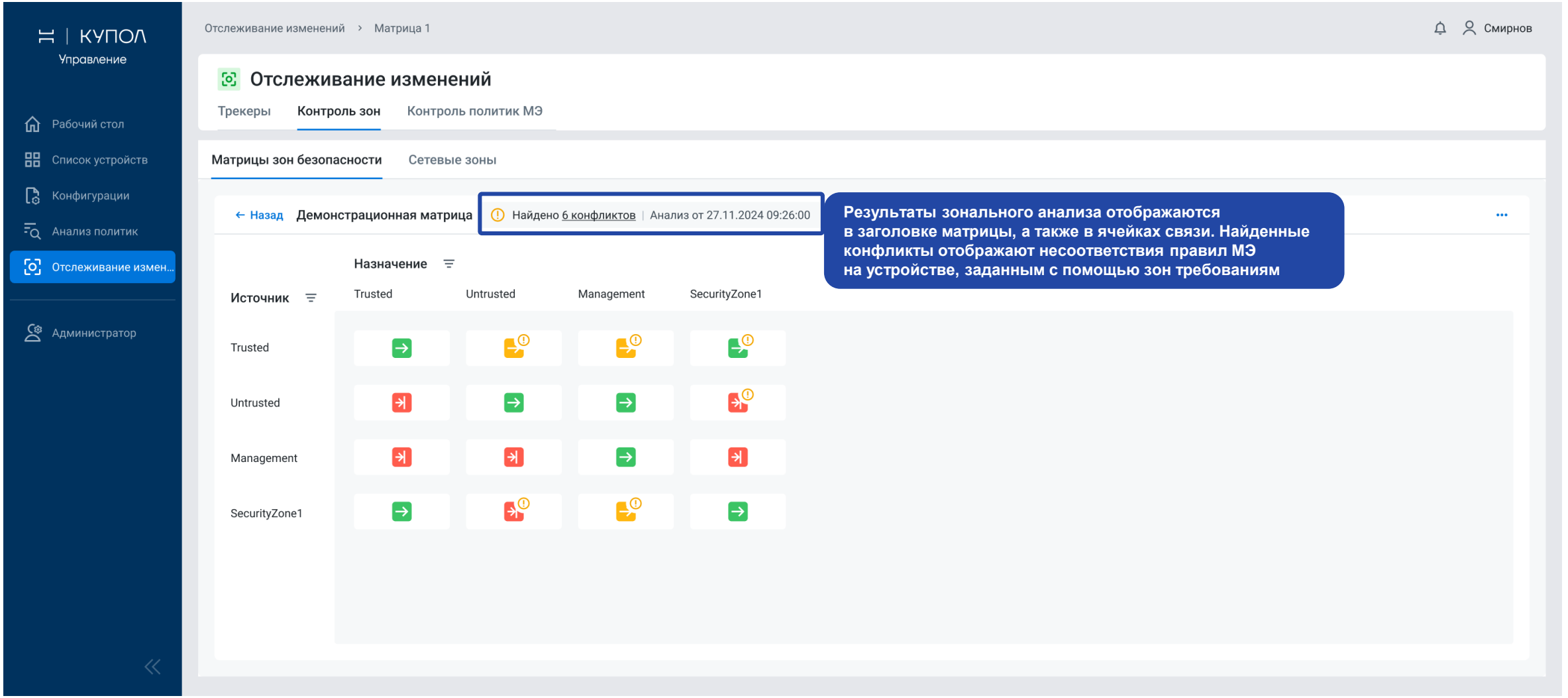
ЗОНАЛЬНЫЙ АНАЛИЗ



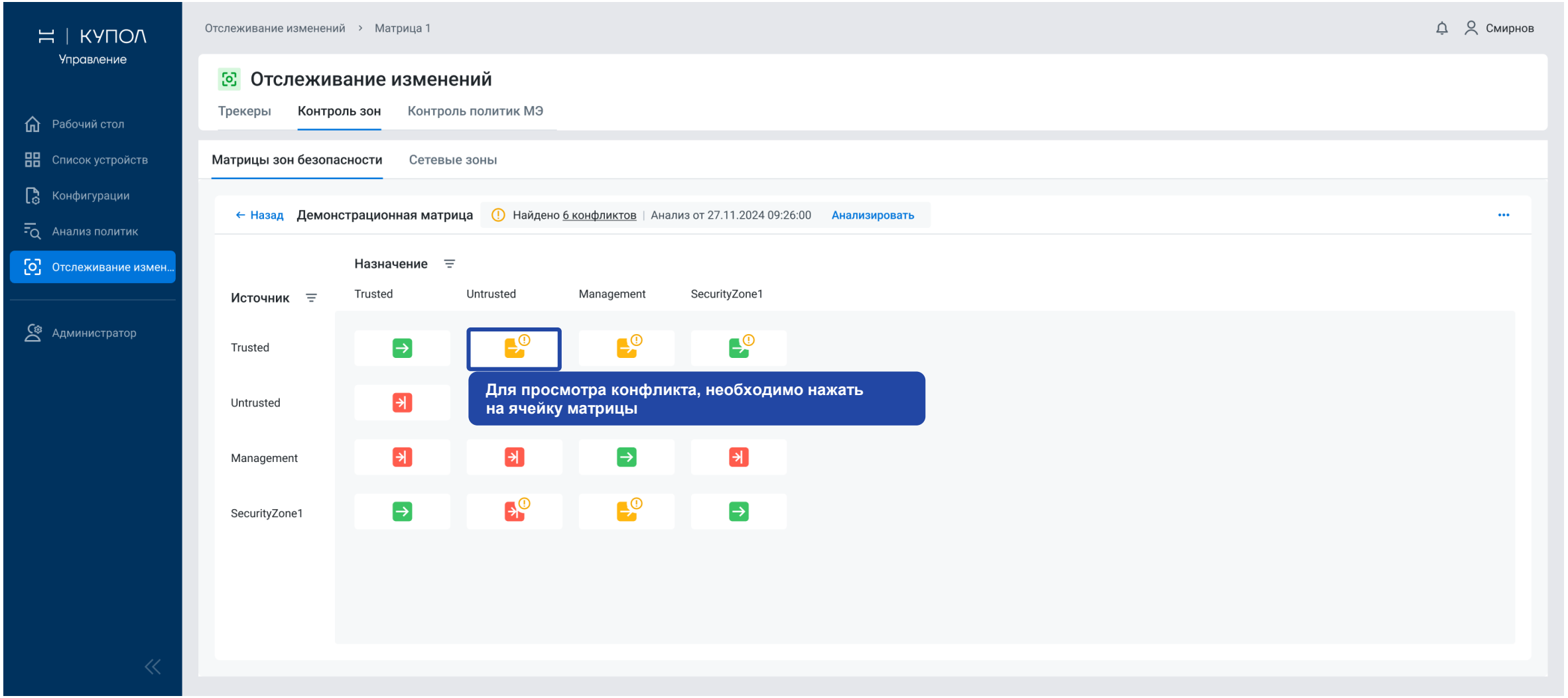
ЗОНАЛЬНЫЙ АНАЛИЗ



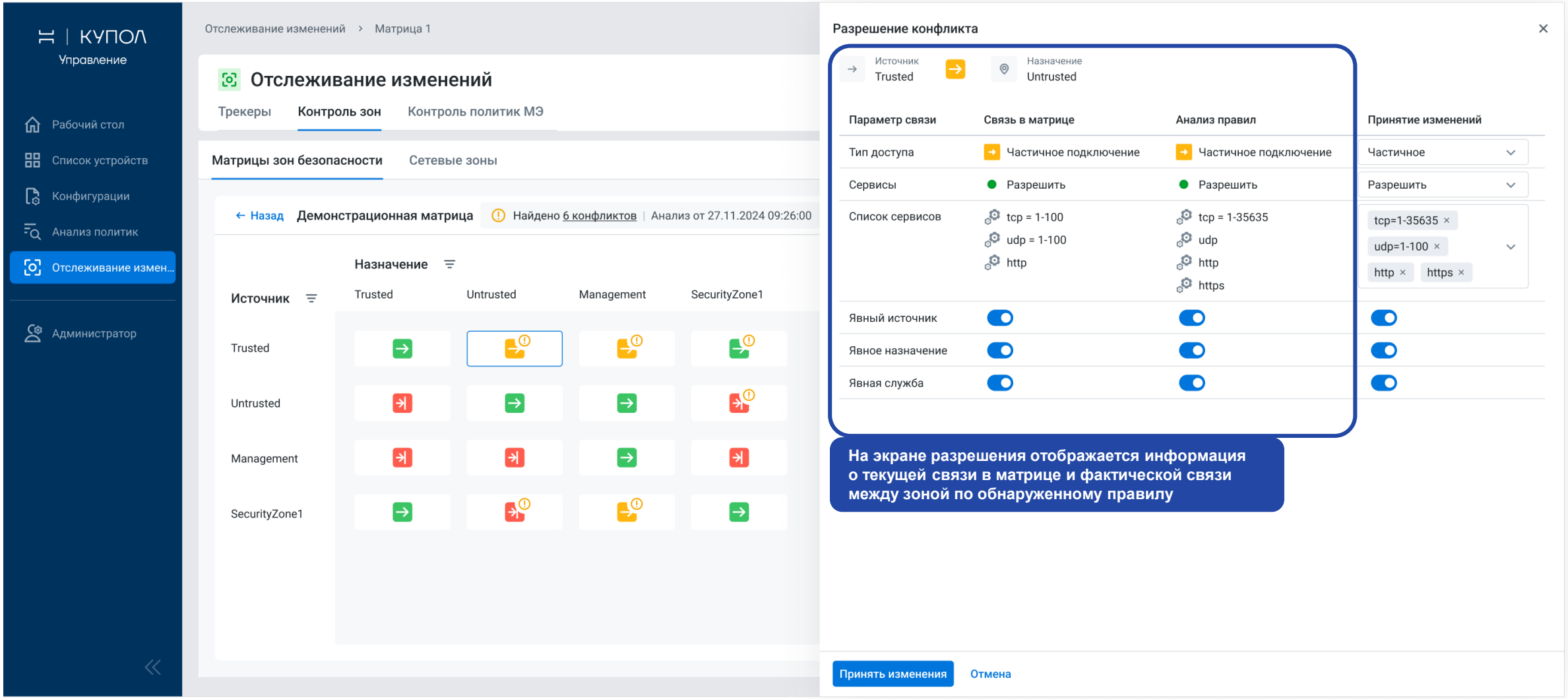
ЗОНАЛЬНЫЙ АНАЛИЗ



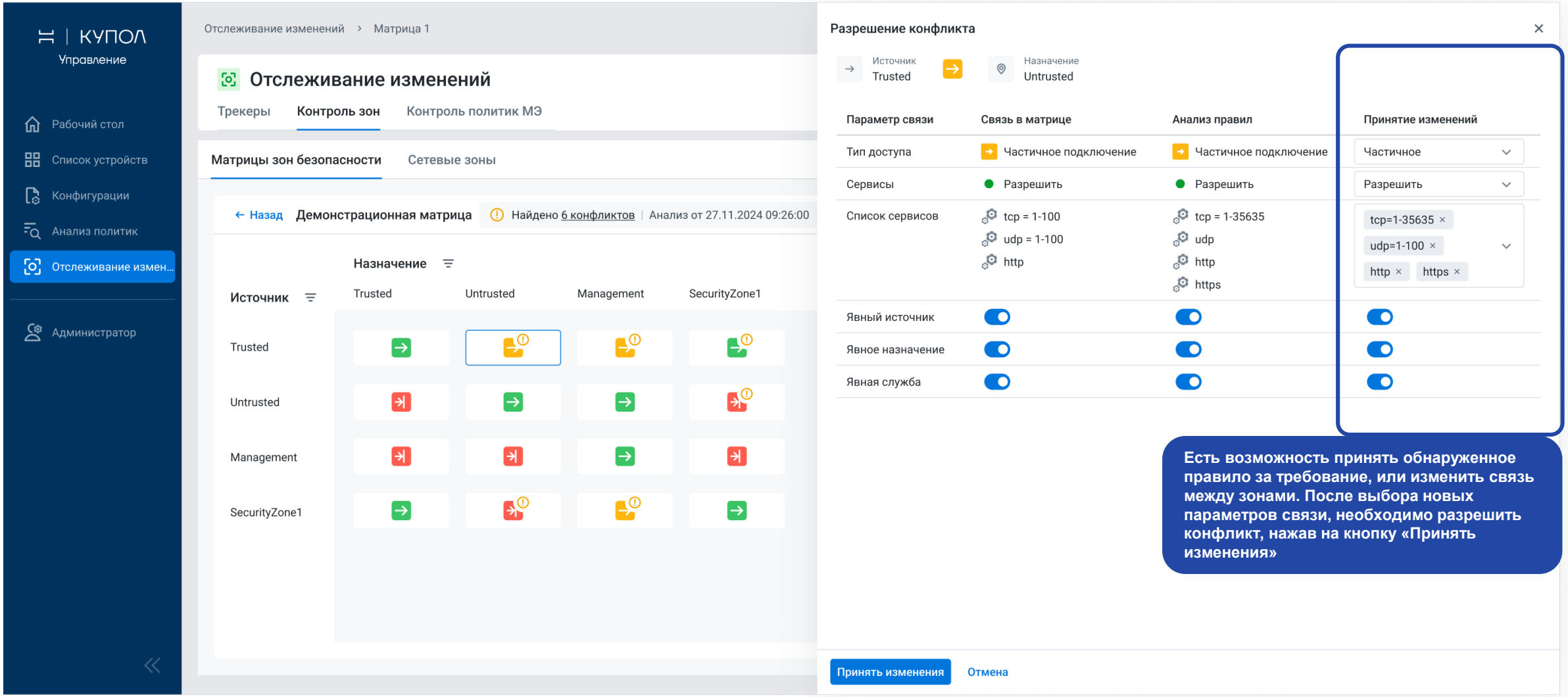
ЗОНАЛЬНЫЙ АНАЛИЗ



ЗОНАЛЬНЫЙ АНАЛИЗ

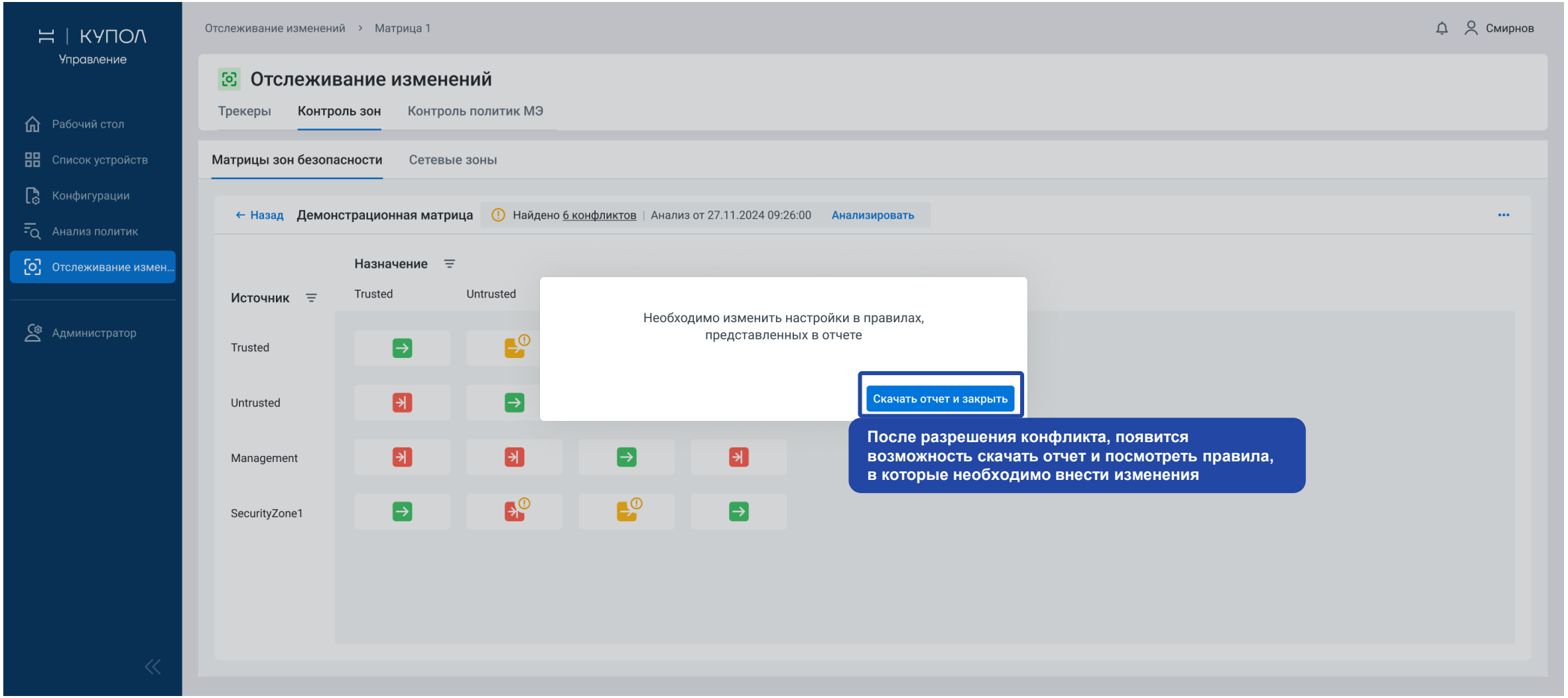


ЗОНАЛЬНЫЙ АНАЛИЗ



Есть возможность принять обнаруженное правило за требование, или изменить связь между зонами. После выбора новых параметров связи, необходимо разрешить конфликт, нажав на кнопку «Принять изменения»

