АПИ-ФАКТОРИ

Опыт внедрения XDR в технологическом сегменте сети

Подготовил: Сафонов Александр

Начальник управления информационной безопасности ООО «АПИ-ФАКТОРИ»

10.2024

1.Предпосылки

- Выполнение требований законодательства

- Уровень зрелости информационной безопасности

2. Защита проекта

Основные критерии

-Обеспечение непрерывности производства (ответственность, деньги)

-Выполнение законодательства (ответственность, деньги)

3.Выбор средств защиты

Основные критерии:

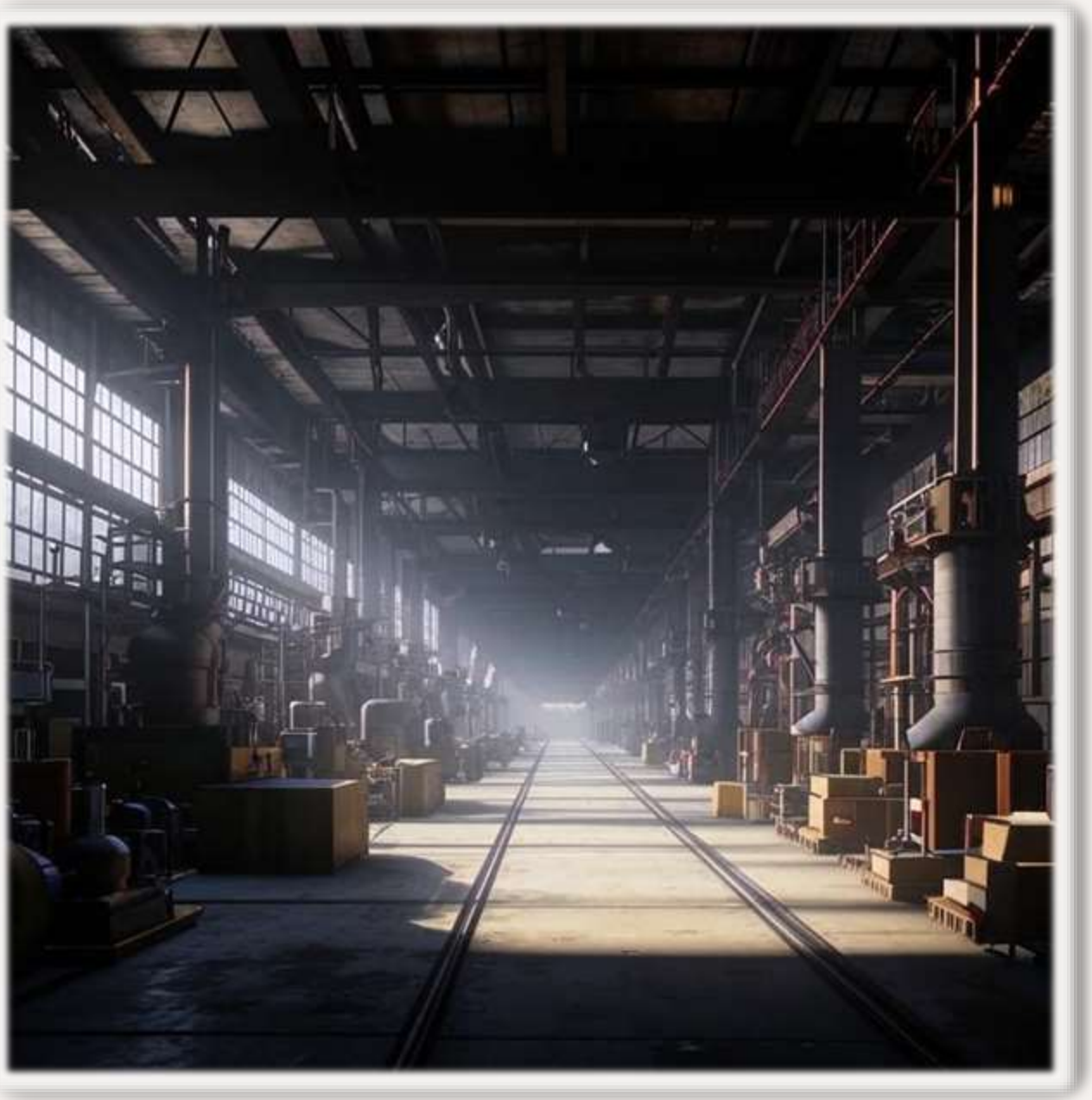
-Выполнение требований законодательства

-Поддержка промышленных протоколов

-Минимальное влияние на технические средства ТСПД

