udv|group

Что нового?

UDV NTA 2.1



2026

ОГЛАВЛЕНИЕ

Меньше рутины вокруг продукта 3

Новые возможности 4

Руководителю SOC: данным можно доверять

- Список активов без дубликатов

Интегратору и коммерческому SOC: продукт встраивается в ваши процессы

- Индикаторы из вашей TI-платформы приходят сами
- Управление через API
- Тонкая настройка с UDV AI Platform в 5 раз быстрее
- Установка за 15 минут

Аналитику: ответ за один фильтр

- Где в сети побывал этот файл?
- Кто обращался к этому ресурсу?
- Откуда узлы берут время?

Как перейти на 2.1 10

Контакты 11

МЕНЬШЕ РУТИНЫ ВОКРУГ ПРОДУКТА



UDV NTA 2.1 забирает у команды ИБ работу по обслуживанию самого NTA. Чистить список активов от дубликатов, переносить индикаторы из TI-платформы, править исключения на каждом сенсоре, часами разворачивать дистрибутив. Теперь большую часть берет на себя система, на остальное уходят минуты.

Мы держимся принципа, с которого начинали 2.0: чем меньше времени человек тратит на управление системой, тем ближе она к идеалу.

Что меняется для команды

1. **Число дубликатов активов сократилось более чем в 3 раза.** Узел остается тем же активом, когда у него меняется сетевая карта или виртуальная машина переезжает на другой хост. История инцидентов при этом не теряется.
2. **Индикаторы и настройки больше не переносятся руками.** Продукт сам забирает индикаторы из TI-платформы, а SOAR, IRP и скрипты управляют инцидентами, активами и правилами через API. С UDV AI Platform исключения настраиваются в 5 раз быстрее.
3. **Установка занимает 15 минут.** Раньше на нее уходило 3–4 часа ввода команд. Мастер ведет по шагам, справится даже неподготовленный специалист.

Обновление до 2.1 входит в действующую техническую поддержку.



Список активов без дубликатов

Список активов нужен почти в каждой задаче команды: в расследовании, на карте сети, в отчетах для проверяющих. До 2.1 продукт узнавал устройство по паре IP- и MAC-адреса. Заменили сетевую карту или перенесли виртуальную машину, и в списке появлялась вторая карточка того же узла. Инциденты оставались привязаны к старой, на карте висели два узла вместо одного, и кому-то приходилось вычищать дубли руками.

В 2.1 узел опознается сразу по нескольким признакам из трафика: адресам, имени машины в домене, сетевым именам, идентификатору DHCP-клиента. Одних адресов для этого мало. Если совпадение спорное, система активы не склеивает. Ошибочно объединить два разных устройства хуже, чем оставить дубликат.

Вся логика работает на сервере управления, так что переучиваться в интерфейсе не придется.

Что получает команда:

- Инцидент остается привязан к тому же активу после замены сетевой карты.
- Узлы за маршрутизатором больше не сливаются в один и не размножаются, поэтому карта сети похожа на настоящую сеть.
- После ремонта, замены оборудования или миграции виртуальных машин список почти не приходится чистить.

Новую логику мы проверили на собственной сети UDV Group: один и тот же сегмент, старый и новый алгоритм.

Показатель	Было	Стало
Активов в списке	5 311	**1 696**
Лишних копий актива под тем же именем	1 902	**152**

Нагляднее всего видно на IP-телефонах одной модели. Раньше они занимали в списке 303 карточки, теперь 63, ровно по числу аппаратов.

ИНТЕГРАТОРУ И КОММЕРЧЕСКОМУ SOC: ПРОДУКТ ВСТРАИВАЕТСЯ В ВАШИ ПРОЦЕССЫ

Индикаторы из вашей TI-платформы приходят сами

Многие SOC уже платят за коммерческие фиды или ведут свою TI-платформу. Индикаторы оттуда приходилось выгружать и загружать в NTA вручную, и часть успевала устареть еще до загрузки.

В 2.1 UDV NTA сам забирает индикаторы из вашей TI-платформы по TAXII в формате STIX. Трафик проверяется по всем источникам сразу: экспертизе UDV Threat Intelligence, собственным спискам организации и подключенным TI-платформам. Если индикатор сработал, в карточке инцидента видно, откуда он пришел.