ЗОНАЛЬНЫЙ АНАЛИЗ

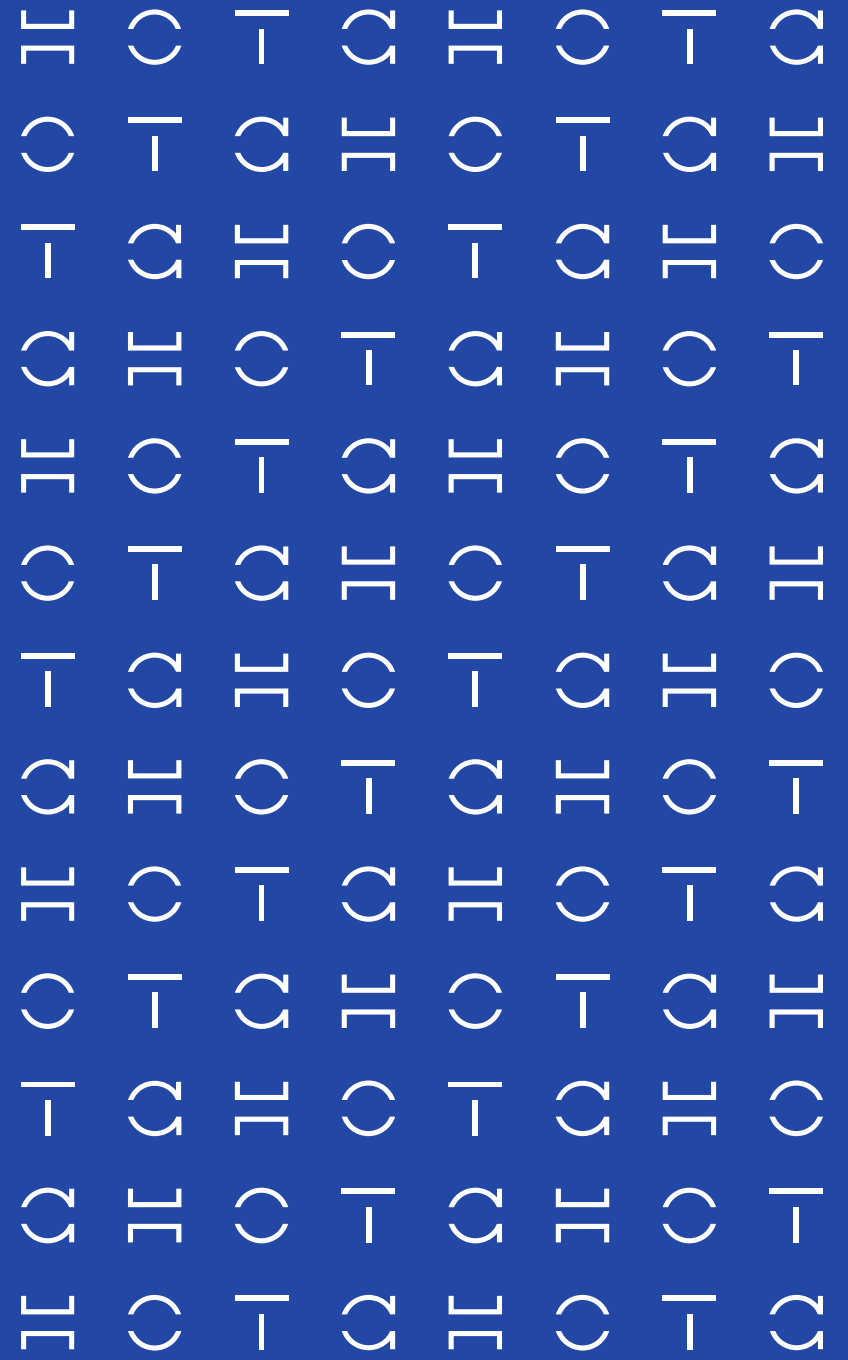


РЕЗЕРВНЫЕ КОПИИ

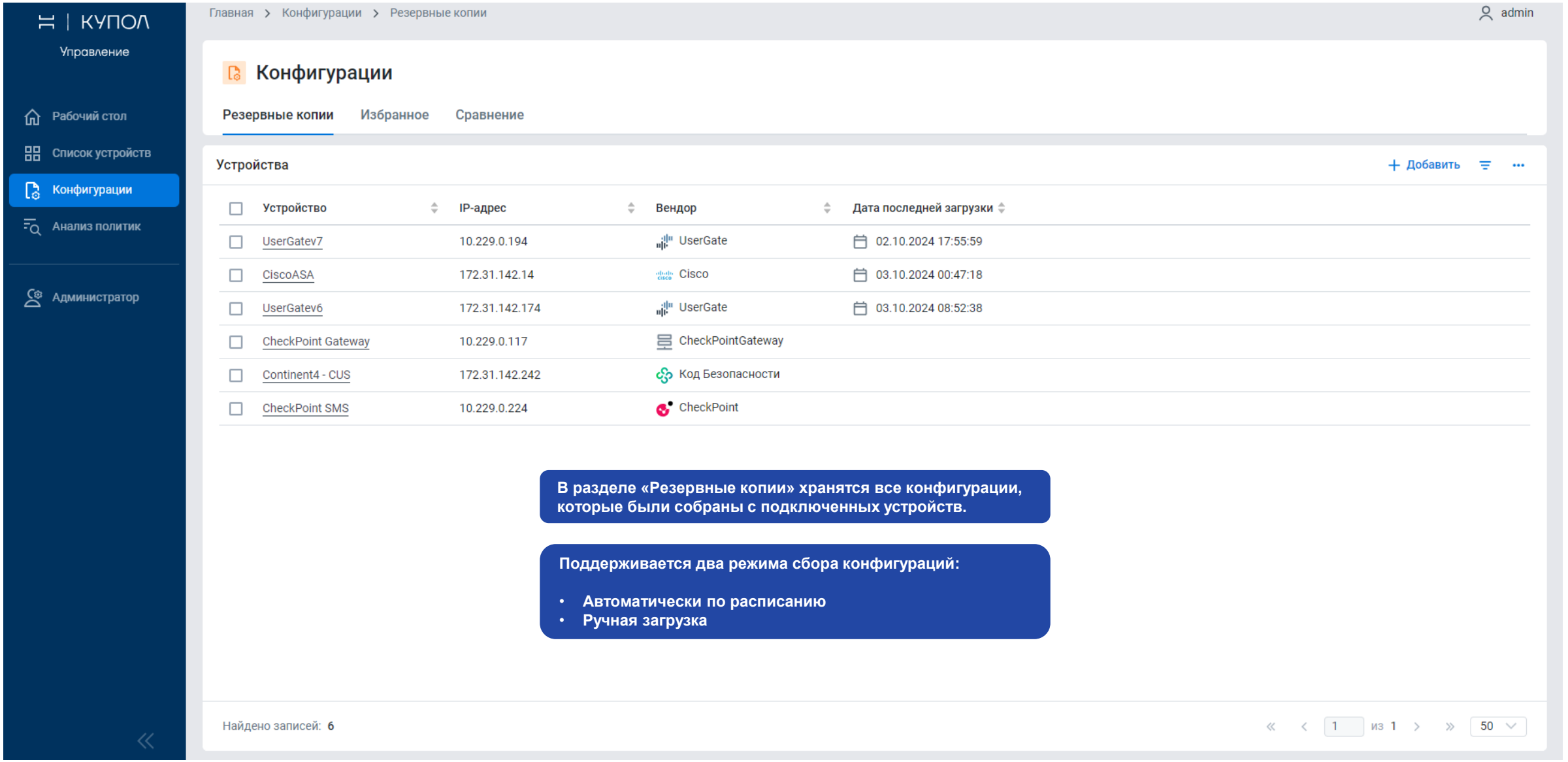
Задача 1: Вернуть систему к состоянию «До нелигитимных/ошибочных/несоответствующих политикам изменений» в случае их изменения сотрудниками компании или злоумышленником.

Кейс: Что-то в работе устройства/сети пошло не так, и нужно быстро откатить инфраструктуру к рабочему состоянию.

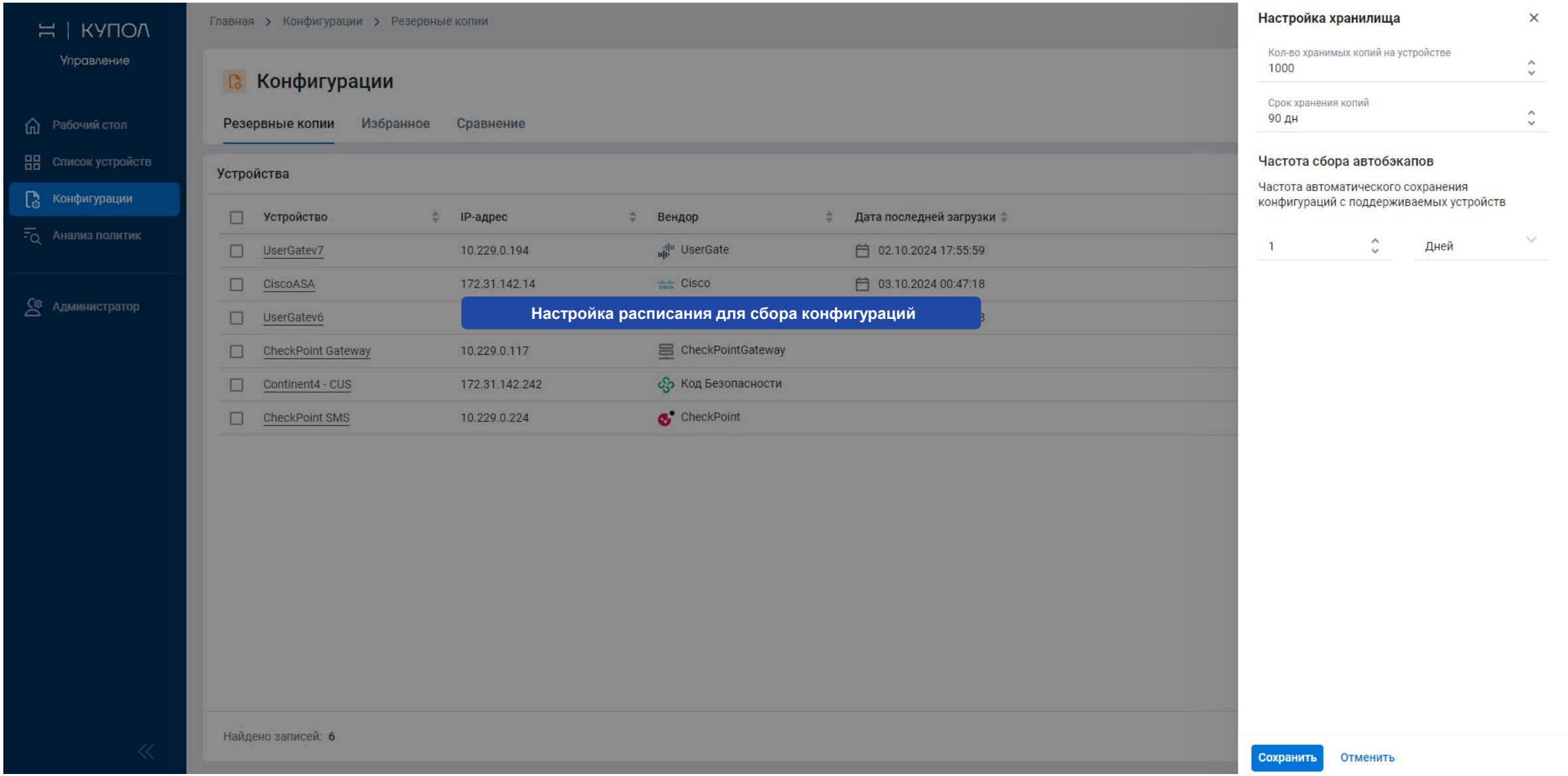
Задача 2: Сравнить разные версии политик на одном или разных устройствах между собой.
Кейс: понять, почему сотрудник потерял доступ к ресурсу.