-Совместимость с уже применяемыми средствами защиты

4.Внедрение решения



АПИ-ФАКТОРИ

Где внедрили

РИМЕРА
ИЖНЕФТЕМАШ

CYBERSTEEL

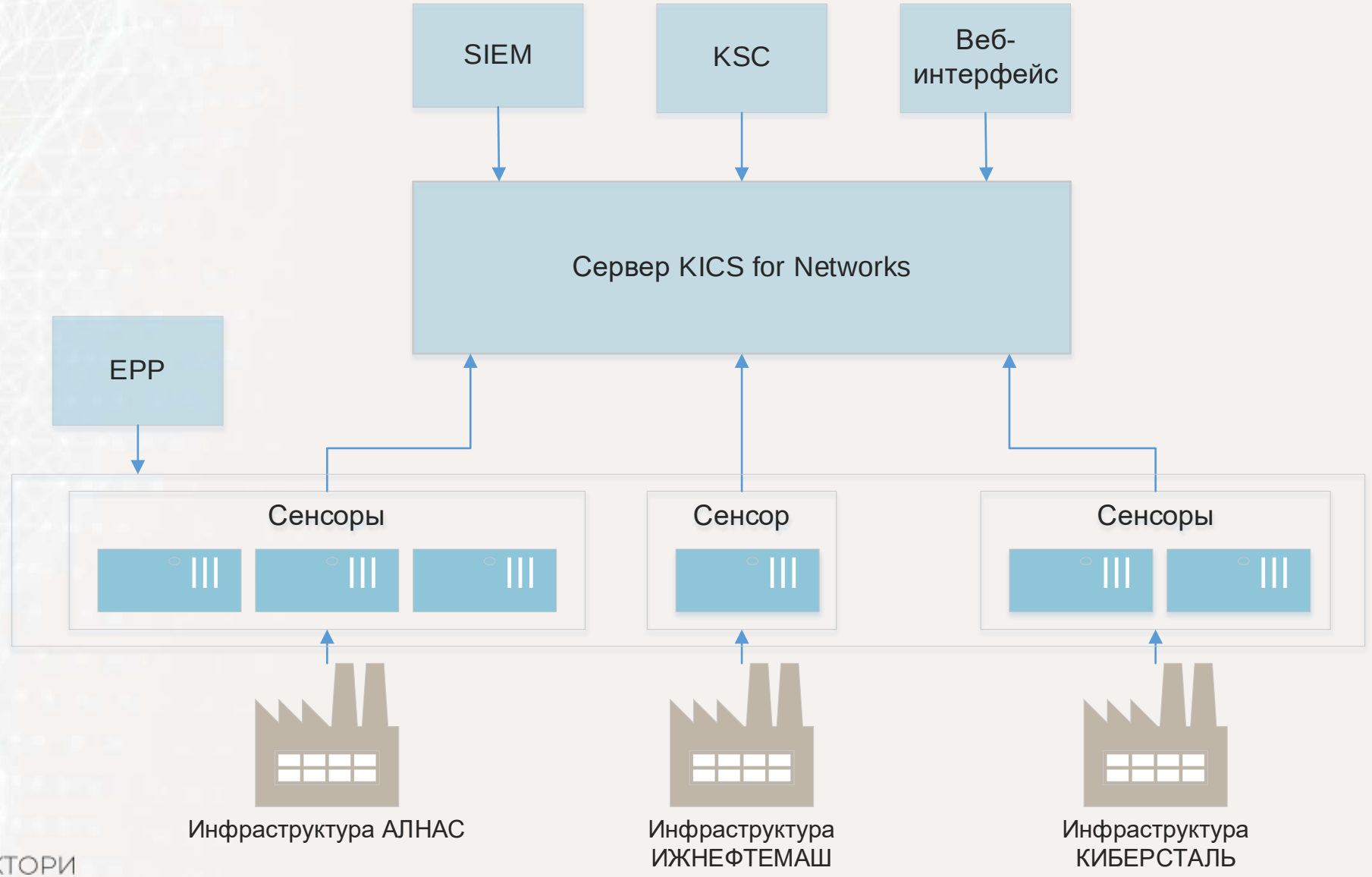
РИМЕРА
АЛНАС

Как внедряли

- Сбор исходных данных о площадках внедрения
- Установка Сервера KICS for Networks
- Установка и подключение сенсоров
- Установка и интеграция EPP*
- Интеграция решения с KUMA SIEM
- Активация точек мониторинга
- Постановка сенсоров в режим обучения

*EPP - Endpoint Protection Platform

Итоговая структура



5.Результаты внедрения

Достижение главных целей

- Выполнение требований законодательства РФ в области защиты критической информационной инфраструктуры