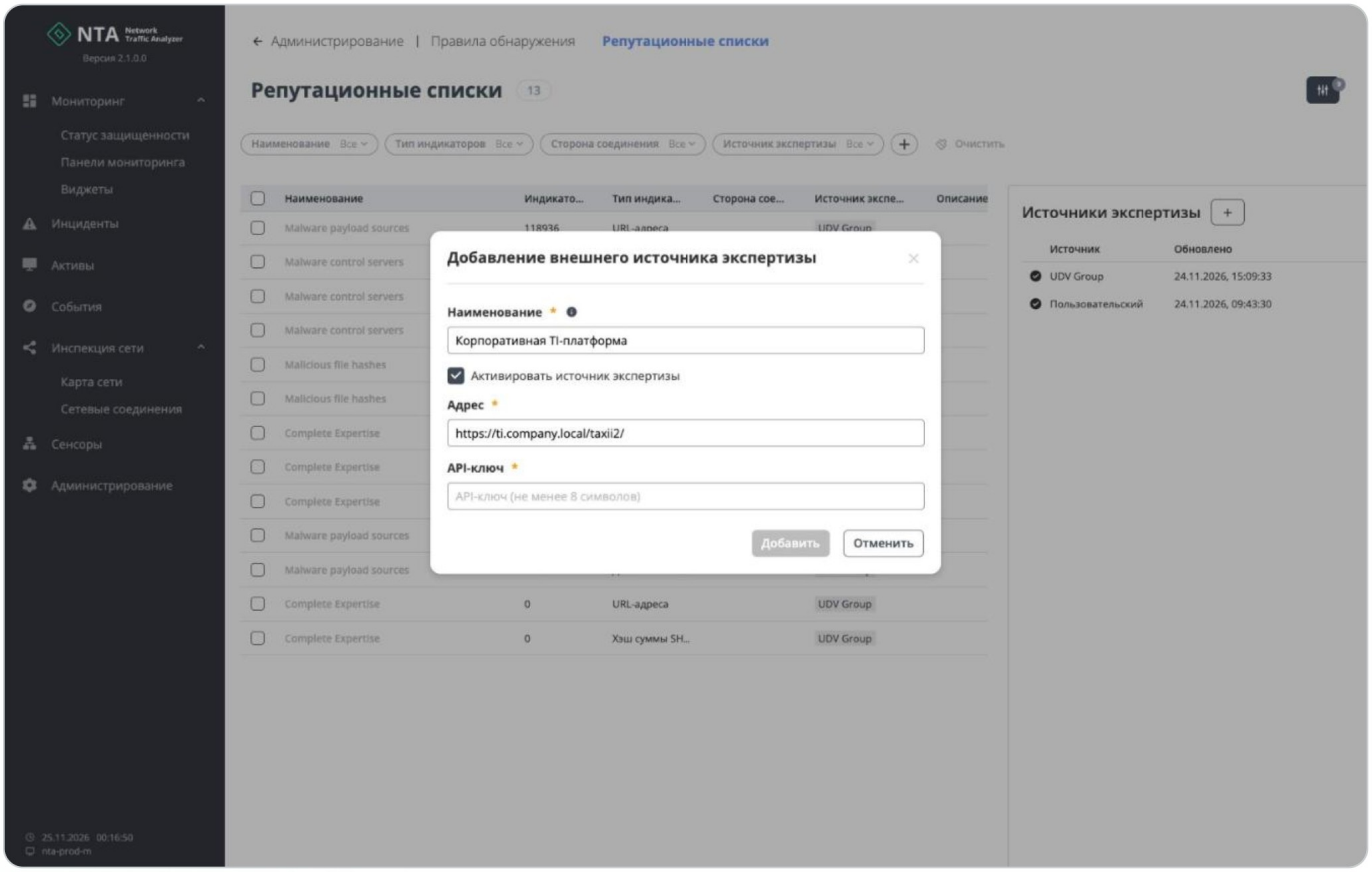

Рис. 1. Добавление TI-платформы в источники экспертизы

ИНТЕГРАТОРУ И КОММЕРЧЕСКОМУ SOC: ПРОДУКТ ВСТРАИВАЕТСЯ В ВАШИ ПРОЦЕССЫ



Управление через API

Через внешний API UDV NTA 2.1 управляется из SOAR, IRP, CMDB и скриптов SOC. Статусы, группы активов и исключения больше не нужно переносить из системы в систему руками.