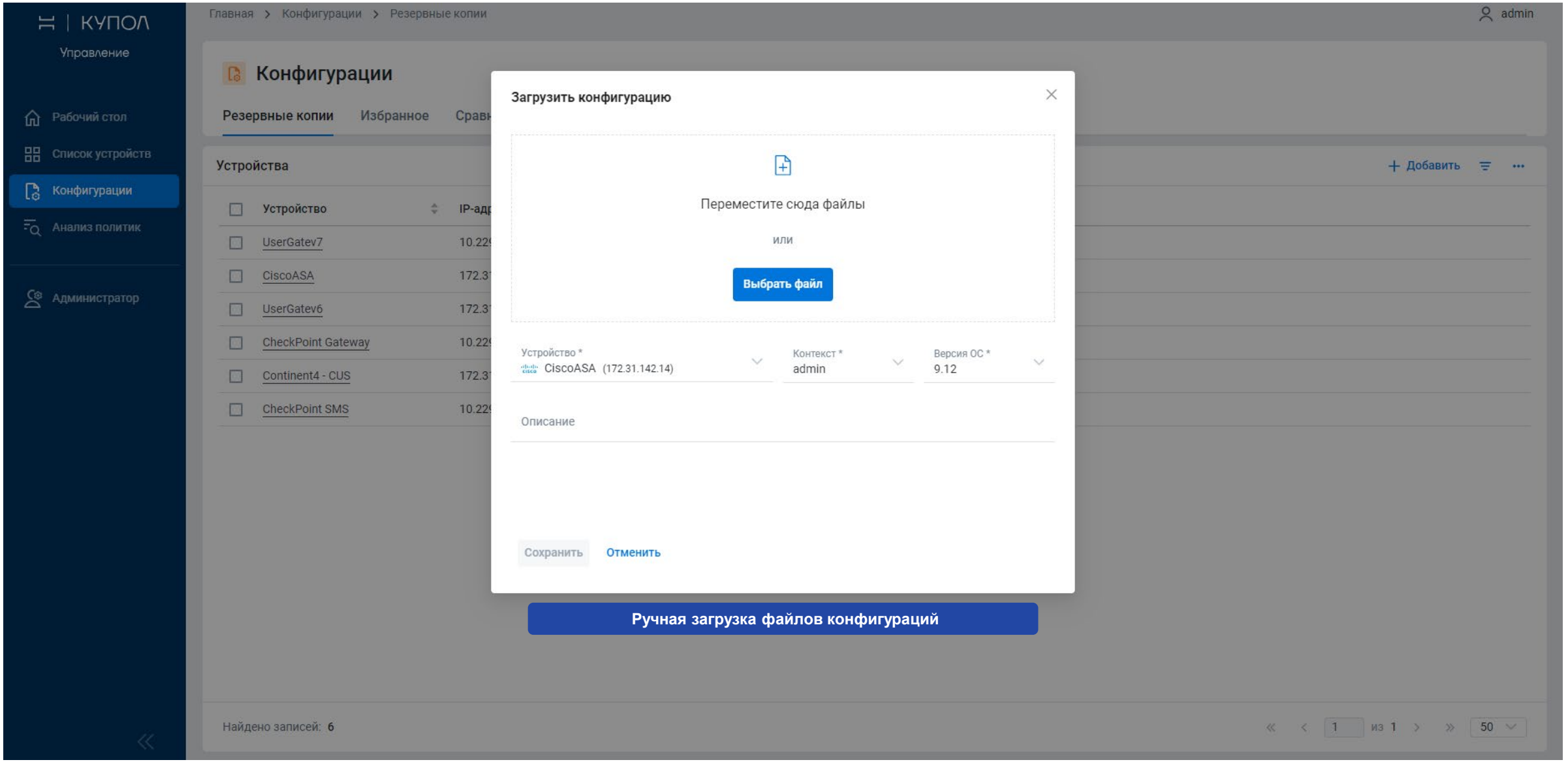
РЕЗЕРВНЫЕ КОПИИ



РЕЗЕРВНЫЕ КОПИИ

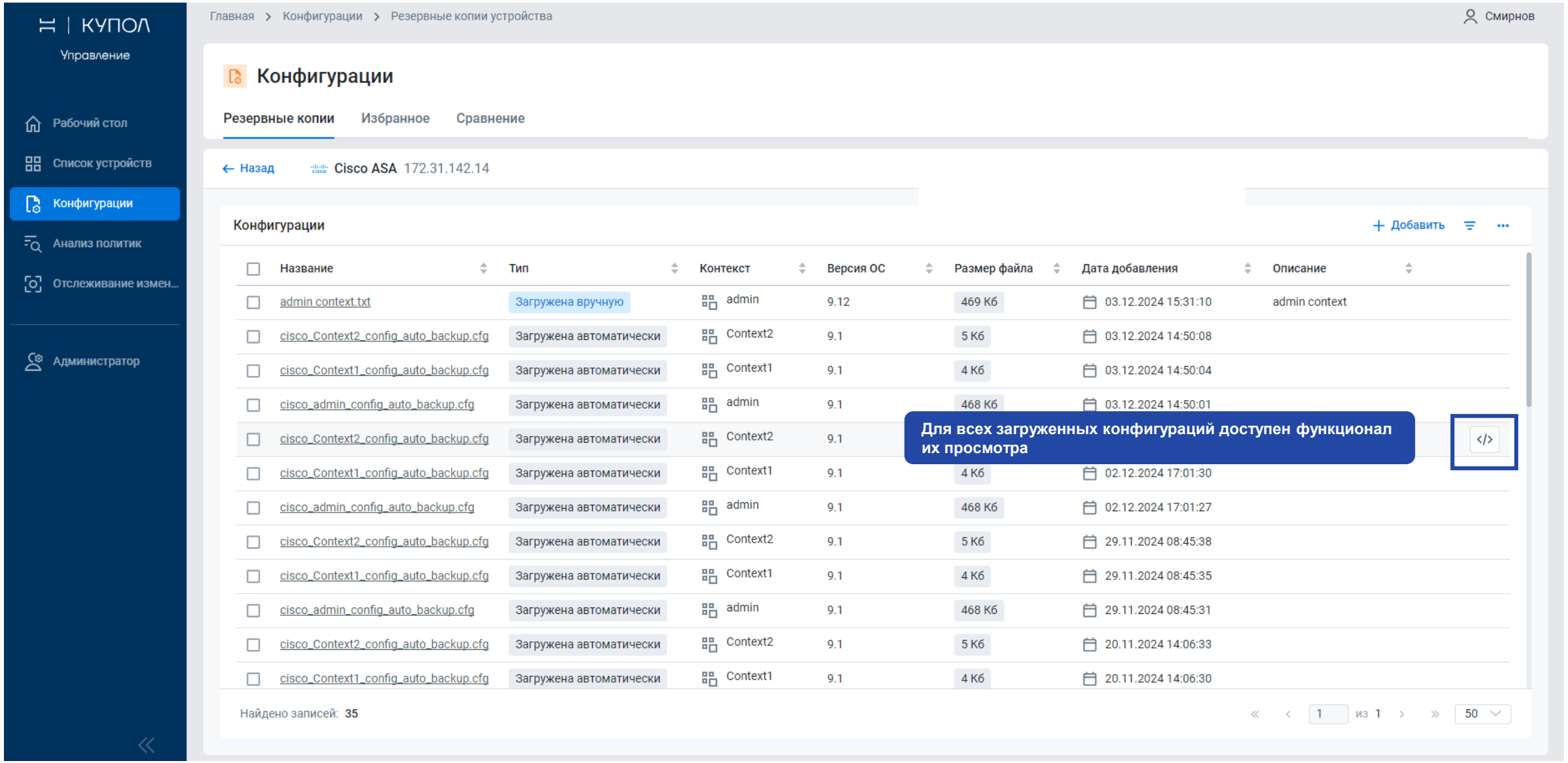


РЕЗЕРВНЫЕ КОПИИ

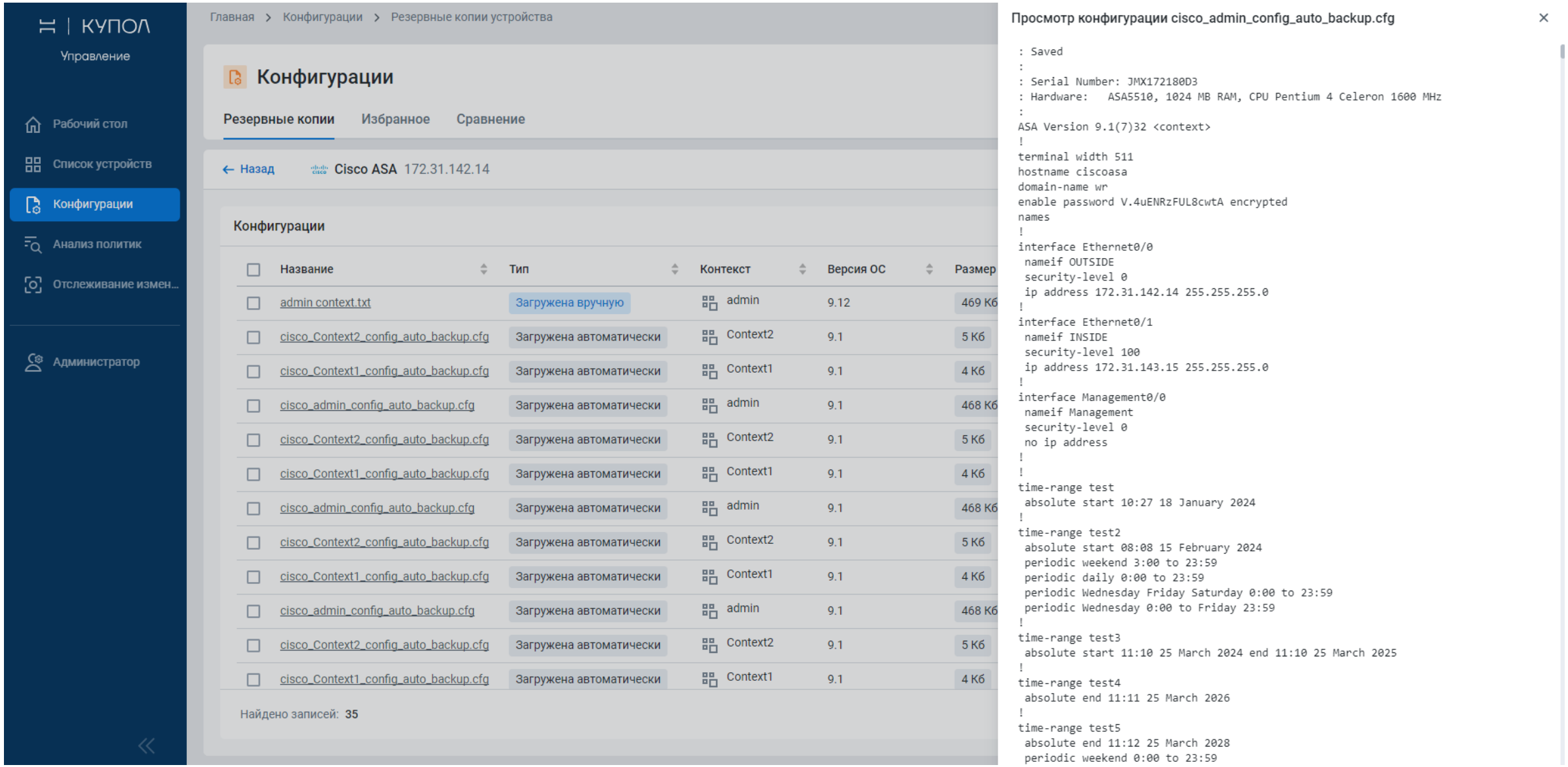


Ручная загрузка файлов конфигураций

РЕЗЕРВНЫЕ КОПИИ



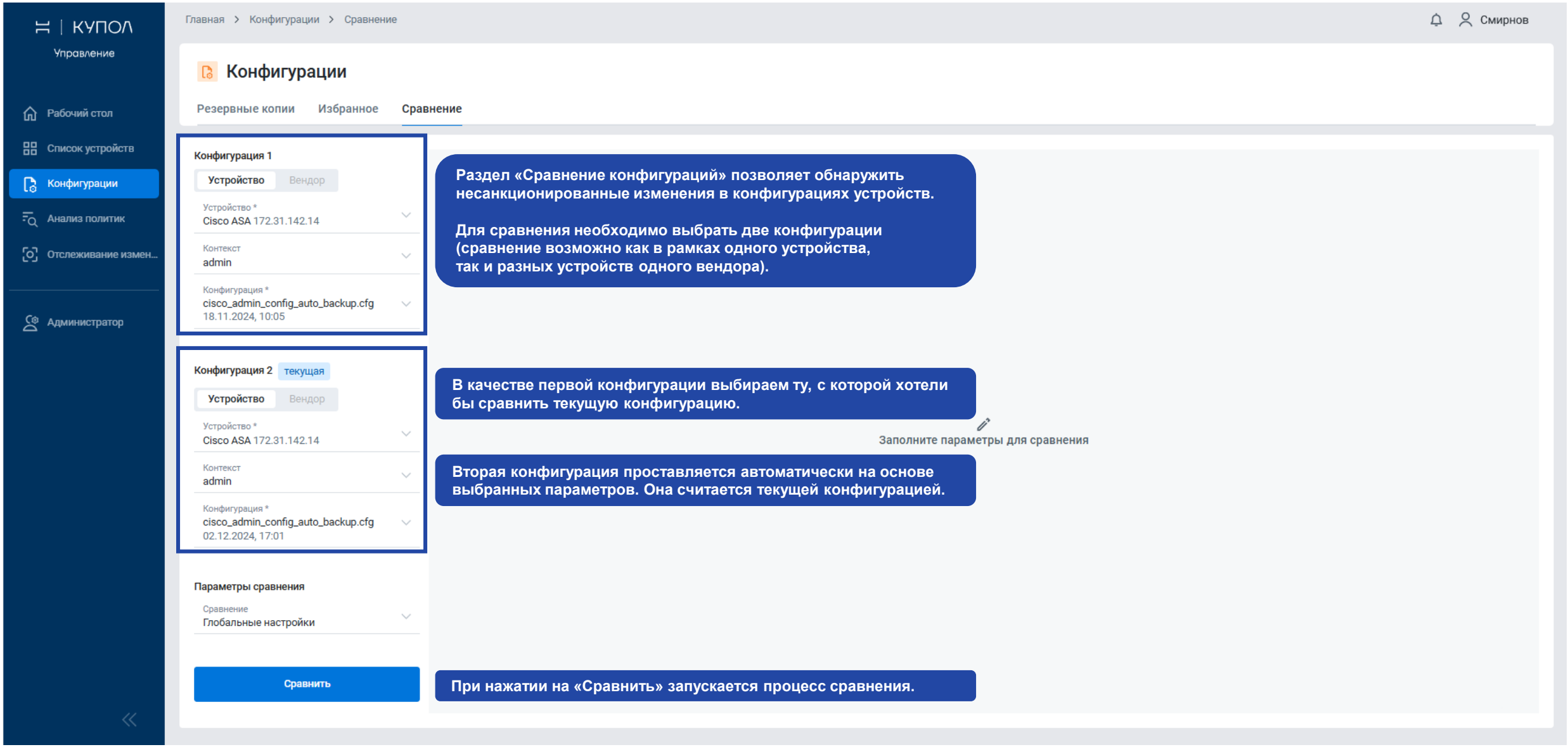
РЕЗЕРВНЫЕ КОПИИ



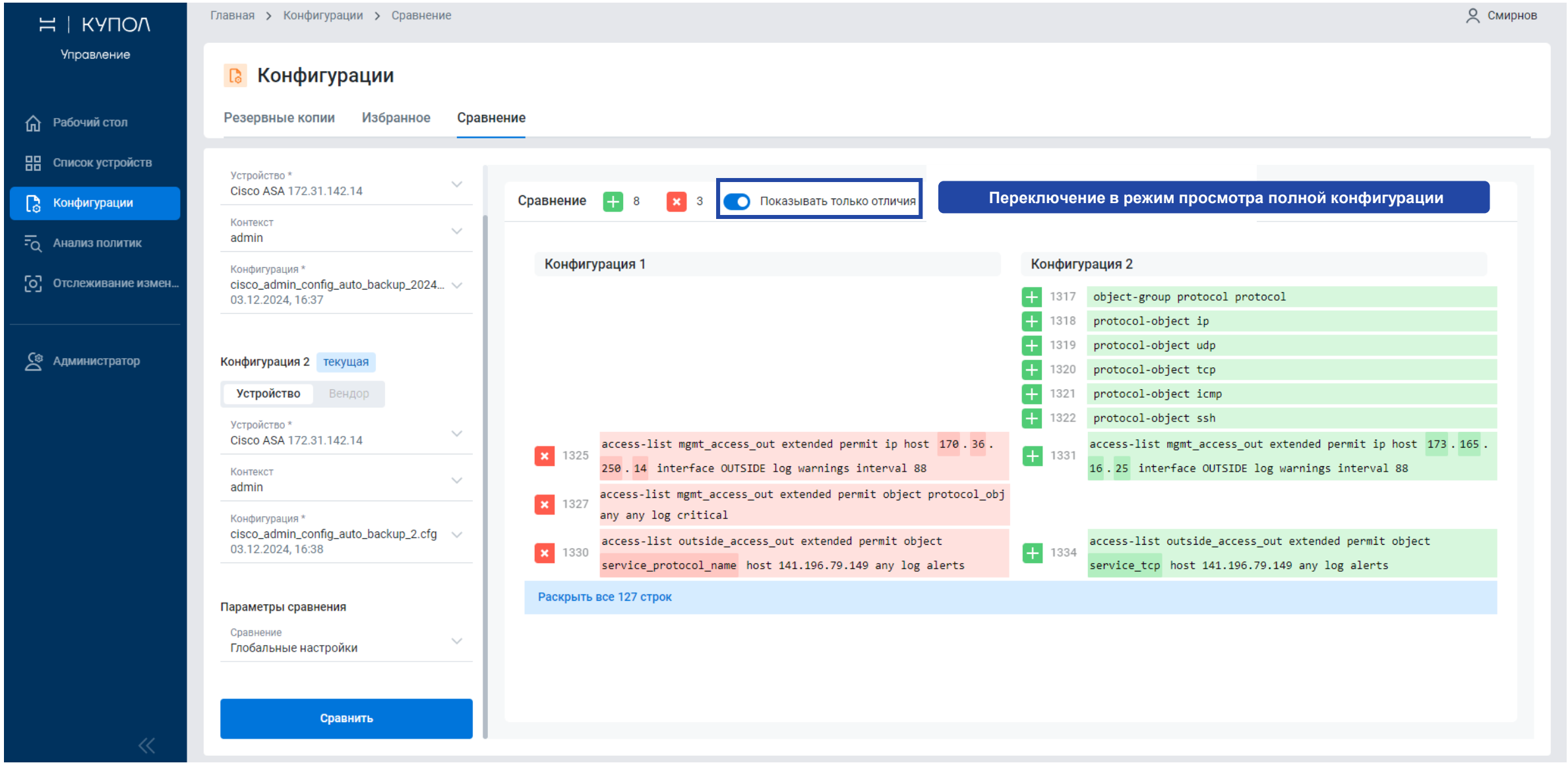
Просмотр конфигурации cisco_admin_config_auto_backup.cfg

```
: Saved
:
: Serial Number: JMX172180D3
: Hardware:   ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz
:
ASA Version 9.1(7)32 <context>
!
terminal width 511
hostname ciscoasa
domain-name wr
enable password V.4uENRzFUL8cwtA encrypted
names
!
interface Ethernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 172.31.142.14 255.255.255.0
!
interface Ethernet0/1
 nameif INSIDE
 security-level 100
 ip address 172.31.143.15 255.255.255.0
!
interface Management0/0
 nameif Management
 security-level 0
 no ip address
!
!
time-range test
 absolute start 10:27 18 January 2024
!
time-range test2
 absolute start 08:08 15 February 2024
 periodic weekend 3:00 to 23:59
 periodic daily 0:00 to 23:59
 periodic Wednesday Friday Saturday 0:00 to 23:59
 periodic Wednesday 0:00 to Friday 23:59
!
time-range test3
 absolute start 11:10 25 March 2024 end 11:10 25 March 2025
!
time-range test4
 absolute end 11:11 25 March 2026
!
time-range test5
 absolute end 11:12 25 March 2028
 periodic weekend 0:00 to 23:59
```

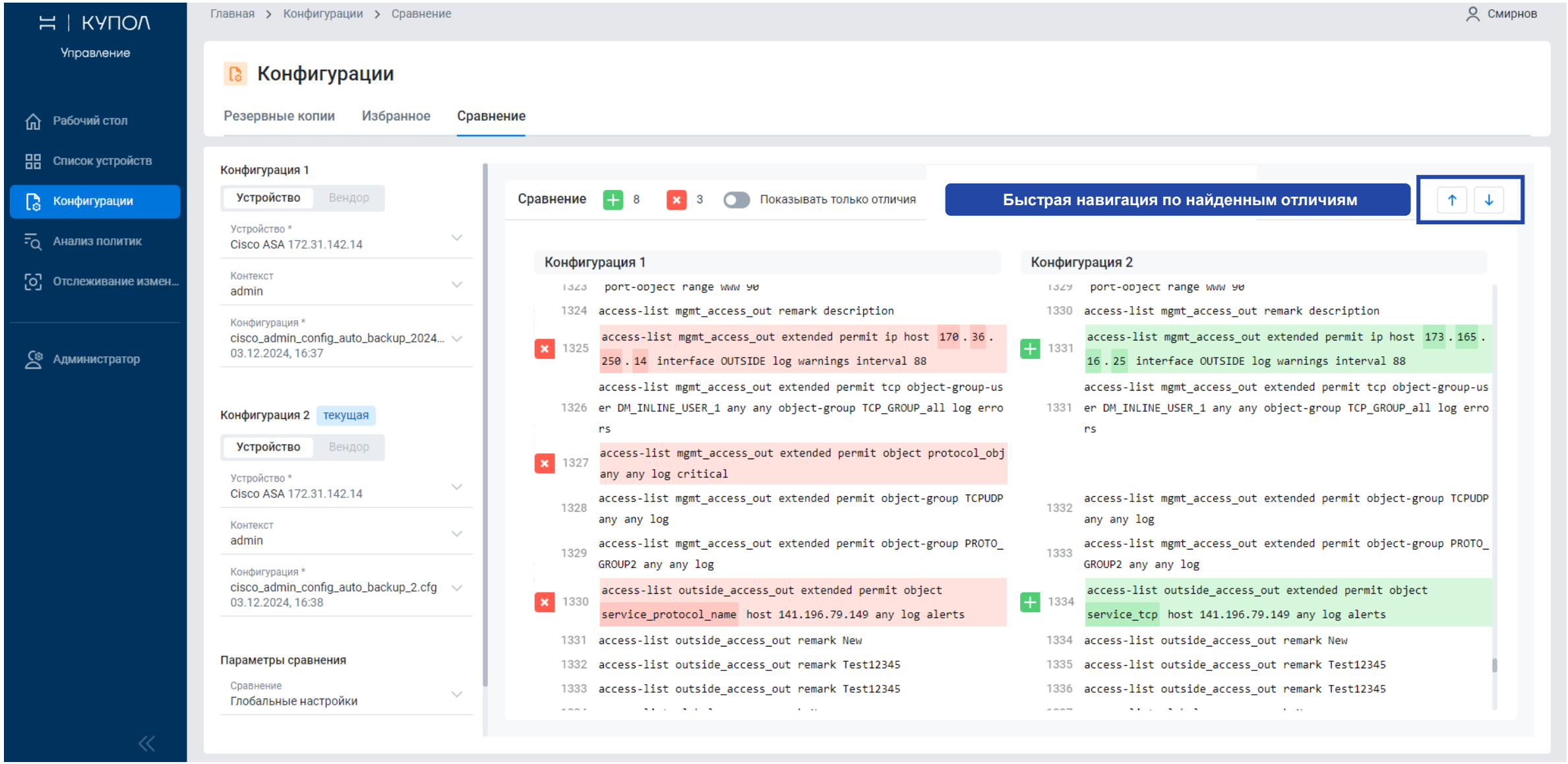
СРАВНЕНИЕ КОНФИГУРАЦИЙ



СРАВНЕНИЕ КОНФИГУРАЦИЙ



СРАВНЕНИЕ КОНФИГУРАЦИЙ



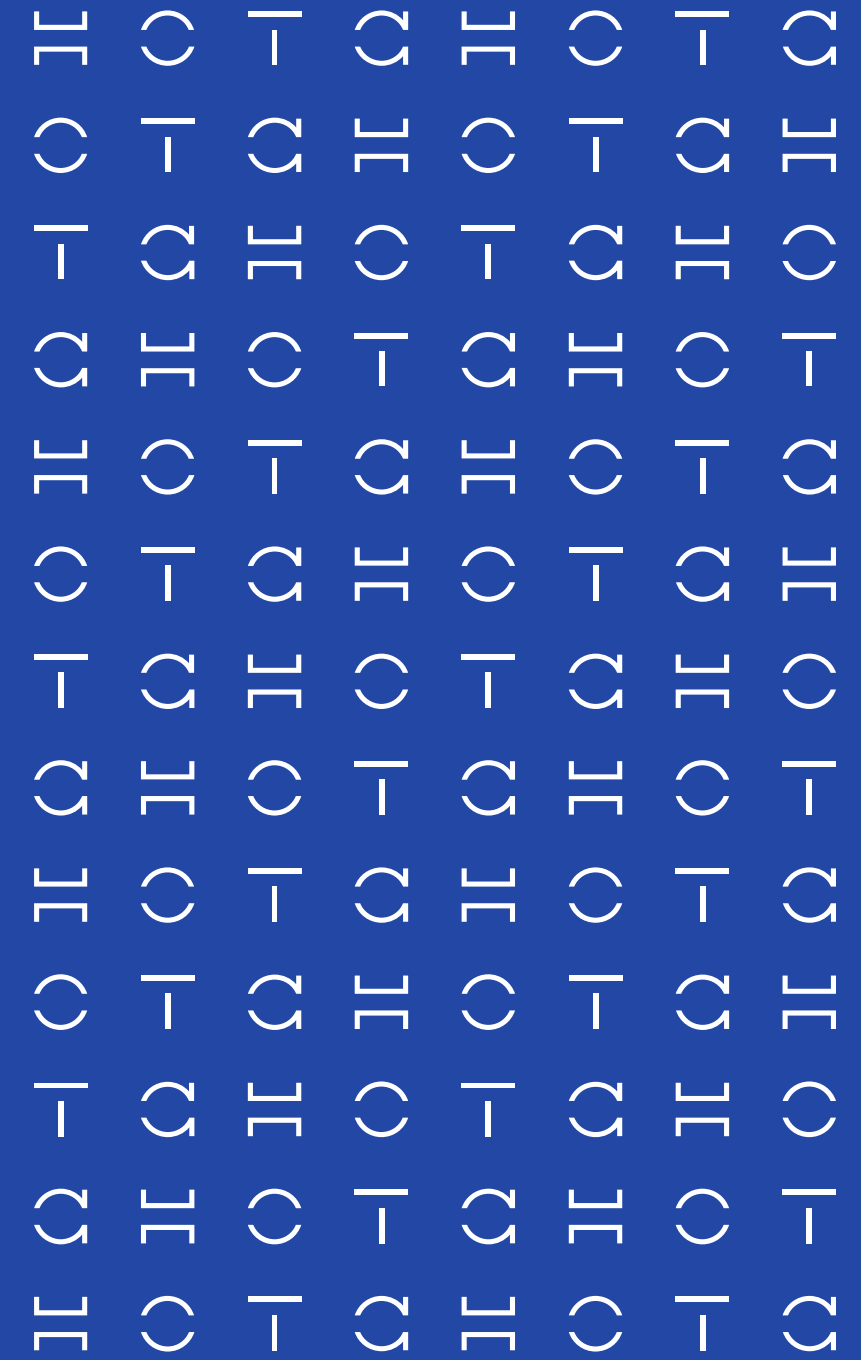
КАРТА СЕТИ

Задачи:

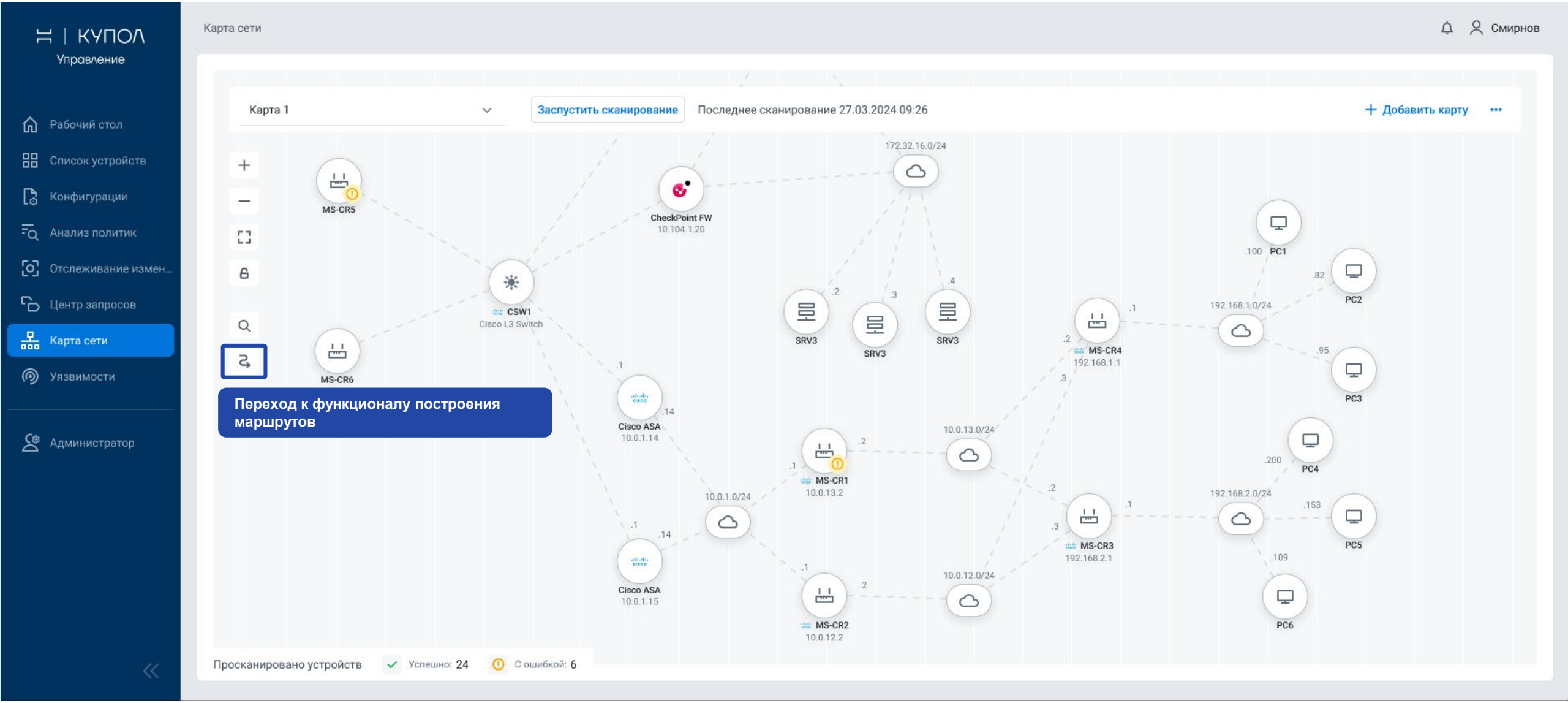
- Проанализировать маршрут прохождения трафика, чтобы понять, доступен ли он или нет, и если нет, то почему.
- Провести анализ векторов атак — определить, компенсируют ли политики ИБ наличие известных уязвимостей.

Кейс 1: «дебаг» политик, когда пользователь потерял доступ к ресурсу.