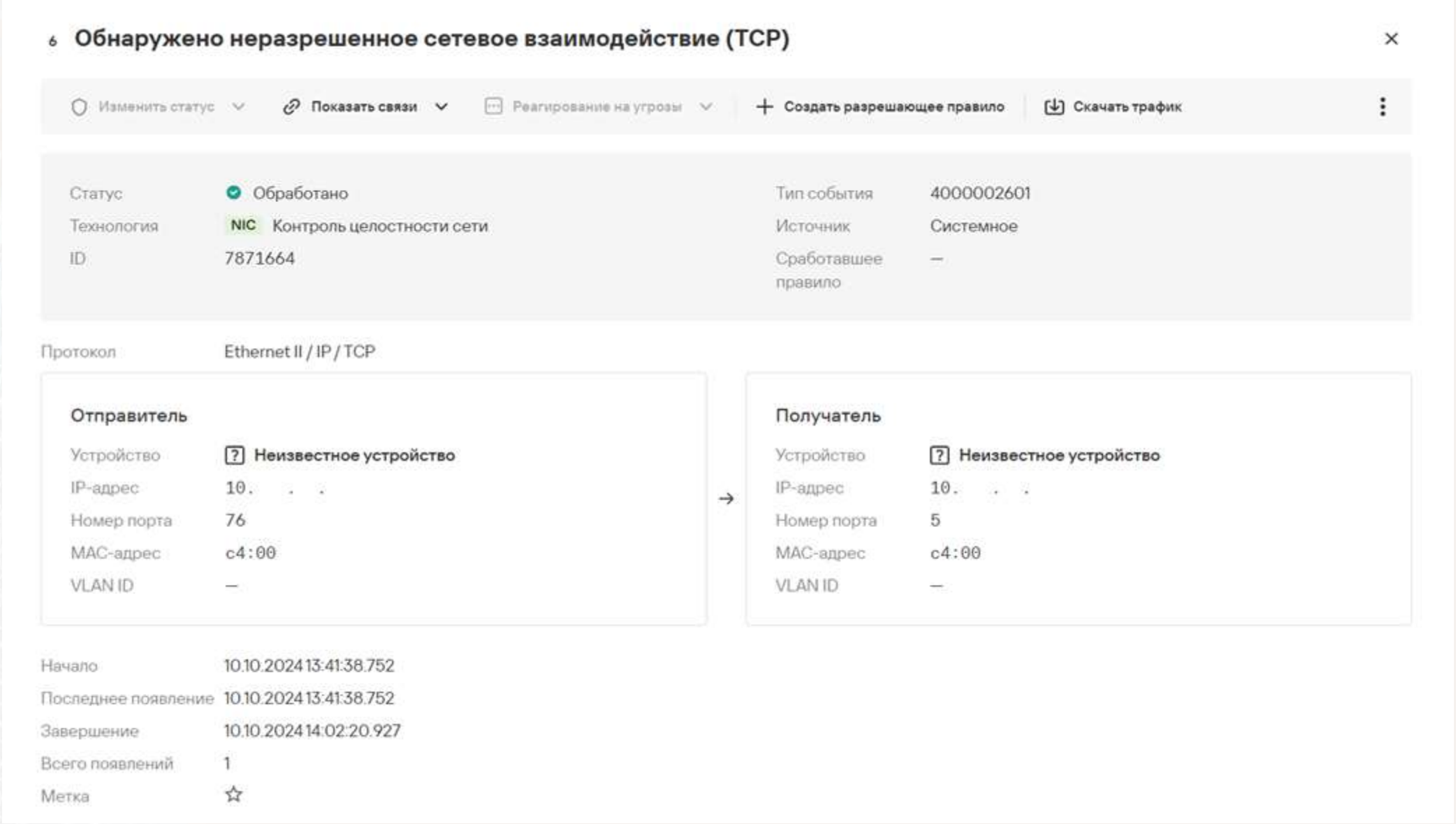
- Внедрение решения для защиты от угроз информационной безопасности в ТСПД