Задача	Как решается через API
Держать статусы инцидентов одинаковыми в NTA и системе обработки инцидентов	Обновление инцидента или сразу набора инцидентов
Сверять список активов и группы с CMDB и корпоративными справочниками	Создание, изменение и удаление активов, в том числе пакетно; замена дерева групп
Хранить правила обнаружения как код и выкатывать их на все сенсоры	Создание, изменение и удаление правил; исключение для набора правил на конкретном сенсоре
Подстроить пороги срабатывания под конкретный сегмент сети	Изменение параметров детекторов сенсора

Коммерческий SOC, который ведет нескольких заказчиков, может управлять всеми инсталляциями UDV NTA из своих привычных инструментов.

Тонкая настройка с UDV AI Platform в 5 раз быстрее

Исключения через API настраиваются для всех решающих правил продукта, включая правила обнаружения. UDV AI Platform пользуется этим API: шумное срабатывание разбирается в диалоге с ассистентом, и он сам готовит и вносит исключение. Править правила на каждом сенсоре вручную больше не нужно.

Пятикратное ускорение касается заказчиков, у которых развернута UDV AI Platform.

Установка за 15 минут

Раньше установка занимала 3–4 часа: инженер вводил команды по документации. В 2.1 мастер сам спрашивает параметры и прописывает их в конфигурацию. На ответы уходит минут 5, на саму установку около 10.

Знать команды и порядок настройки не нужно. Инженер партнера ставит продукт сам, без созвона с вендором на каждом шаге.

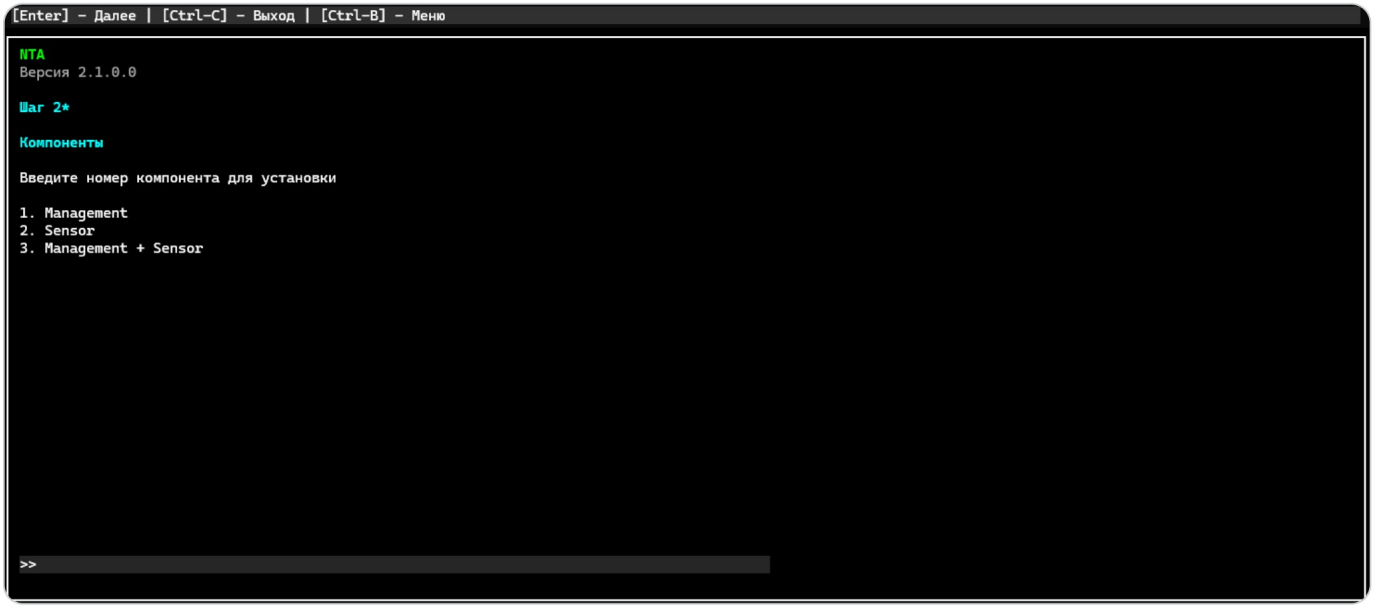

Рис. 2. Выбор компонентов в мастере установки

АНАЛИТИКУ: ОТВЕТ ЗА ОДИН ФИЛЬТР

Есть три вопроса, которые аналитик задает почти в каждом расследовании. В 2.1 на каждый отвечает один фильтр.

Где в сети побывал этот файл?