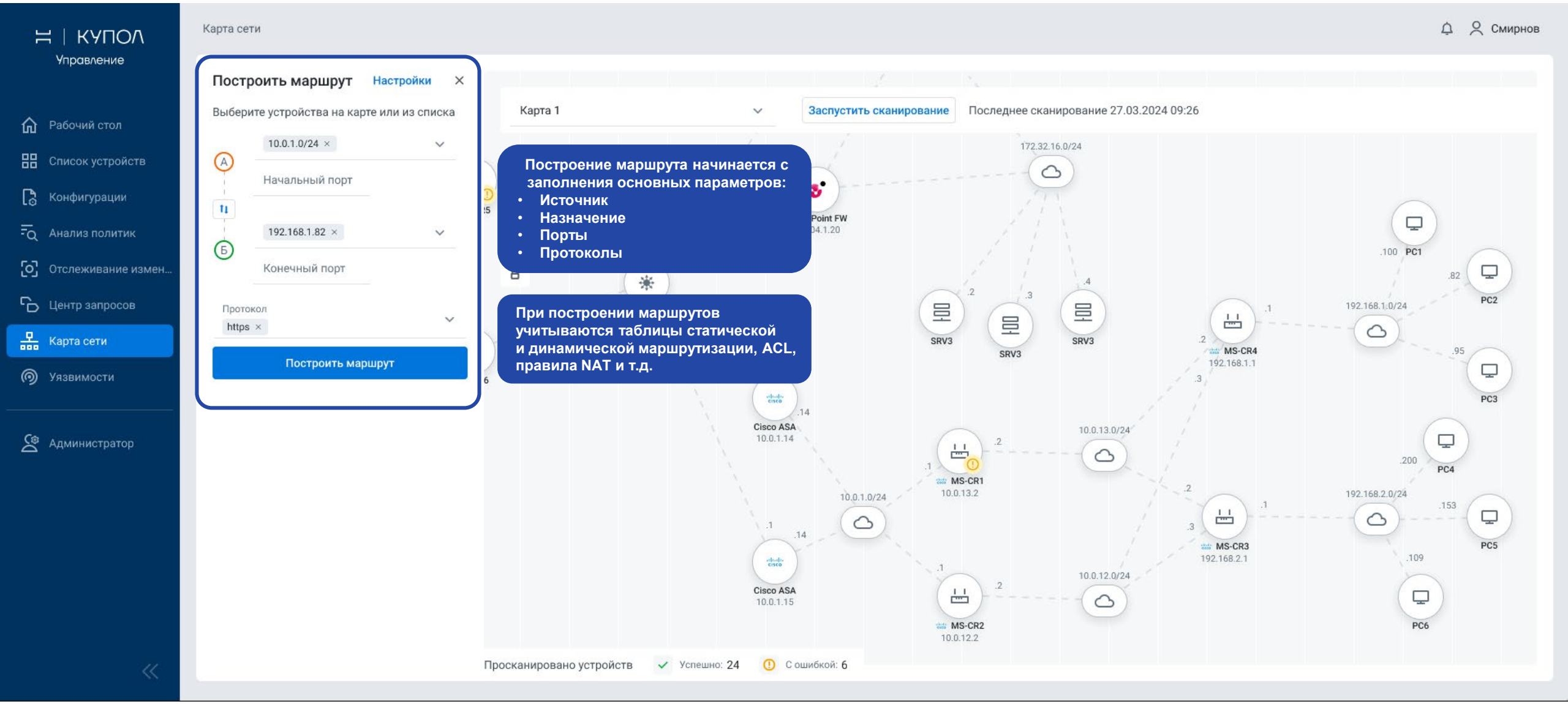
Кейс 2: анализ возможности доступа к уязвимому ресурсу.



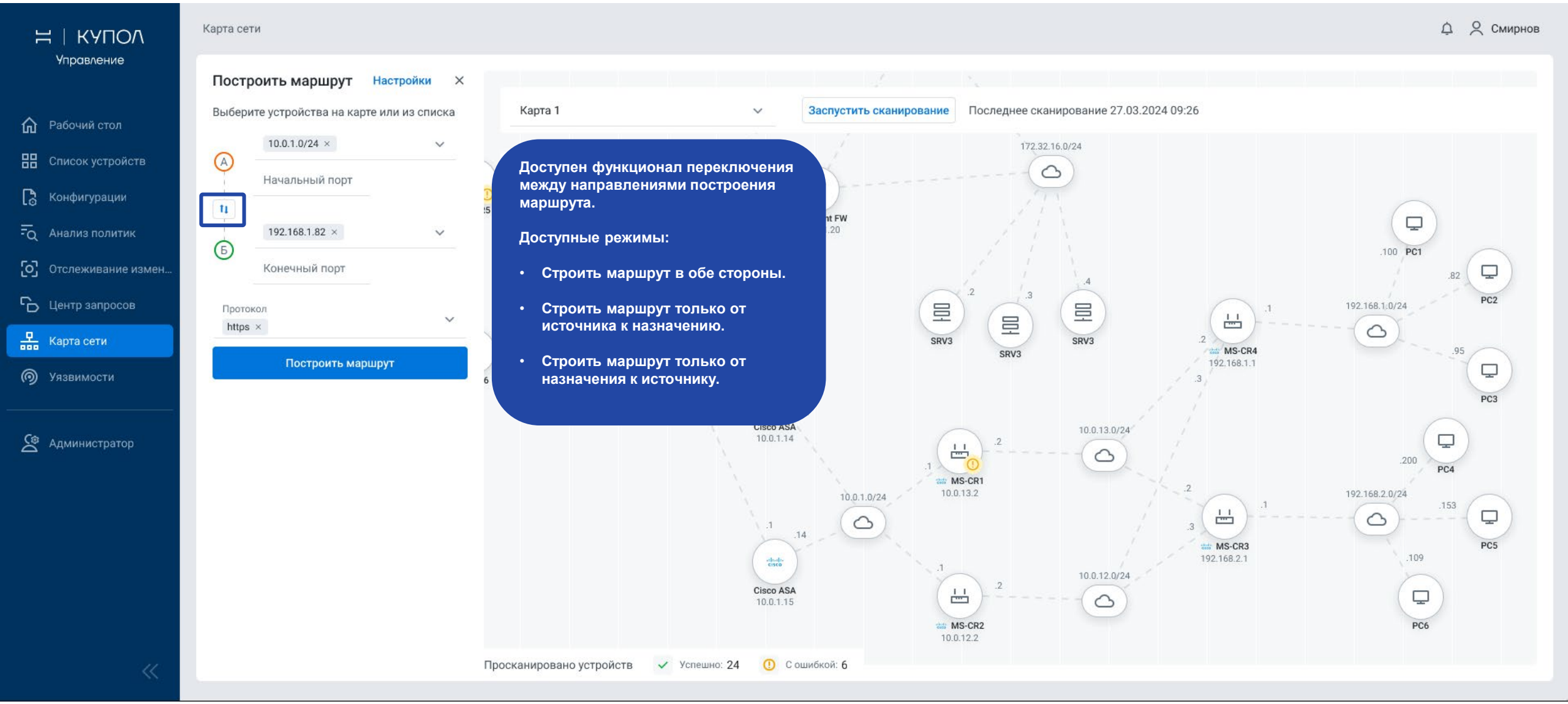
КАРТА СЕТИ — ПОСТРОЕНИЕ МАРШРУТОВ



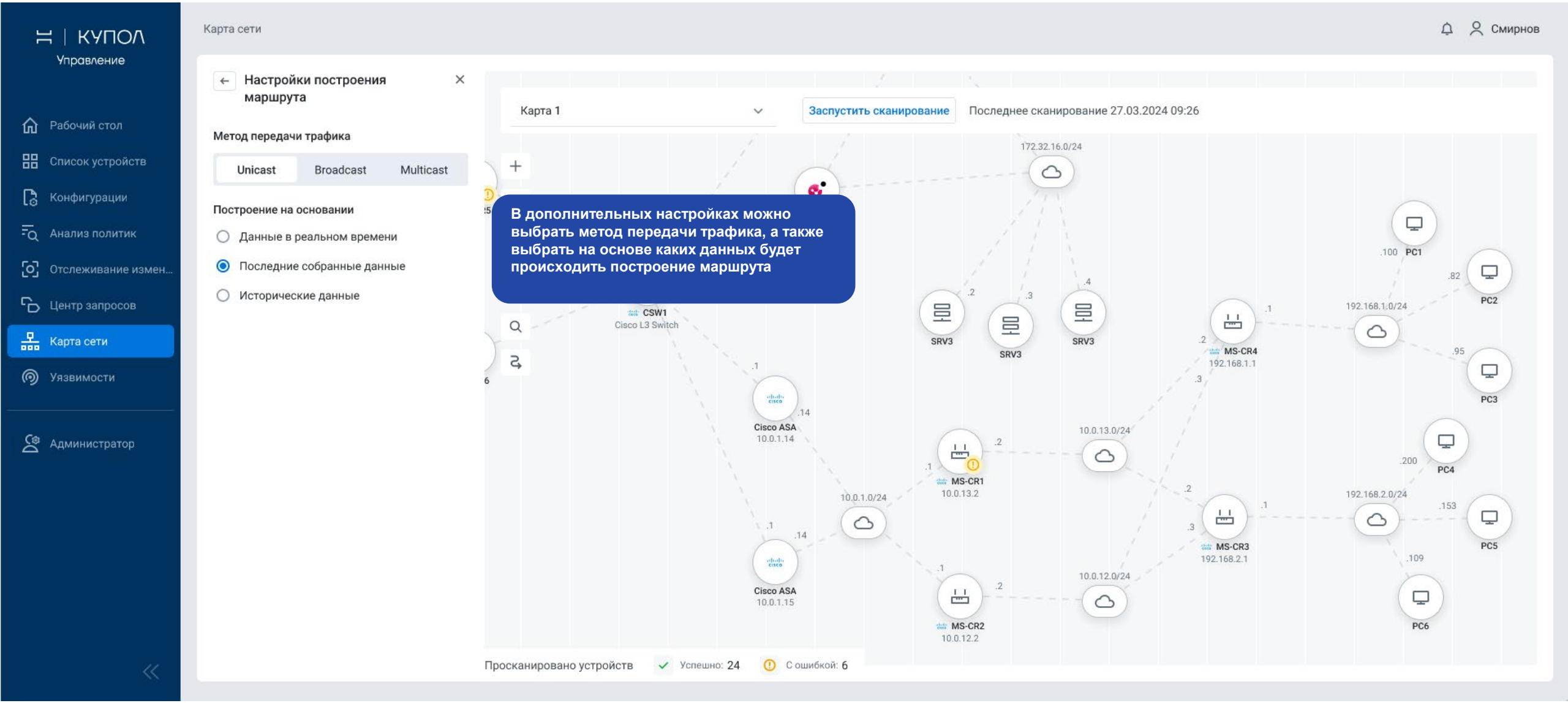
КАРТА СЕТИ — СОЗДАНИЕ МАРШРУТА



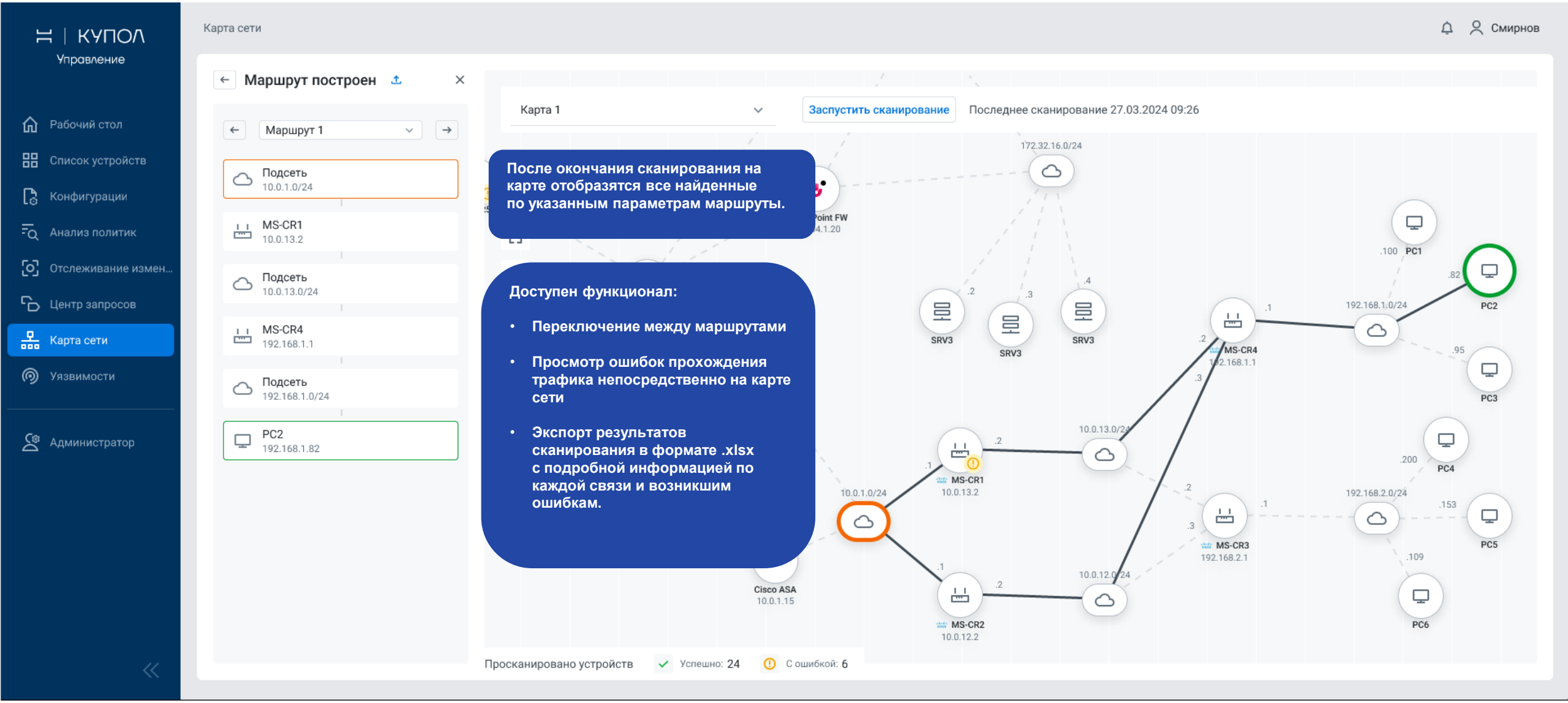
КАРТА СЕТИ — СОЗДАНИЕ МАРШРУТА



КАРТА СЕТИ — НАСТРОЙКИ МАРШРУТА



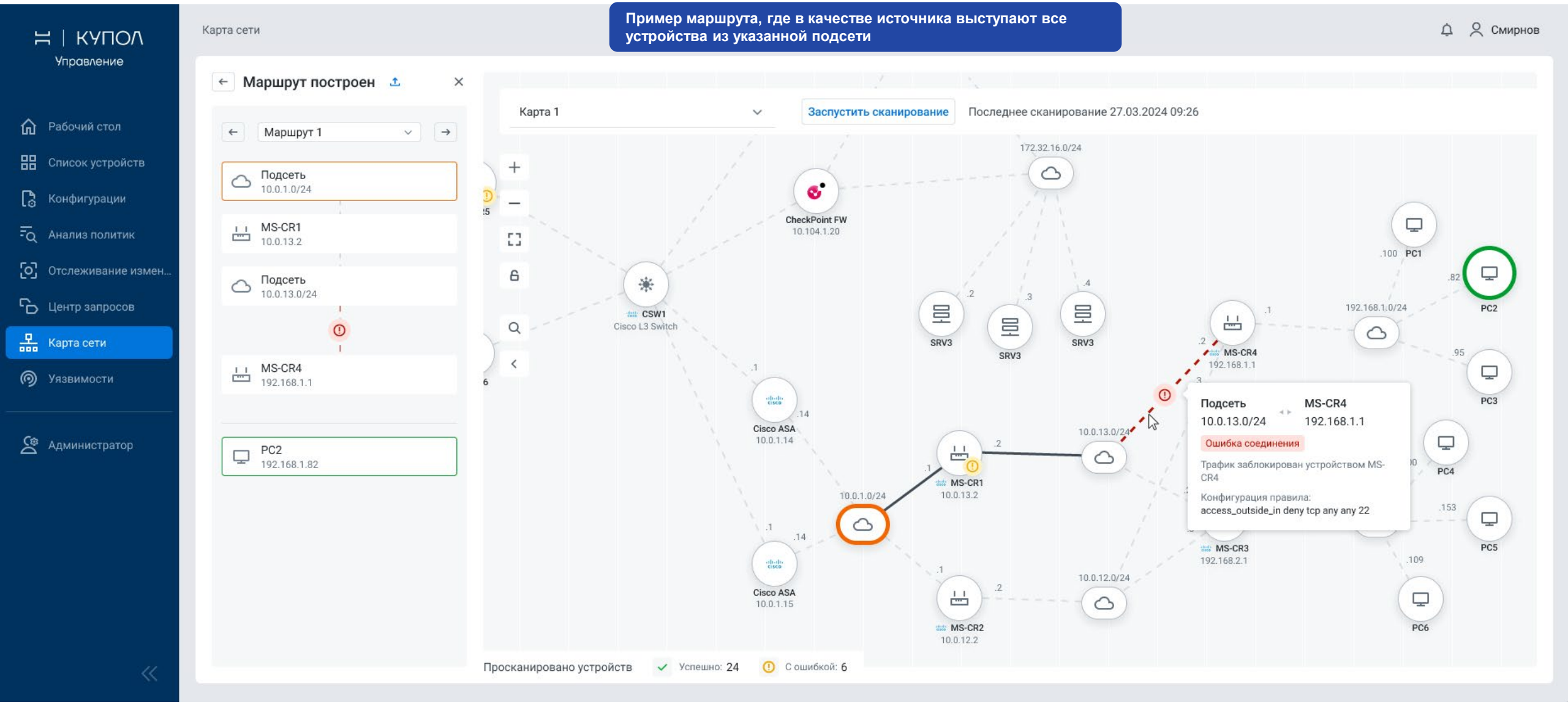
КАРТА СЕТИ — ПРОСМОТР МАРШРУТОВ



КАРТА СЕТИ — ПРОСМОТР МАРШРУТОВ

НСТС | КУПОЛ

Пример маршрута, где в качестве источника выступают все устройства из указанной подсети