- Отсутствие негативного влияния на ТСПД и конечные точки из сегмента АСУ ТП

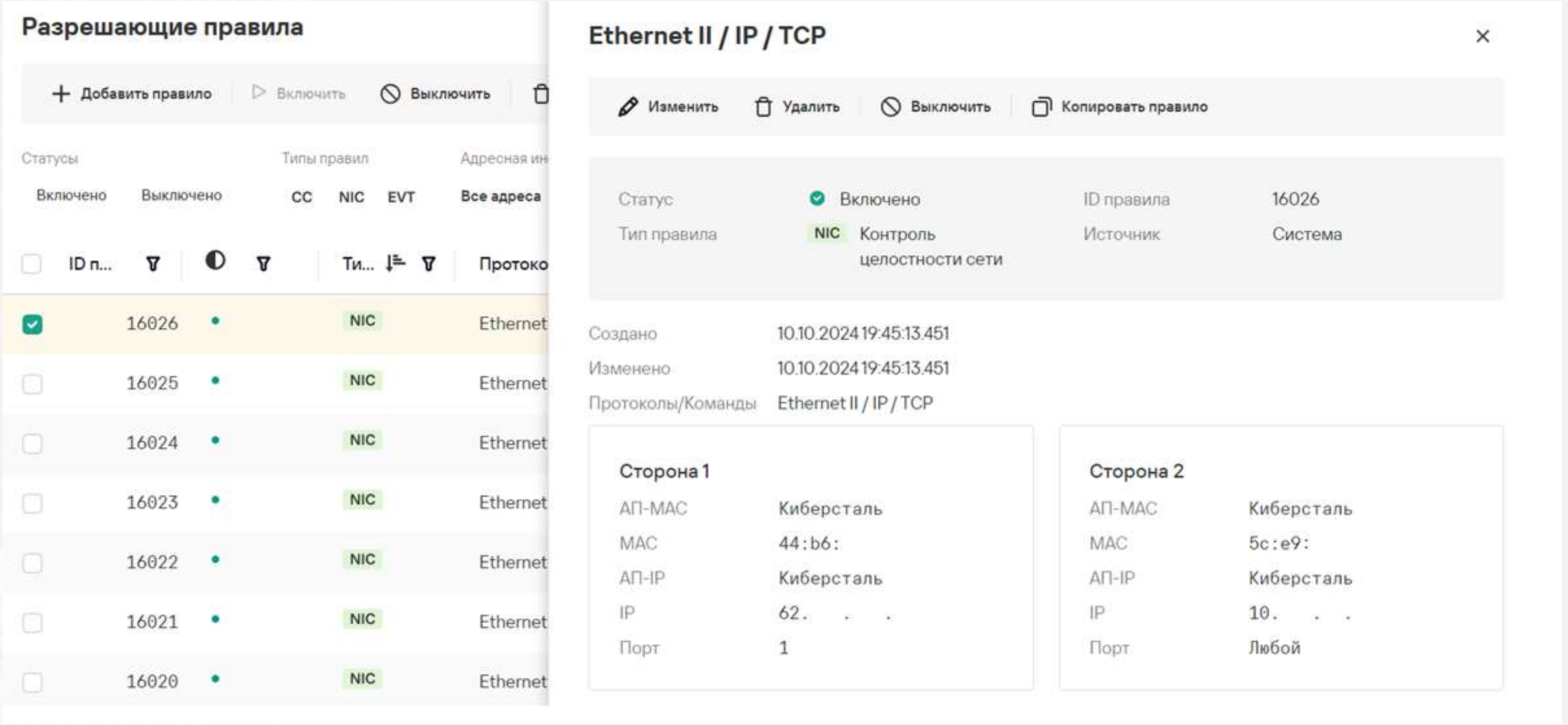
Новые возможности реагирования (в ТСПД)

- Анализ сетевого трафика между узлами
- Проверка соответствия сетевого взаимодействия заданным правилам
- Обнаружение вторжений
- Сбор событий безопасности и интеграция с SIEM
- Обнаружение рисков для ресурсов информационных систем
- Защита конечных точек