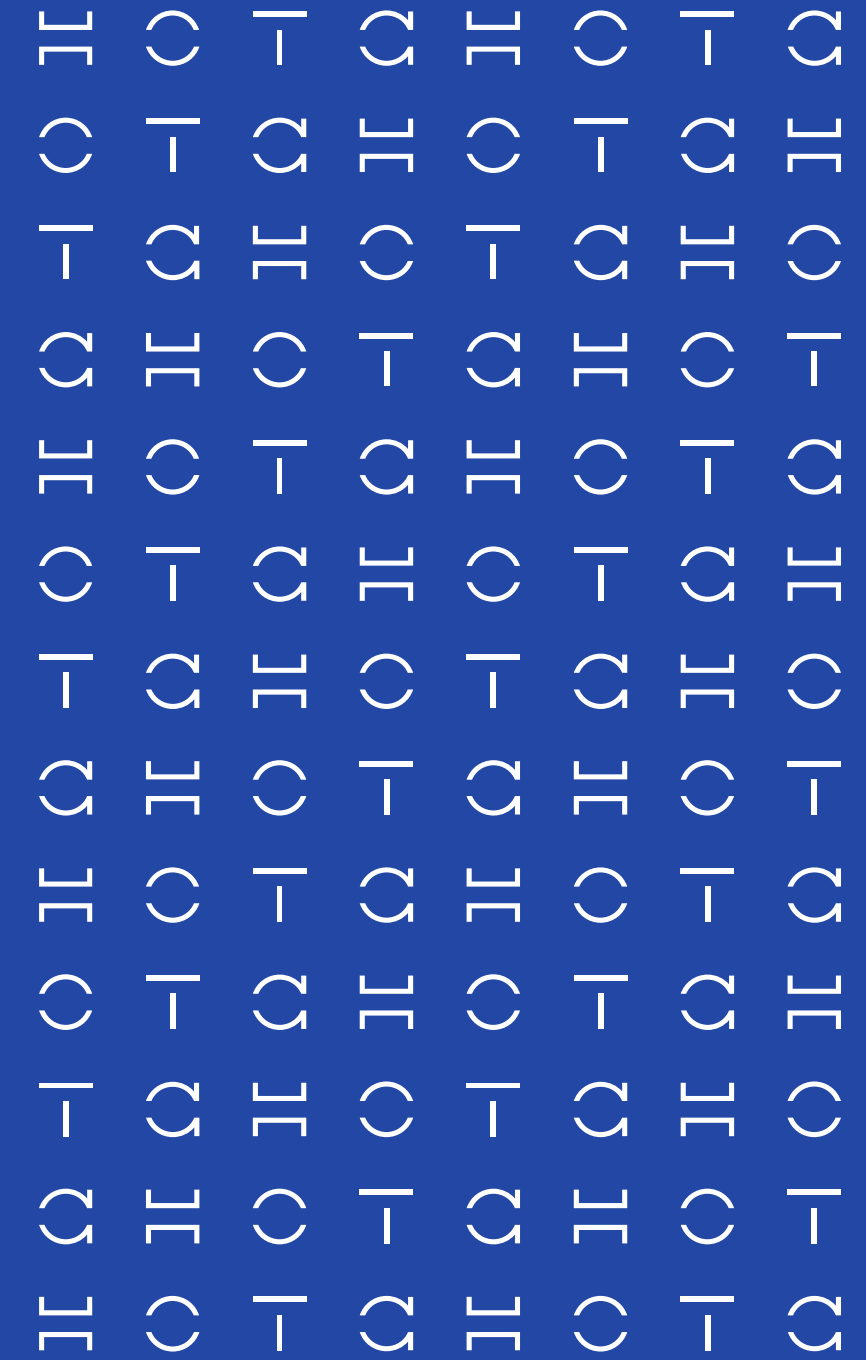


ЦЕНТР ЗАПРОСОВ

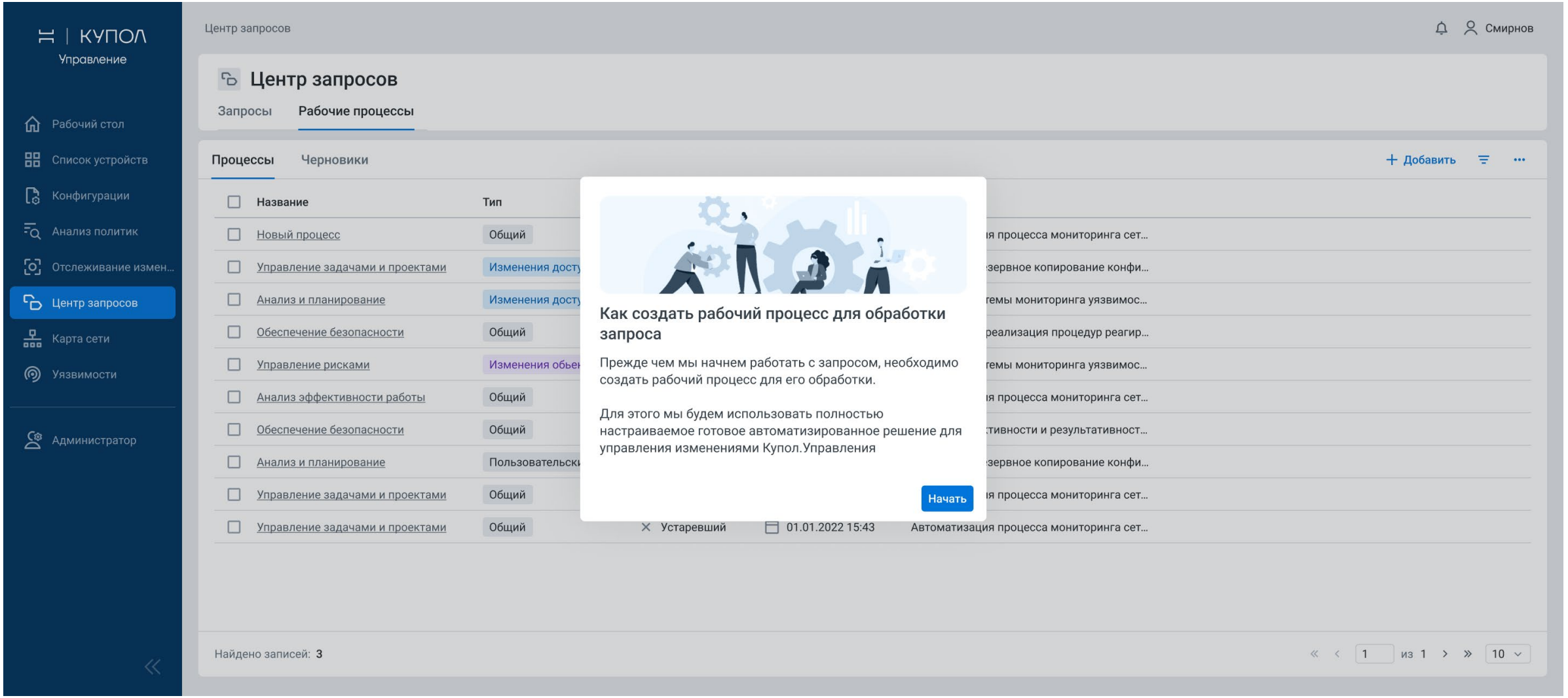
Предположим, что каждая задача отлично работает сама по себе, но теперь нужно связать несколько сотрудников между собой.

Задача: автоматизация рассмотрения заявок на доступы,а именно:

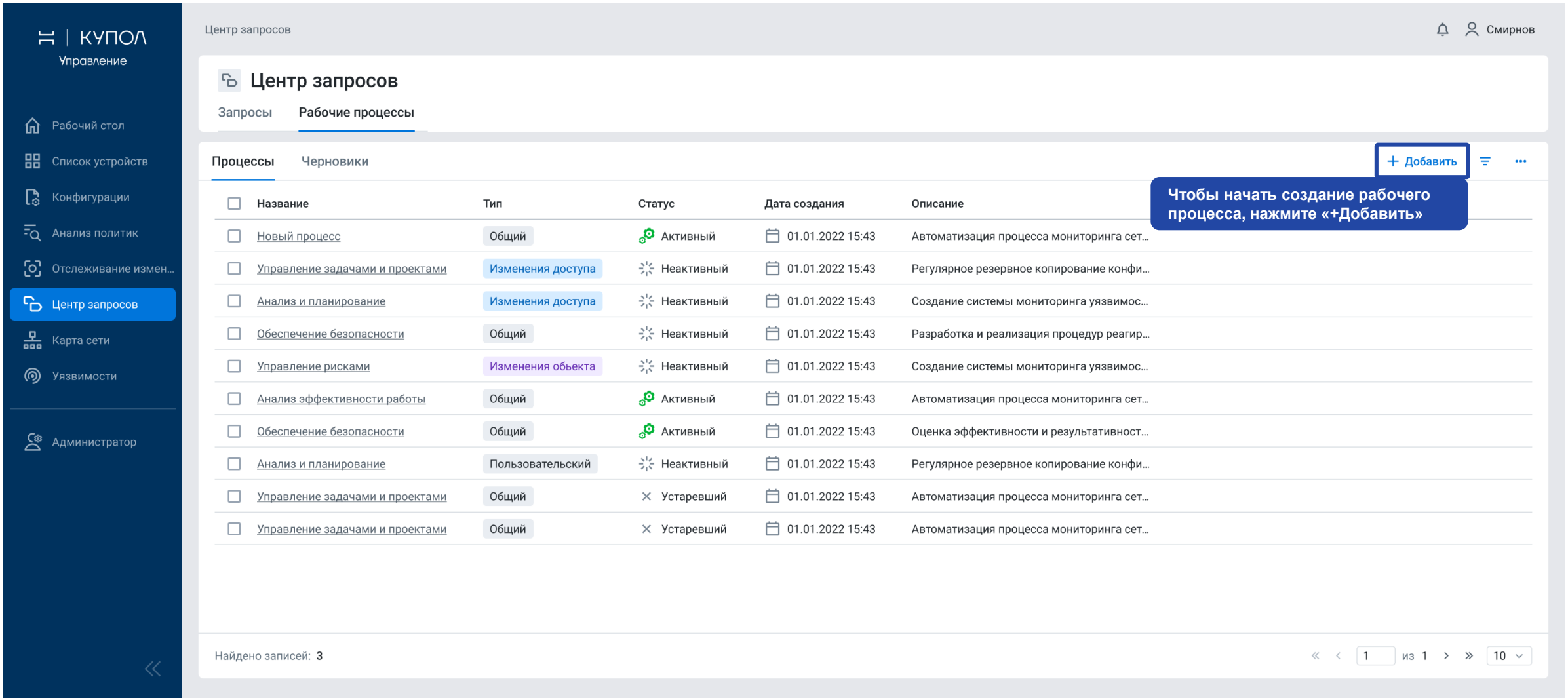
- анализ поступивших заявок на соответствие политикам
- ускорение процесса предоставления доступа (система рекомендует правило, автоматизация применения изменений)
- контроль возможных ошибок до применения политик на устройствах
- унификация процесса и согласование.



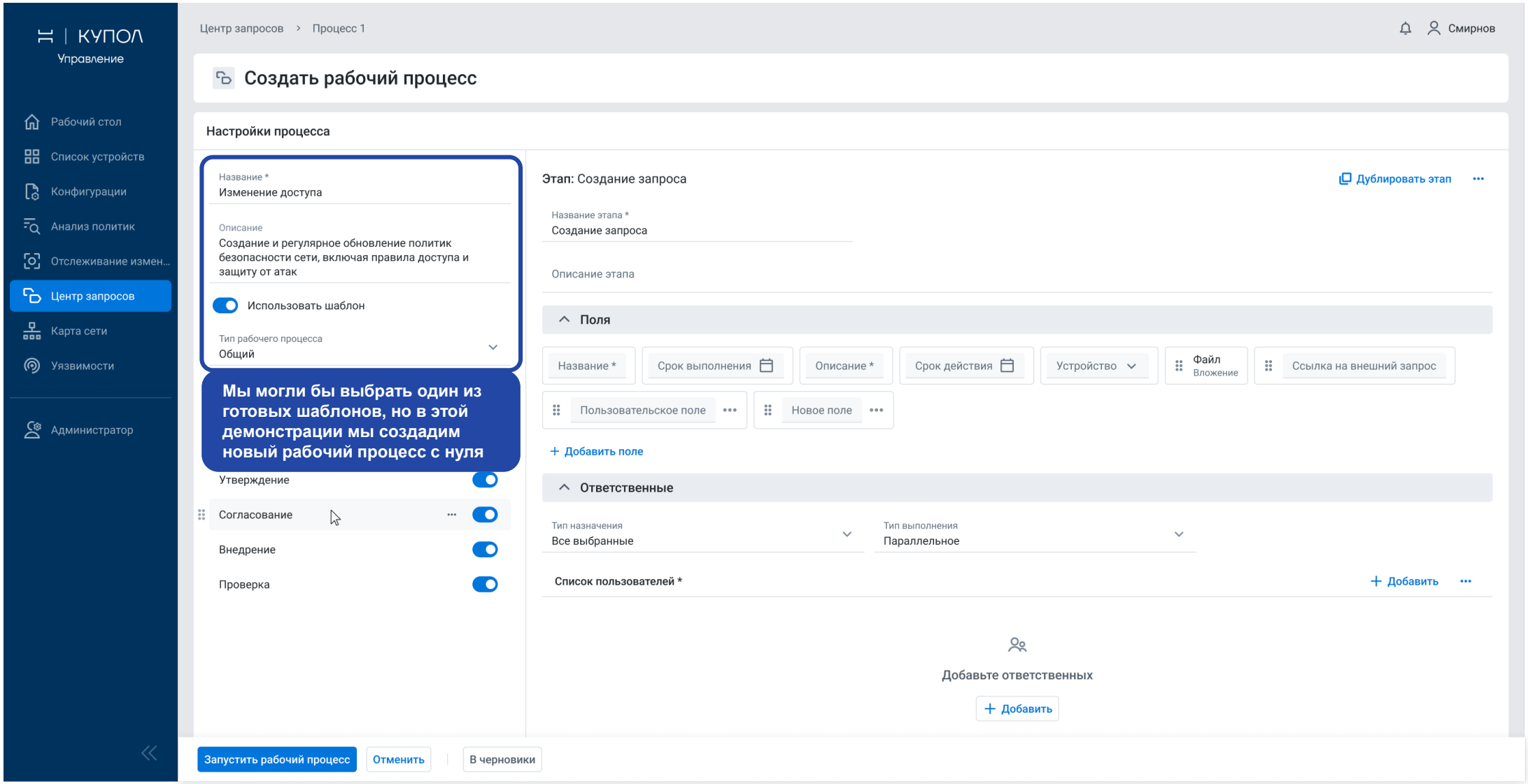
ЦЕНТР ЗАПРОСОВ — РАБОЧИЕ ПРОЦЕССЫ



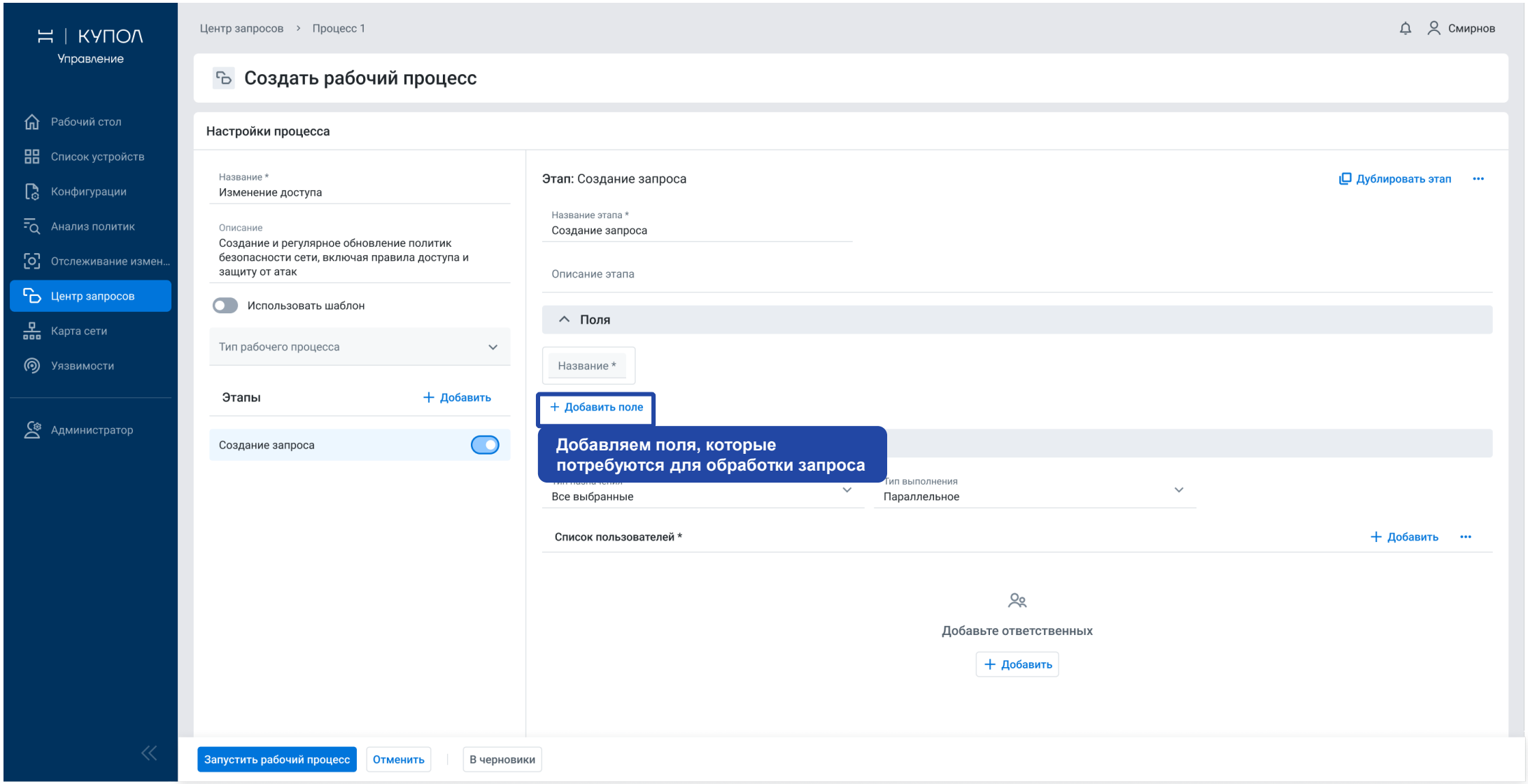
ЦЕНТР ЗАПРОСОВ — РАБОЧИЕ ПРОЦЕССЫ



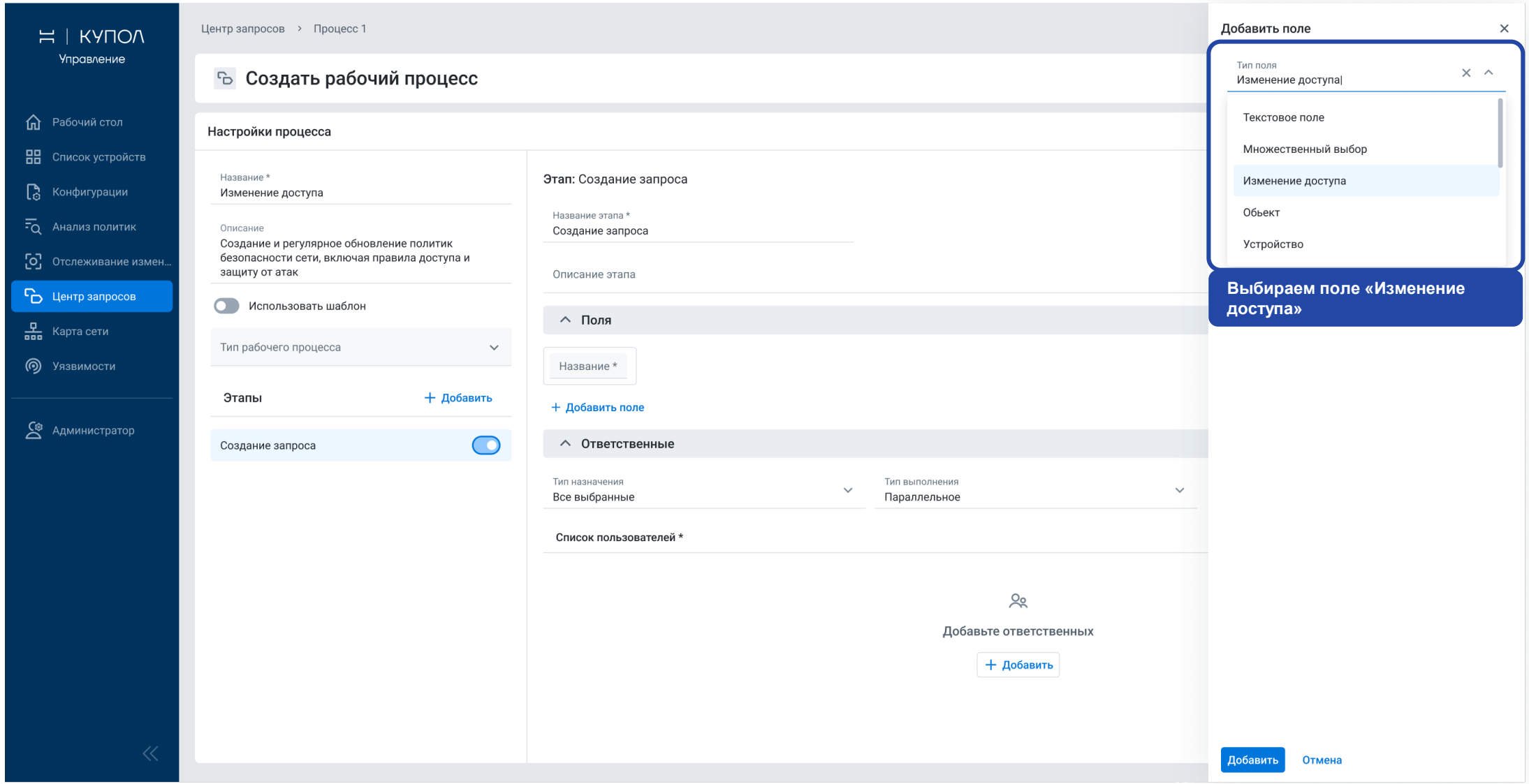
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ



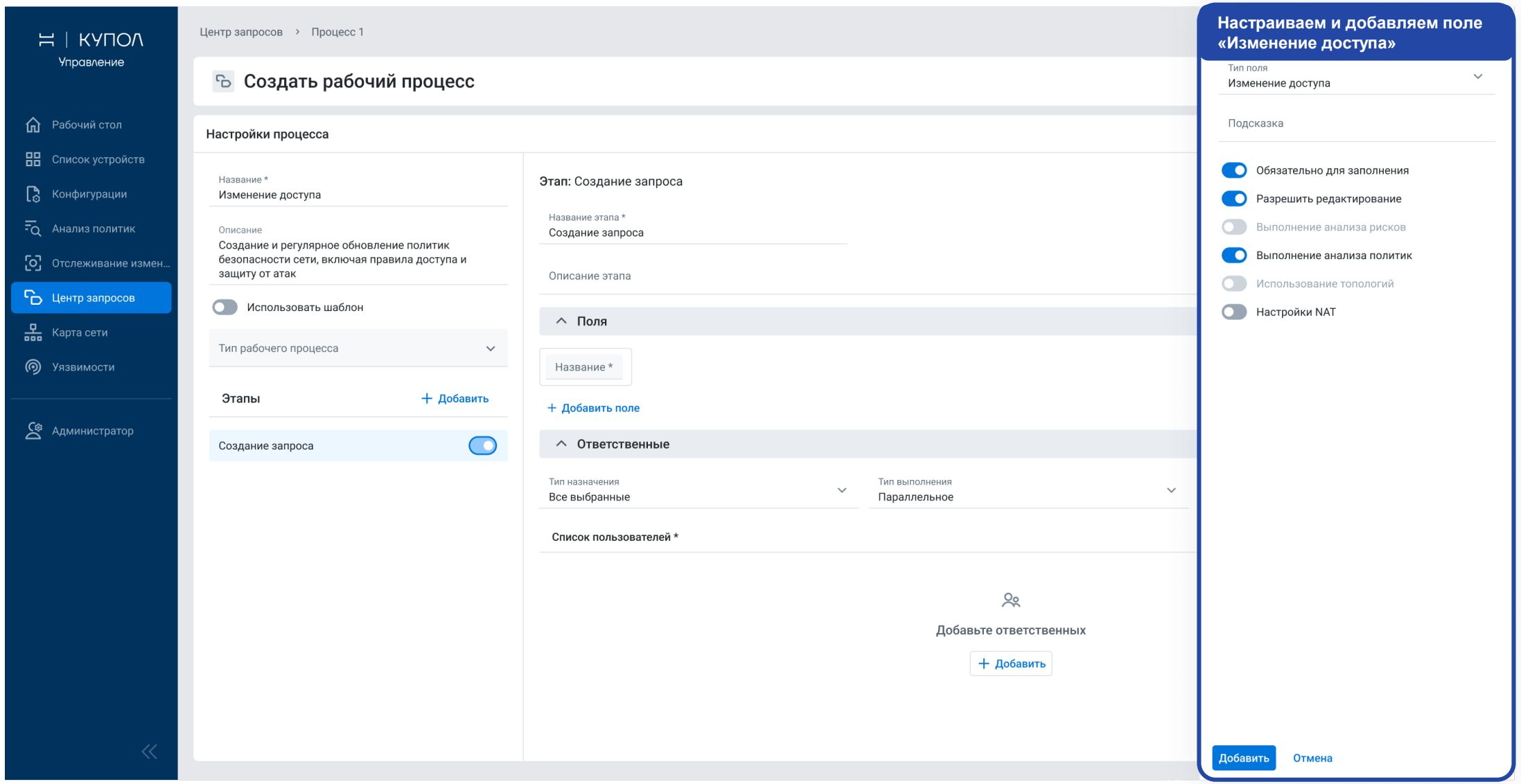
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ



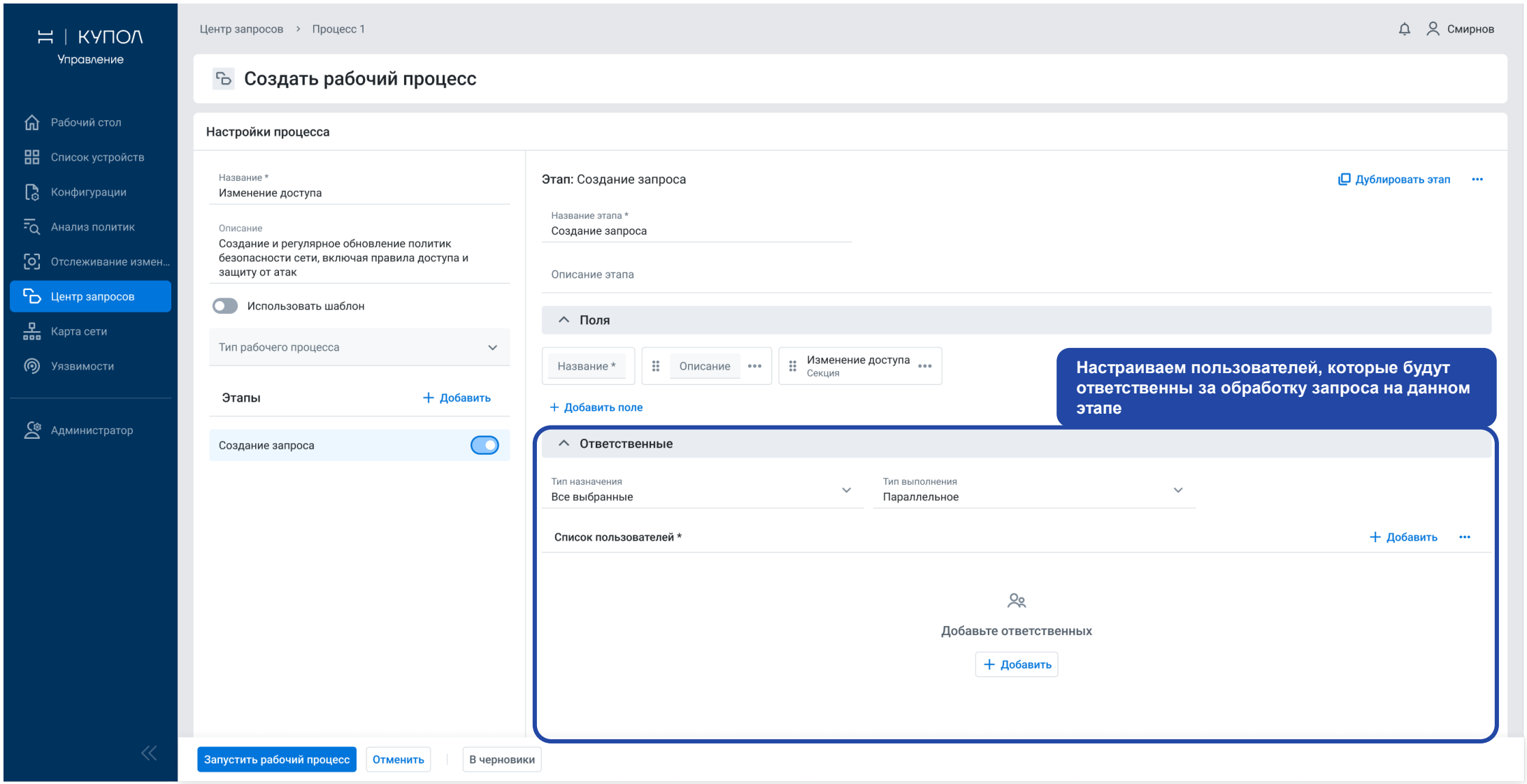
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ



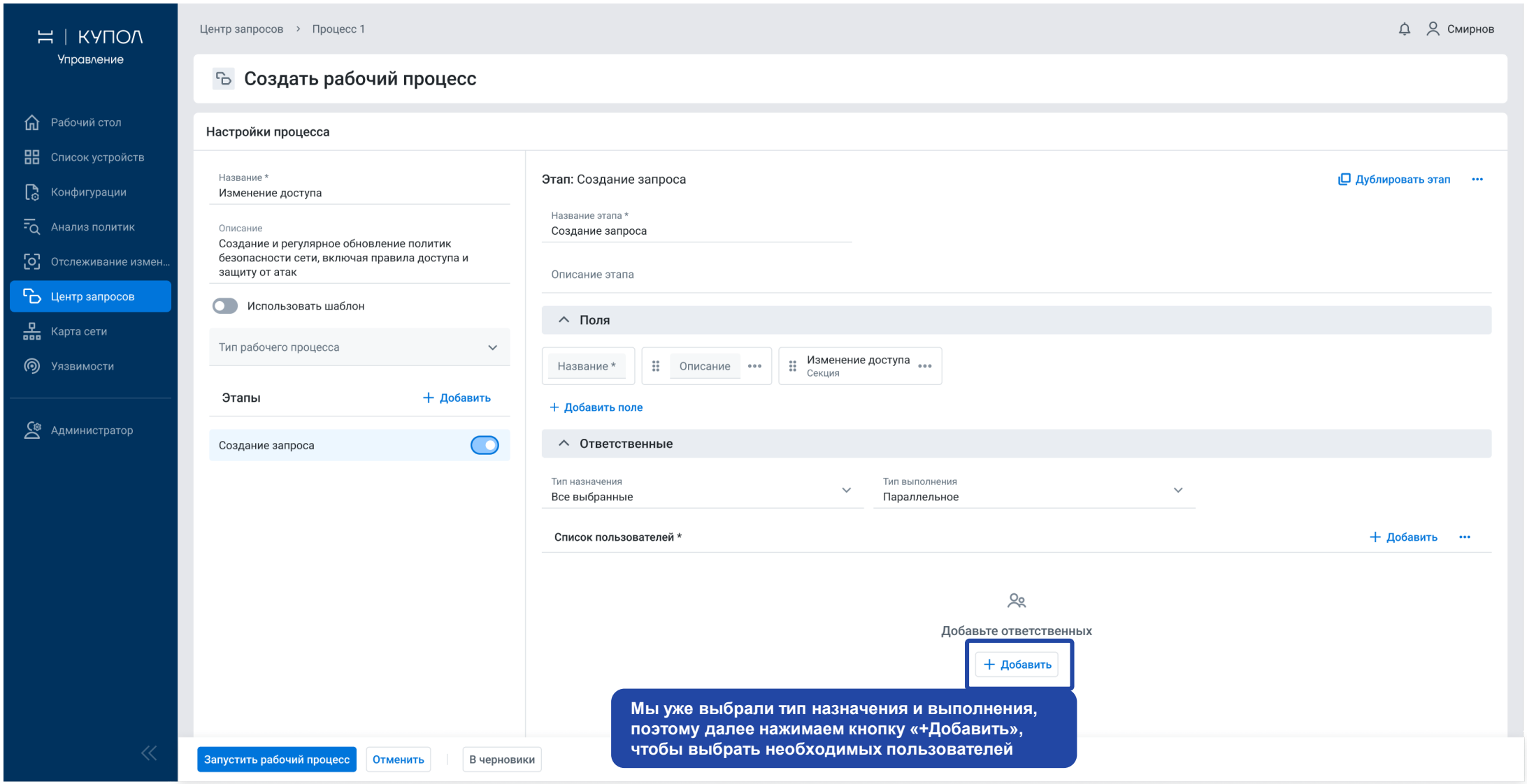
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ



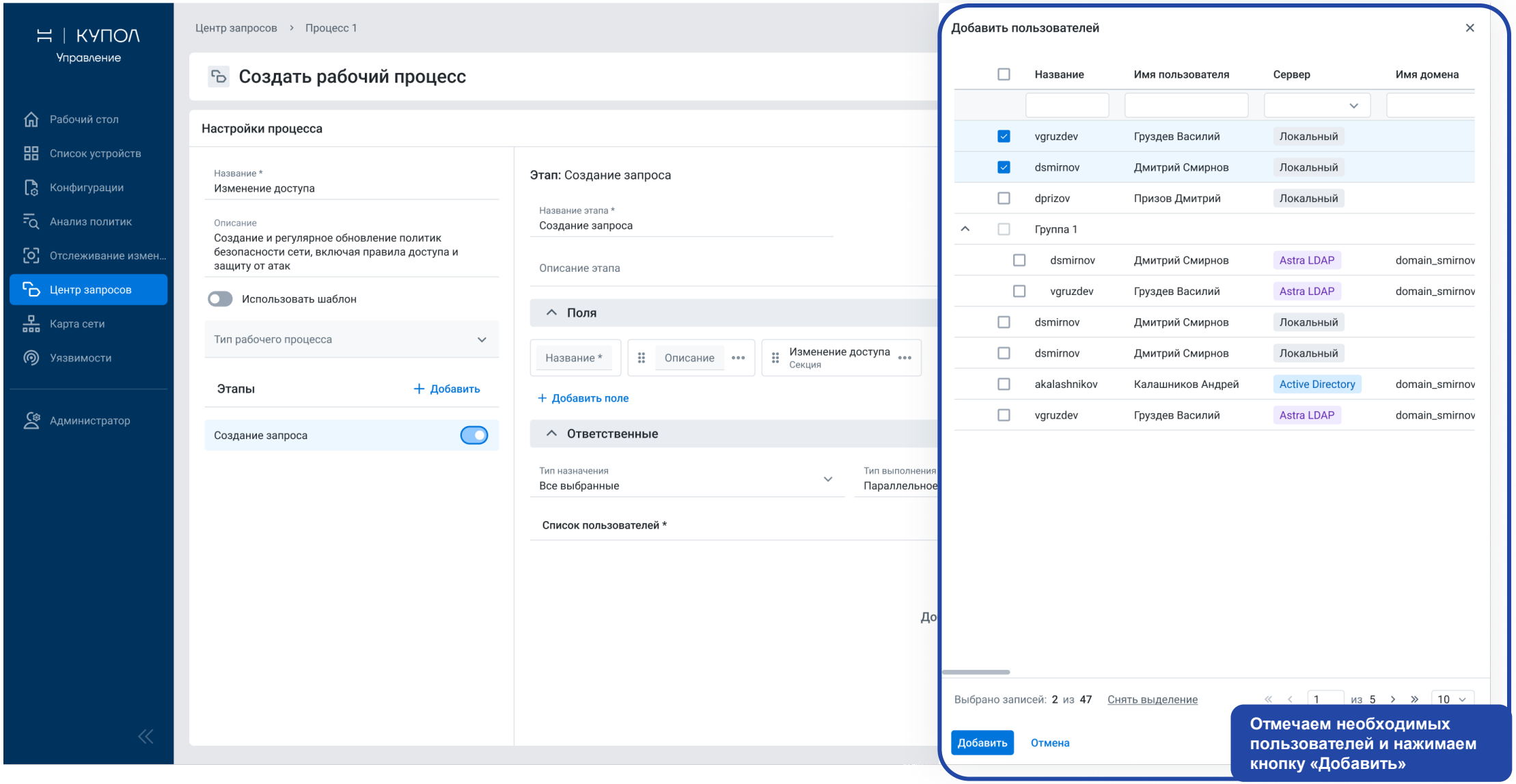
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ



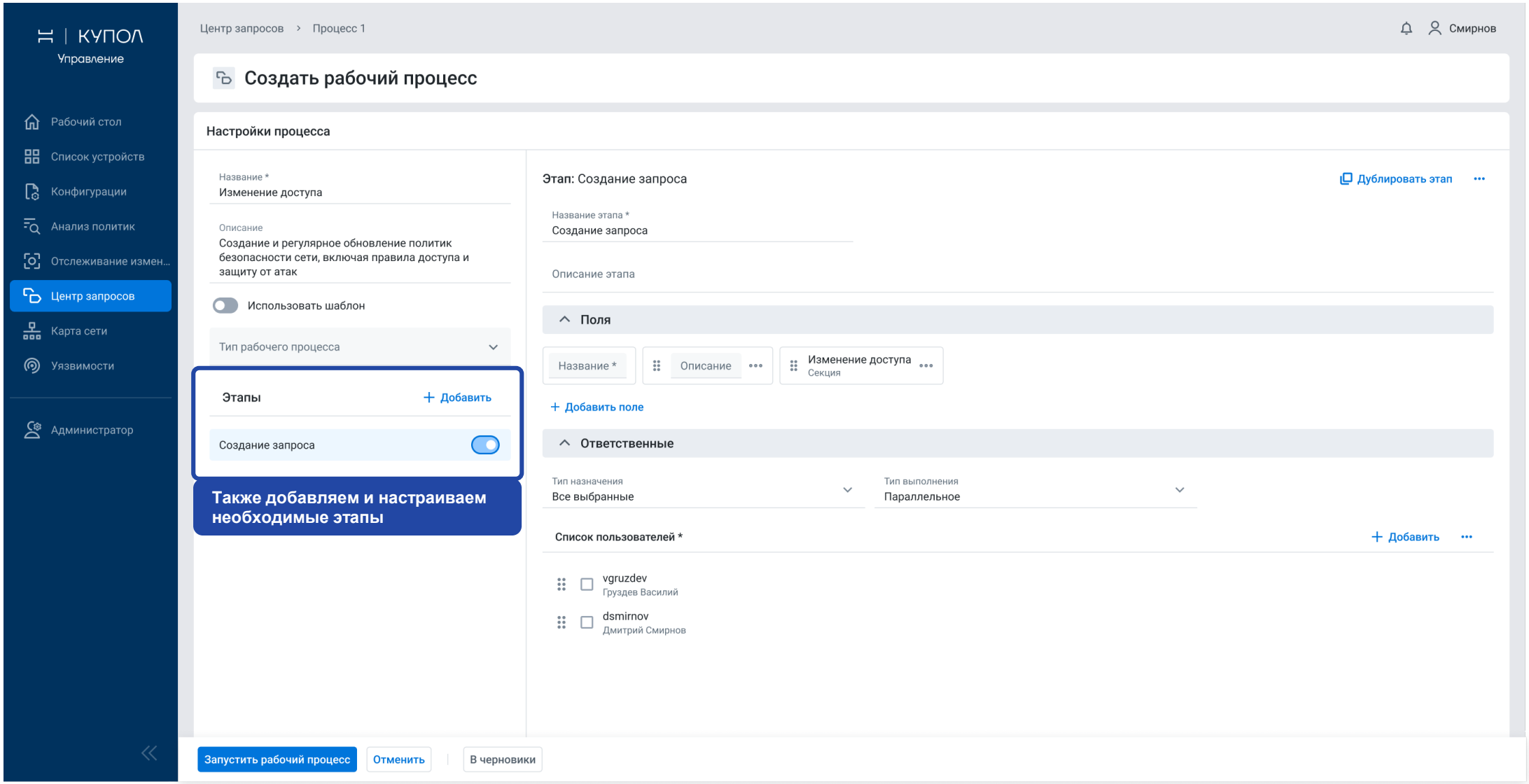
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ



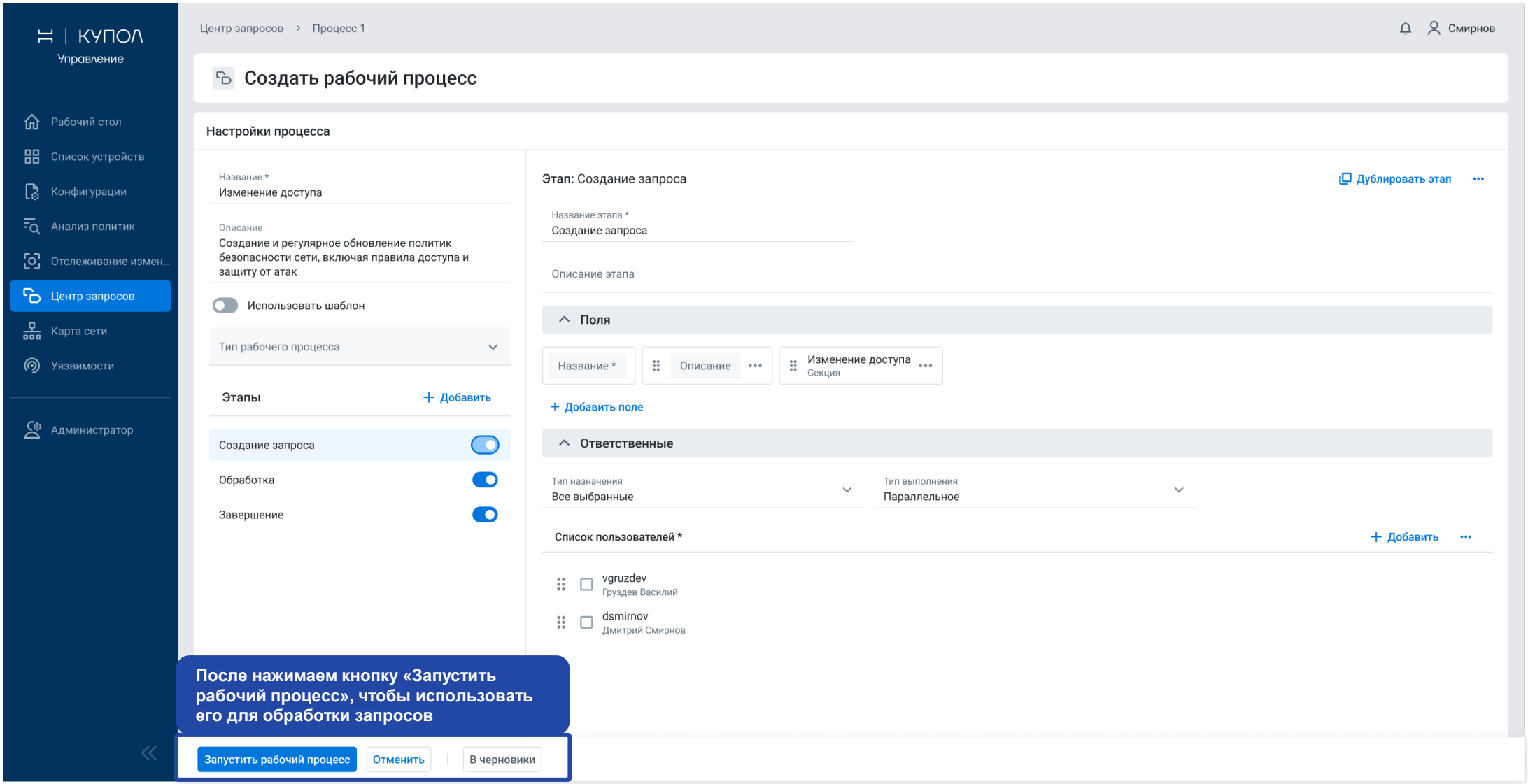
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ