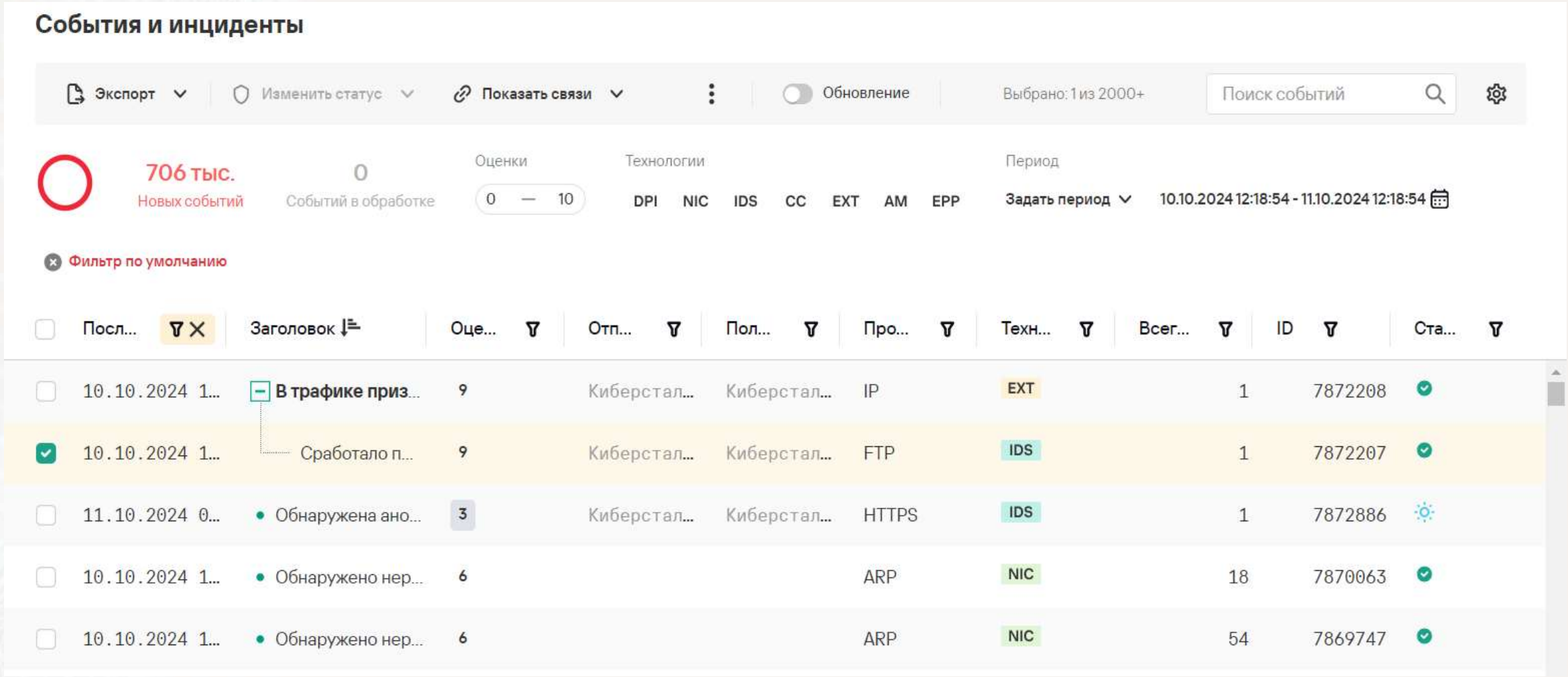
Приложение 1. Анализ сетевого трафика



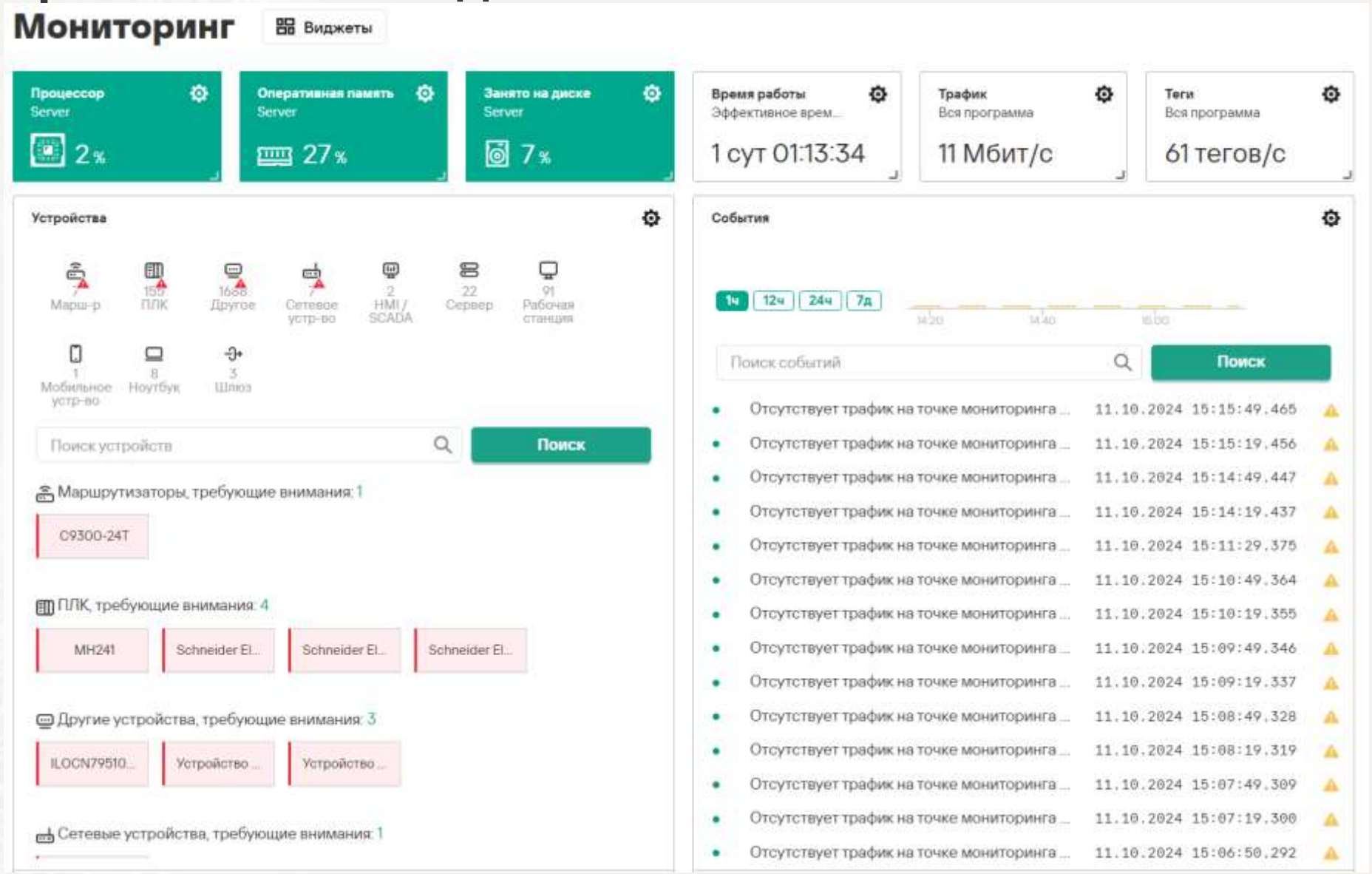
Приложение 2. Разрешающие правила