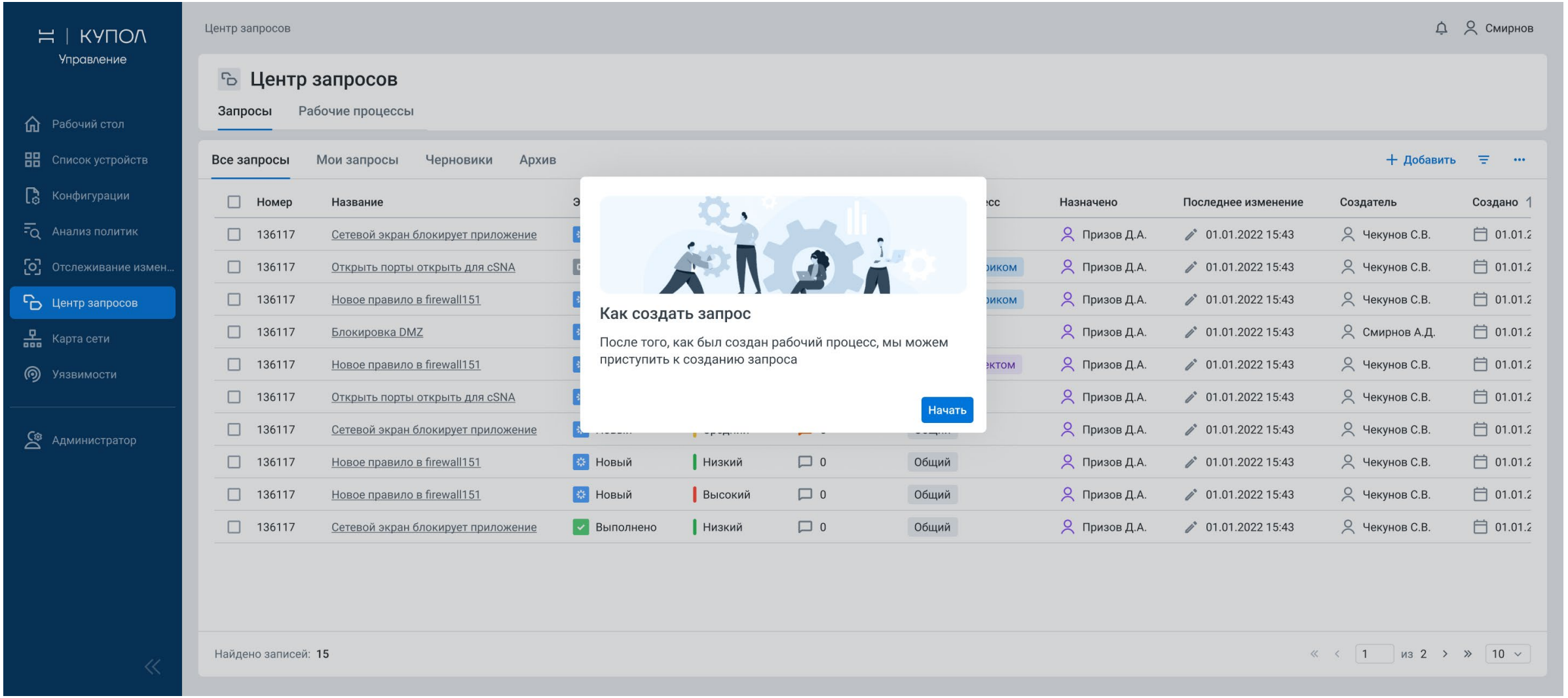
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ



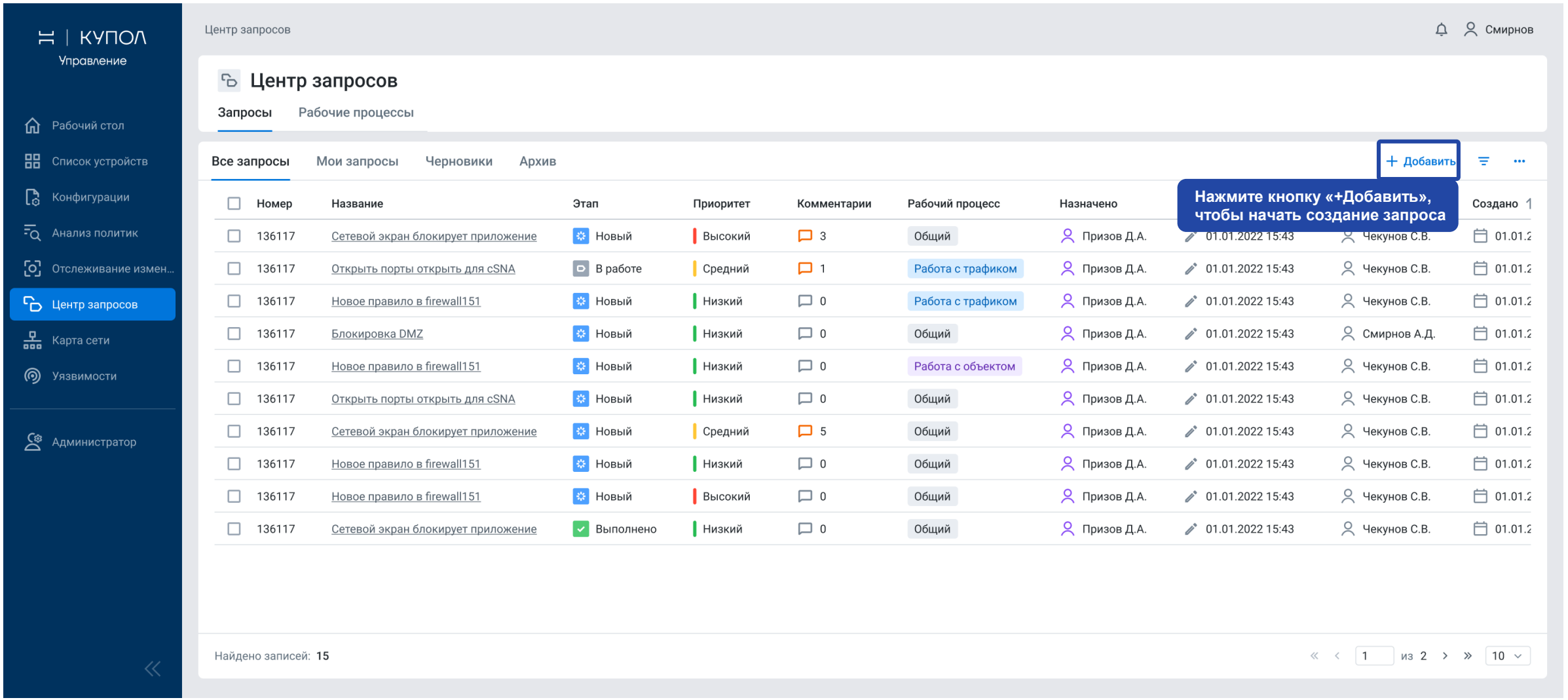
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ РАБОЧИХ ПРОЦЕССОВ



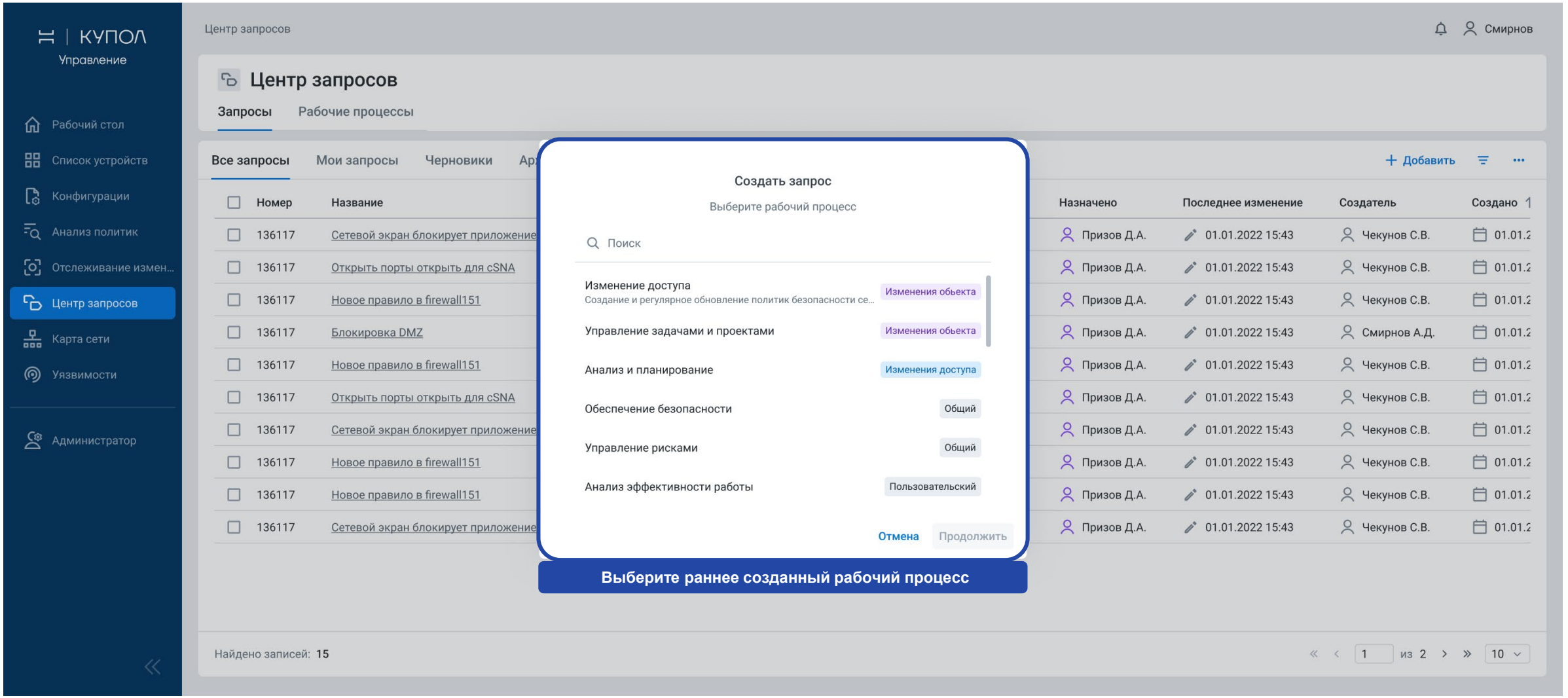
ЦЕНТР ЗАПРОСОВ — ЗАПРОСЫ



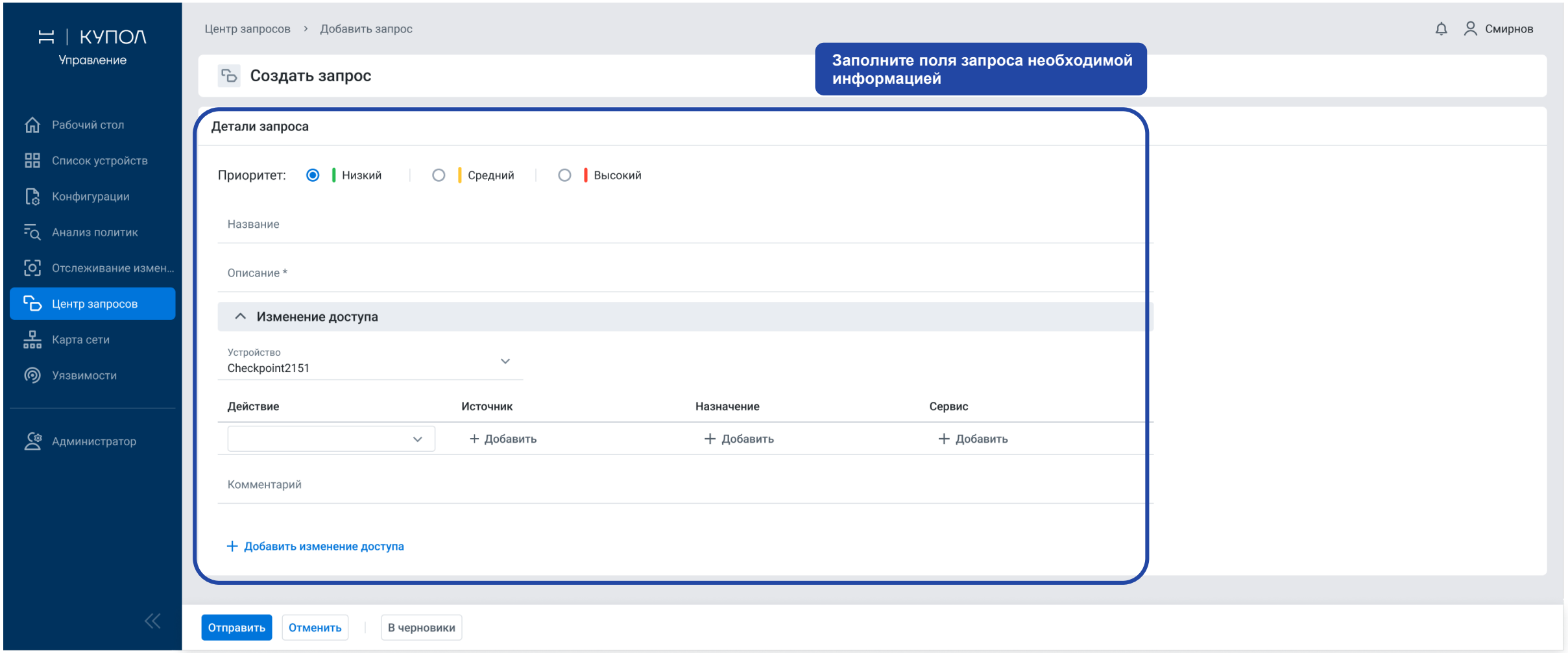
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ ЗАПРОСОВ



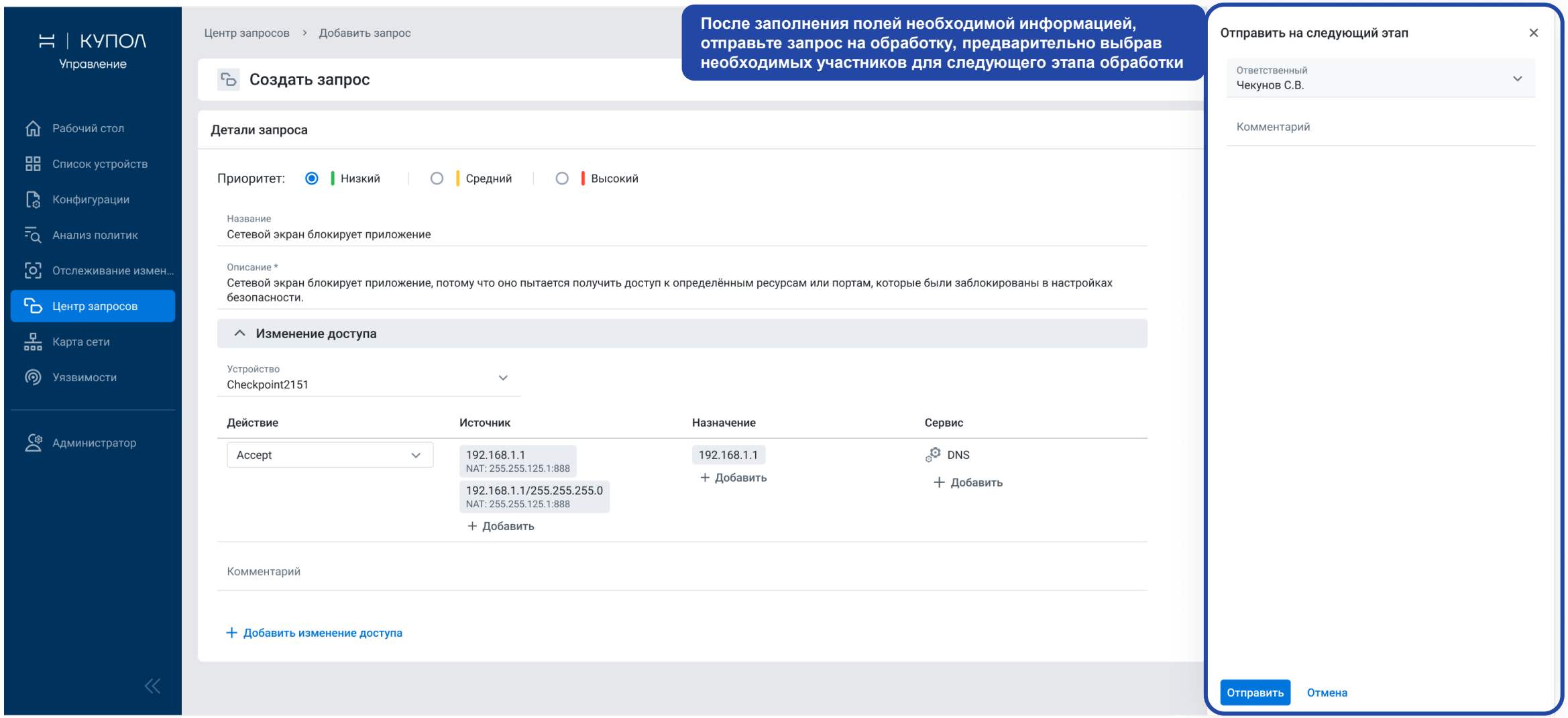
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ ЗАПРОСОВ



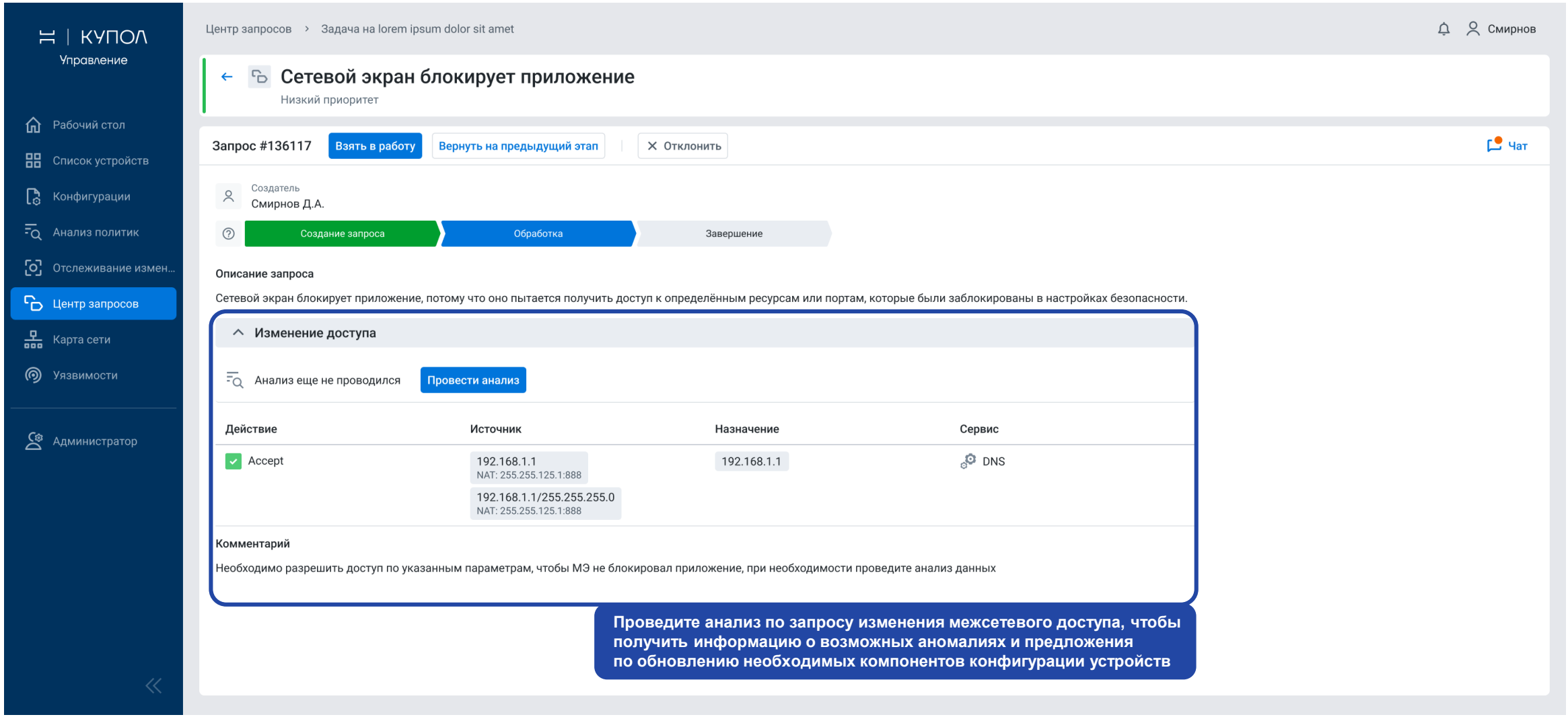
ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ ЗАПРОСОВ



ЦЕНТР ЗАПРОСОВ — СОЗДАНИЕ ЗАПРОСОВ

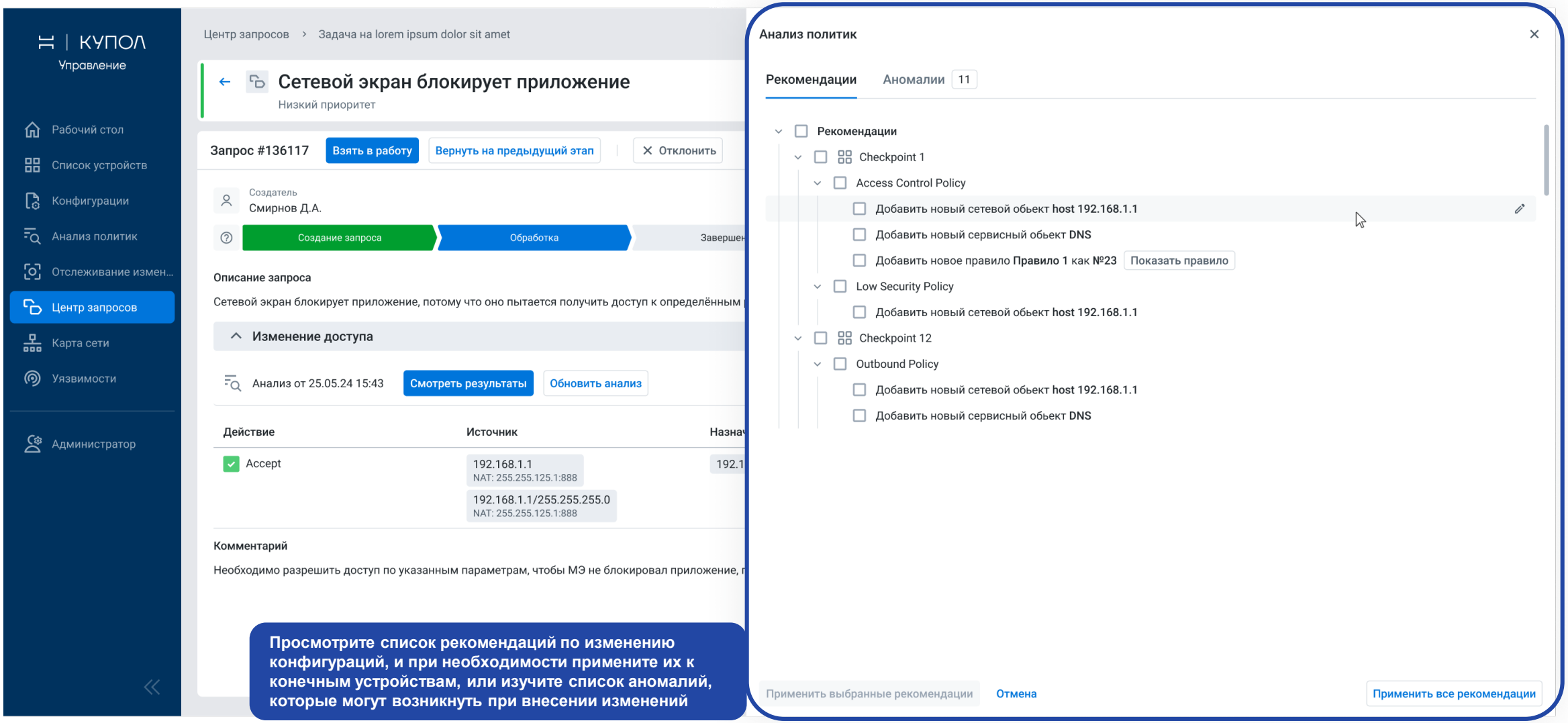


ЦЕНТР ЗАПРОСОВ — ОБРАБОТКА ЗАПРОСОВ



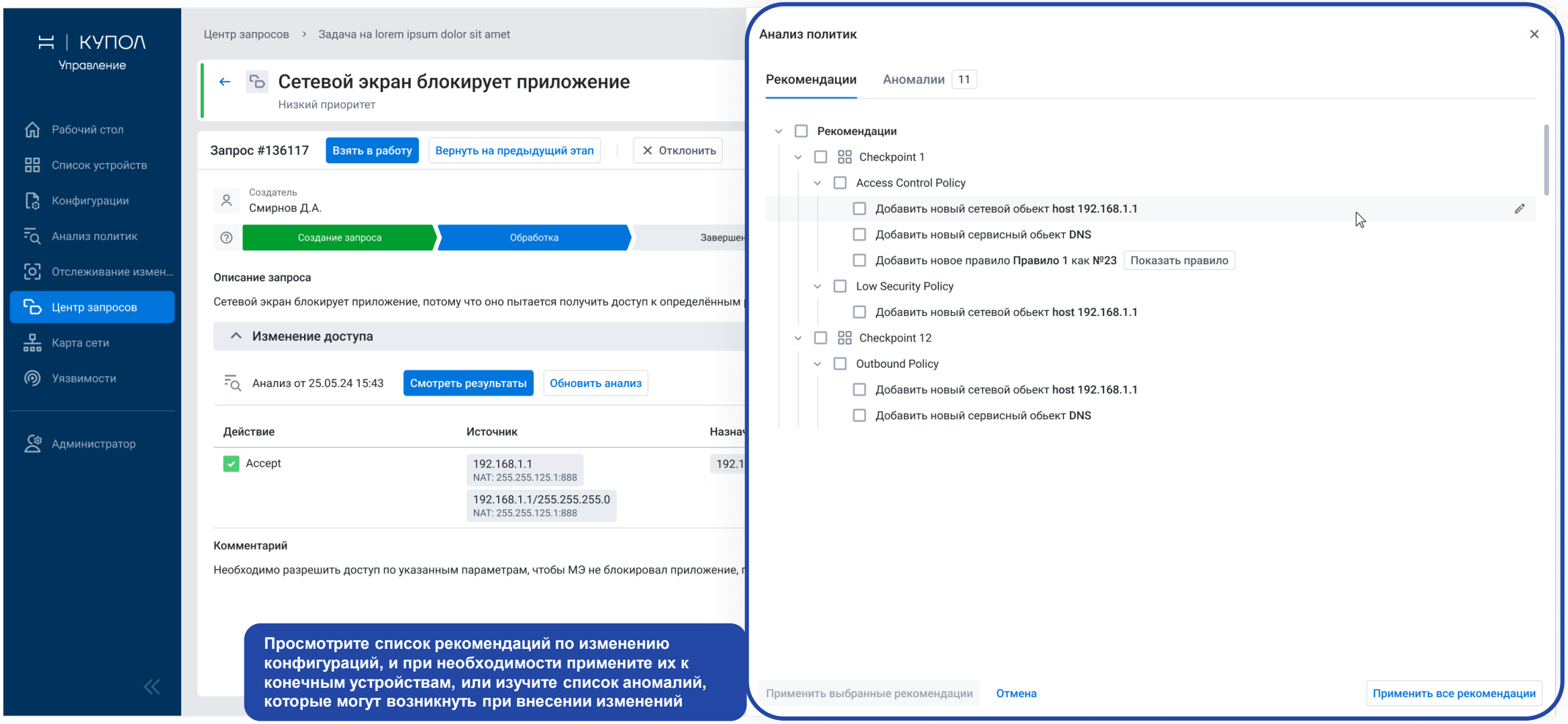
ЦЕНТР ЗАПРОСОВ — ОБРАБОТКА ЗАПРОСОВ

НСТС | КУПОЛ



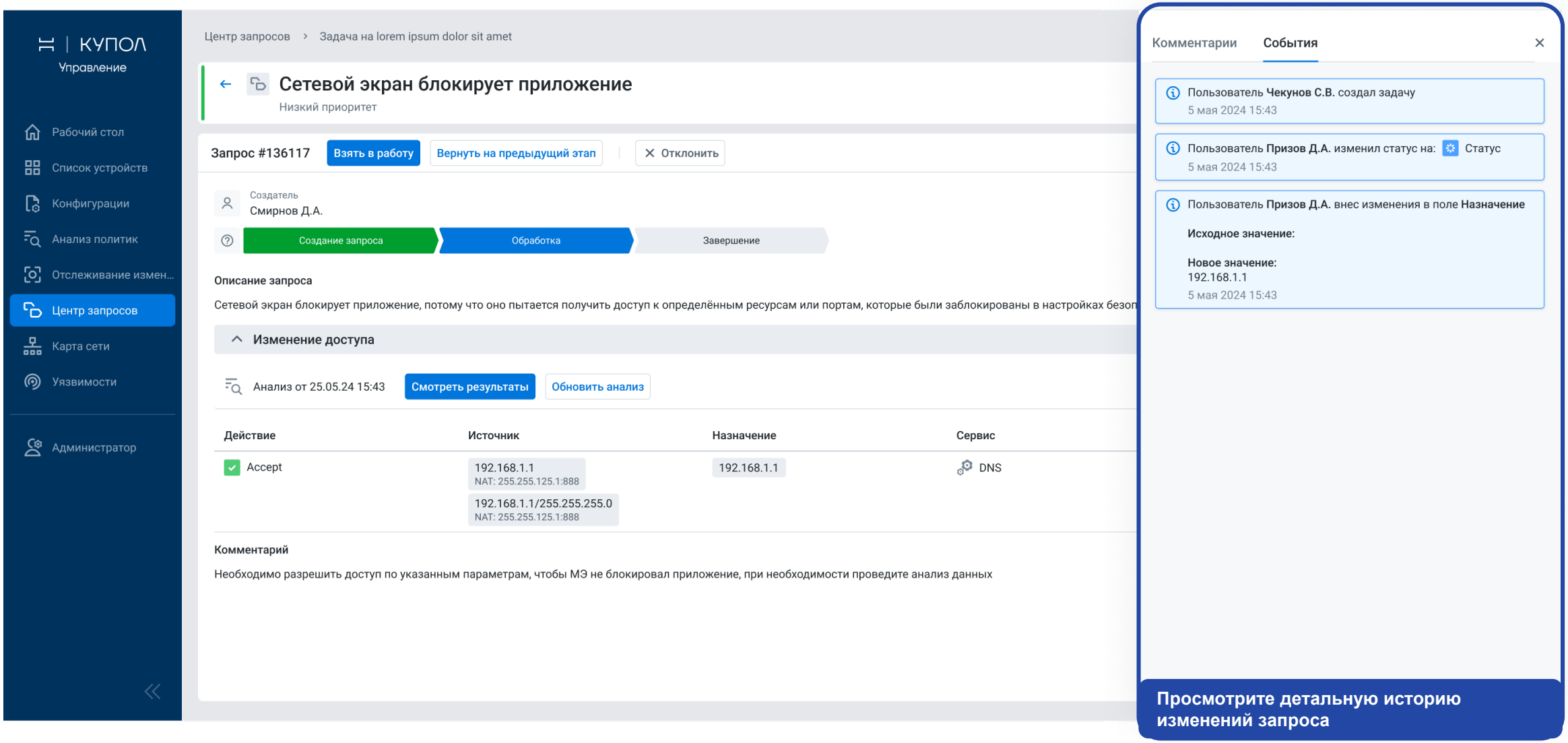
Просмотрите список рекомендаций по изменению конфигураций, и при необходимости примените их к конечным устройствам, или изучите список аномалий, которые могут возникнуть при внесении изменений

ЦЕНТР ЗАПРОСОВ — ОБРАБОТКА ЗАПРОСОВ

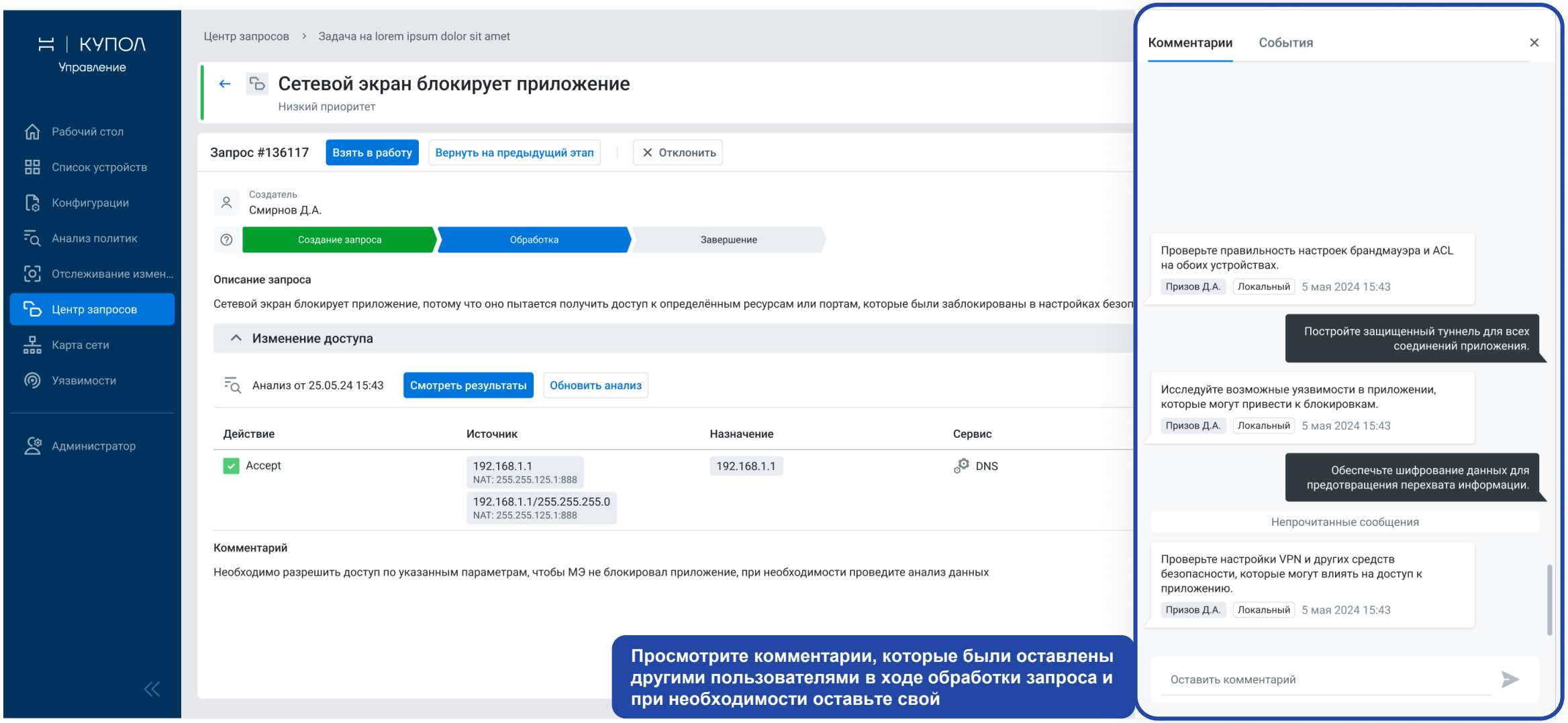


Просмотрите список рекомендаций по изменению конфигураций, и при необходимости примените их к конечным устройствам, или изучите список аномалий, которые могут возникнуть при внесении изменений

ЦЕНТР ЗАПРОСОВ — ОБРАБОТКА ЗАПРОСОВ

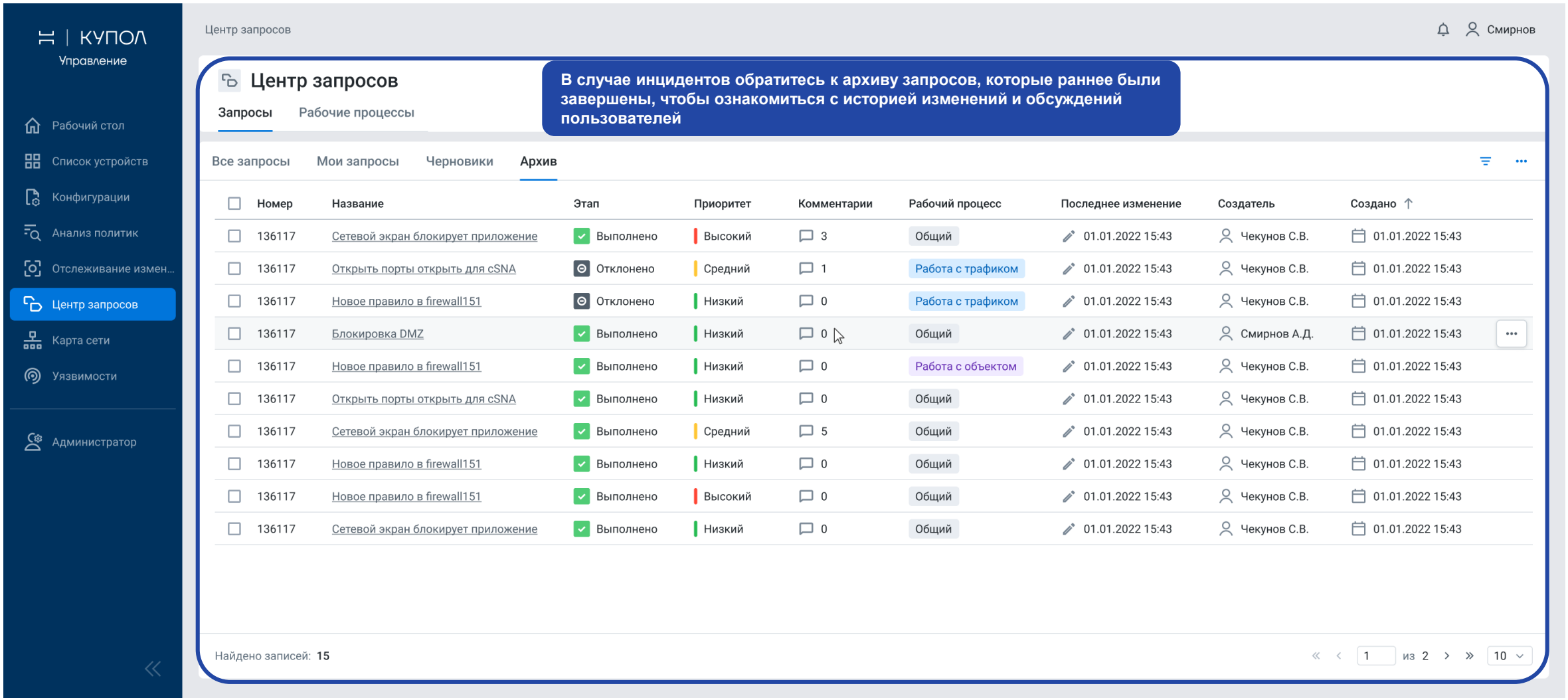


ЦЕНТР ЗАПРОСОВ — ОБРАБОТКА ЗАПРОСОВ



Просмотрите комментарии, которые были оставлены другими пользователями в ходе обработки запроса и при необходимости оставьте свой

ЦЕНТР ЗАПРОСОВ — АРХИВЫ ЗАПРОСОВ



НОТА | КУПОЛ

СПАСИБО ЗА ВНИМАНИЕ!

Игорь Душа

Директор портфеля решений
по информационной безопасности
НОТА КУПОЛ
idusha@nota.tech

ЗАПИСАТЬСЯ НА ПЕРСОНАЛЬНУЮ ДЕМОНСТРАЦИЮ

+ITI