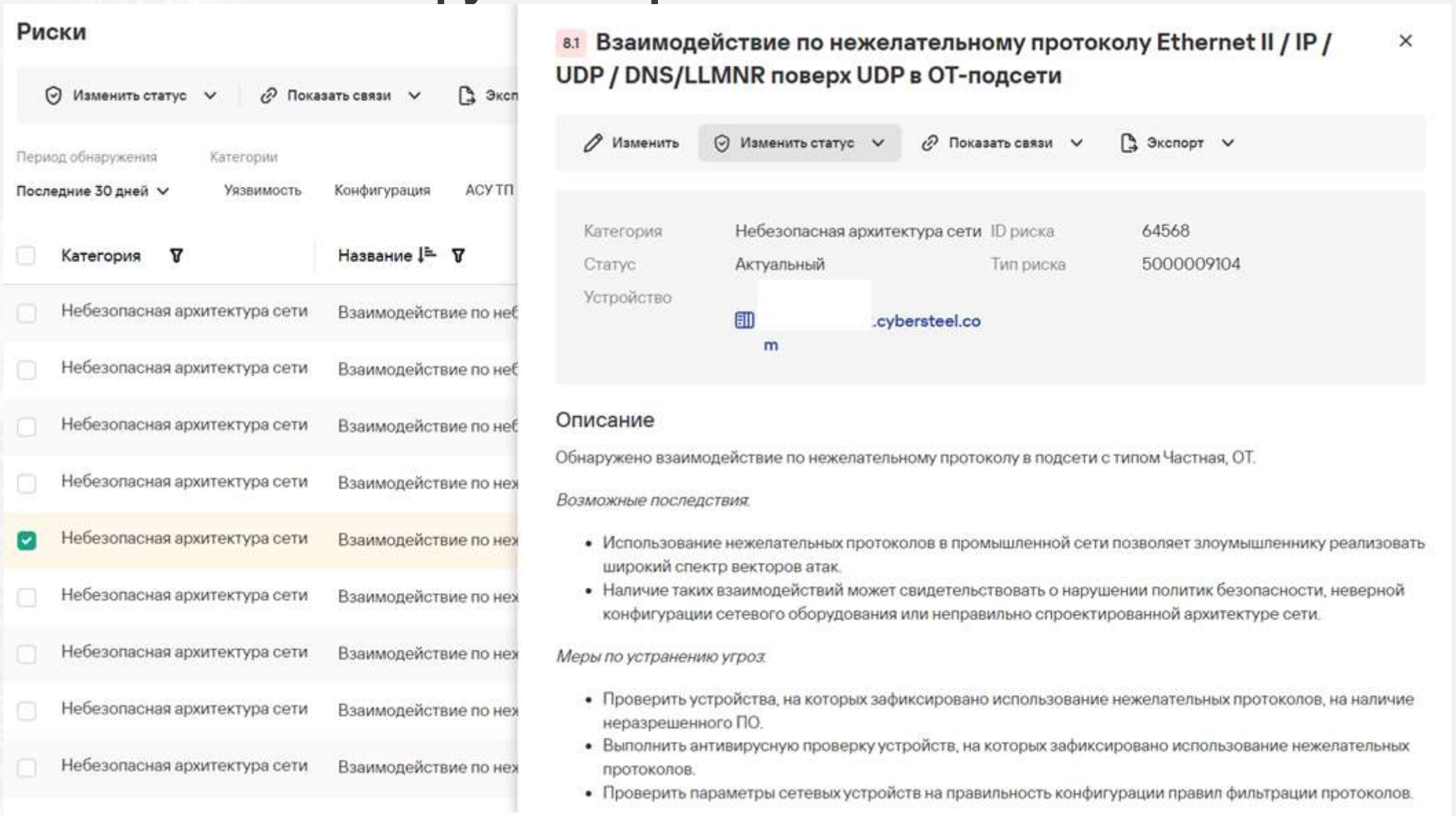
Приложение 3. Сбор событий безопасности



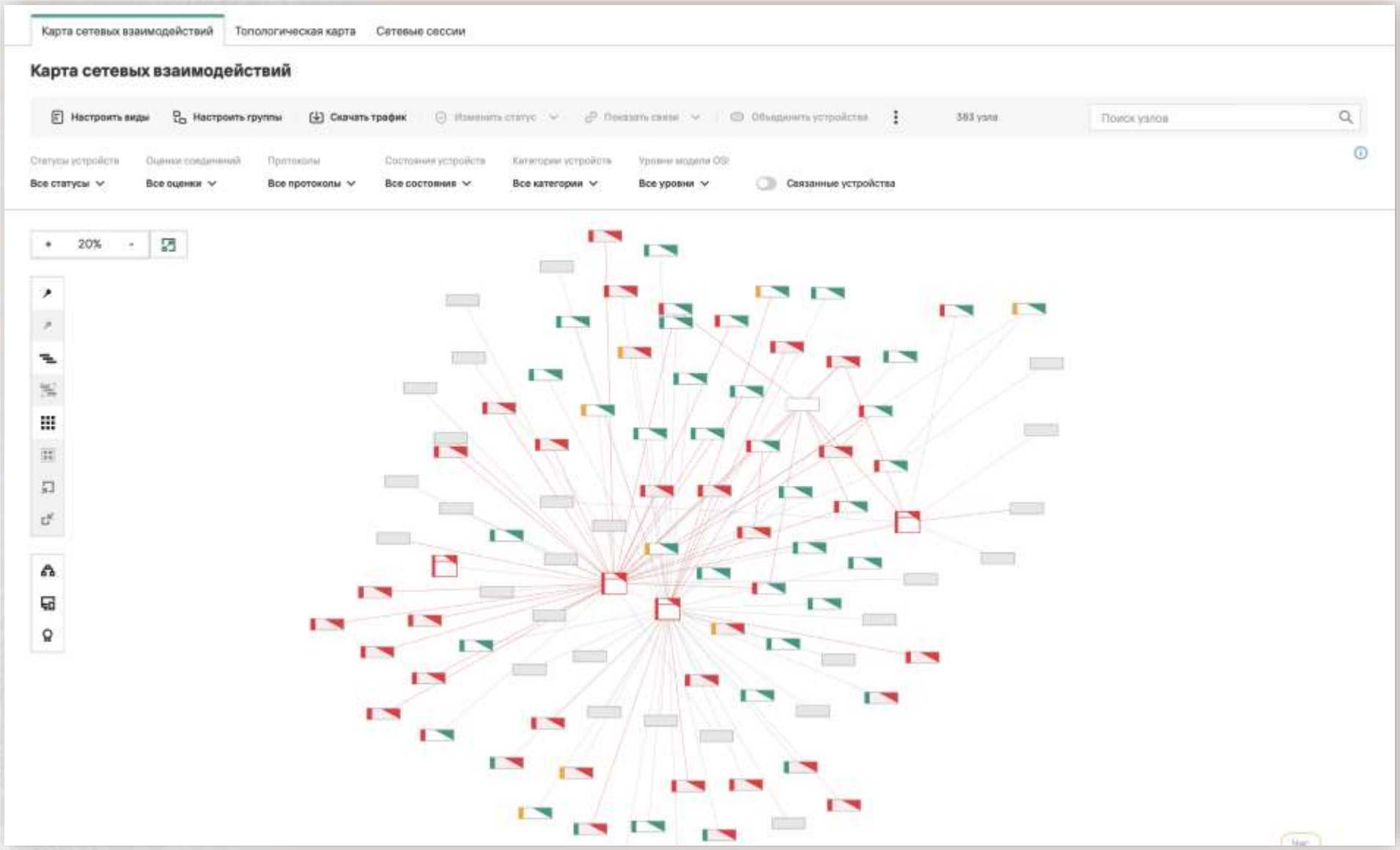
Приложение 4. Виджеты



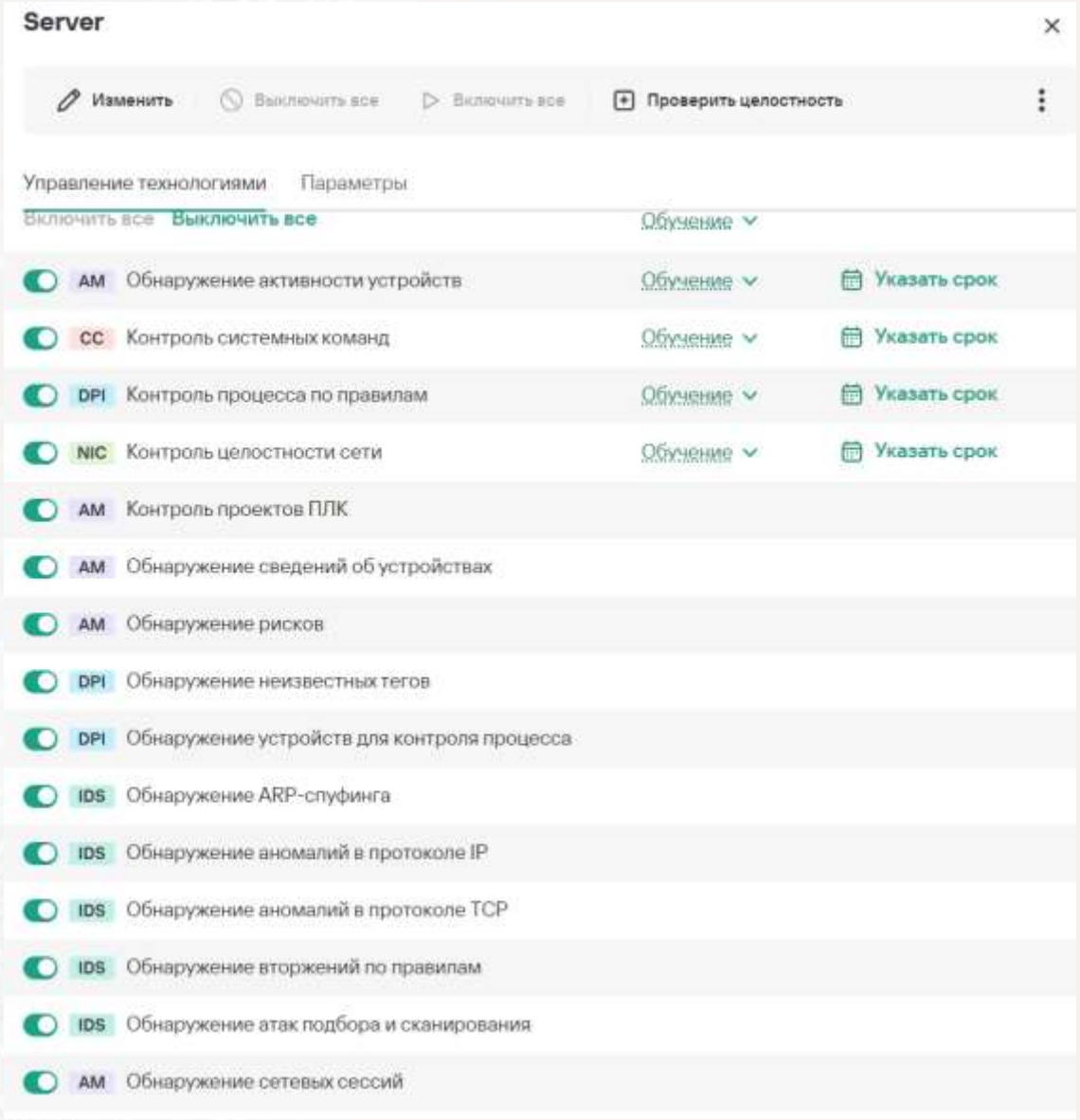
Приложение 5. Обнаружение рисков



Приложение 6. Карта сетевых взаимодействий



Приложение 7. Интерфейс управления технологиями защиты



Благодарю за внимание!

Сафонов Александр

Начальник управления информационной безопасности ООО «АПИ-ФАКТОРИ»

Aleksandr.Safonov@rimera.com

АПИ-ФАКТОРИ