В списке извлеченных из трафика файлов появились хеш-суммы MD5 и SHA-256. Достаточно вставить в фильтр хеш из бюллетеня или отчета песочницы, и видно, когда и между какими узлами передавался файл.

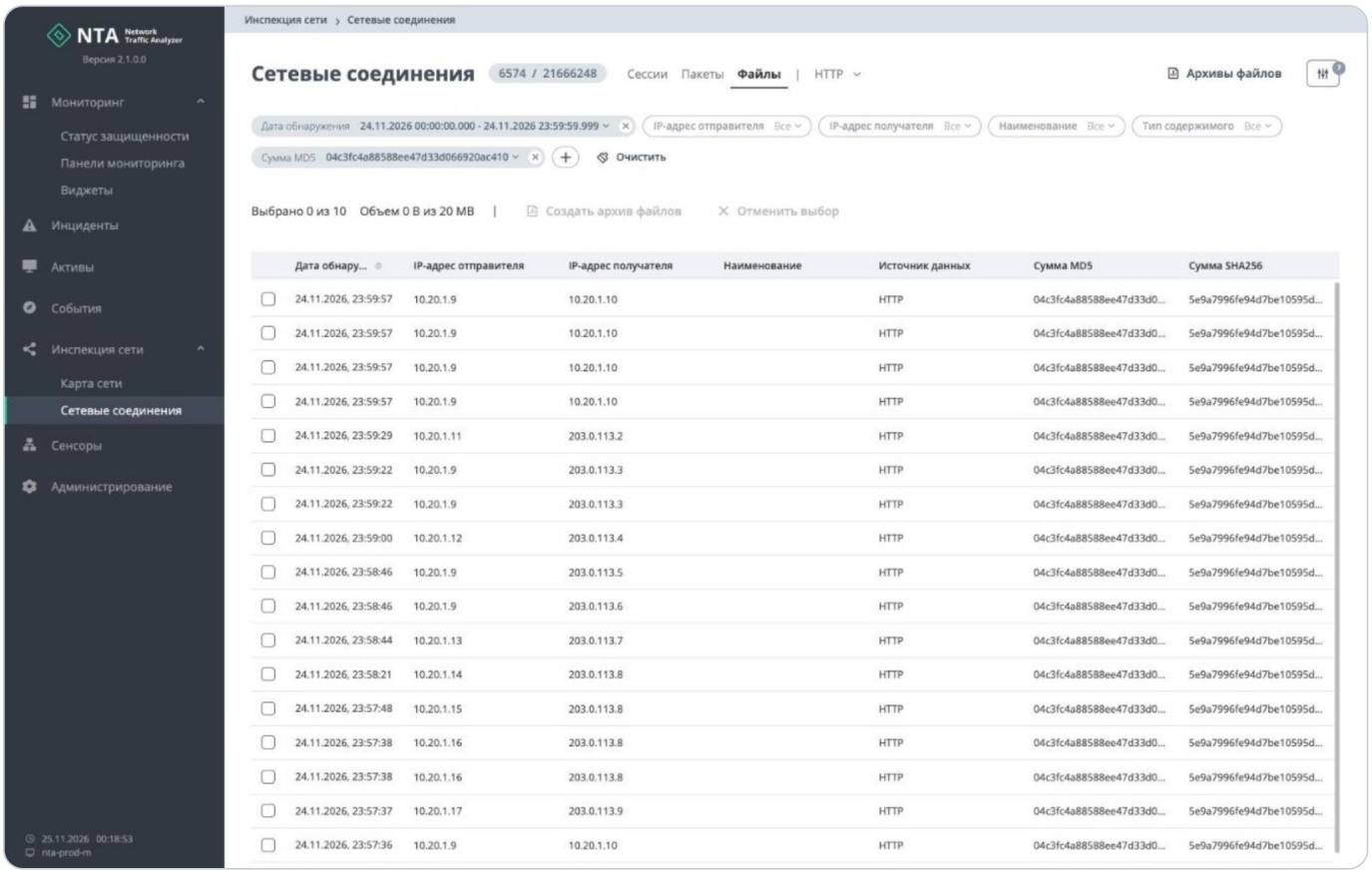

Рис. 3. Файлы с одним хешем MD5, переданные между разными узлами

Кто обращался к этому ресурсу?

Фильтр по полю «URI получателя» находит все обращения к странице администрирования, загруженному веб-шеллу или адресу из описания уязвимости. Если добавить фильтр по приложению клиента, станет понятно, каким инструментом пользовались.

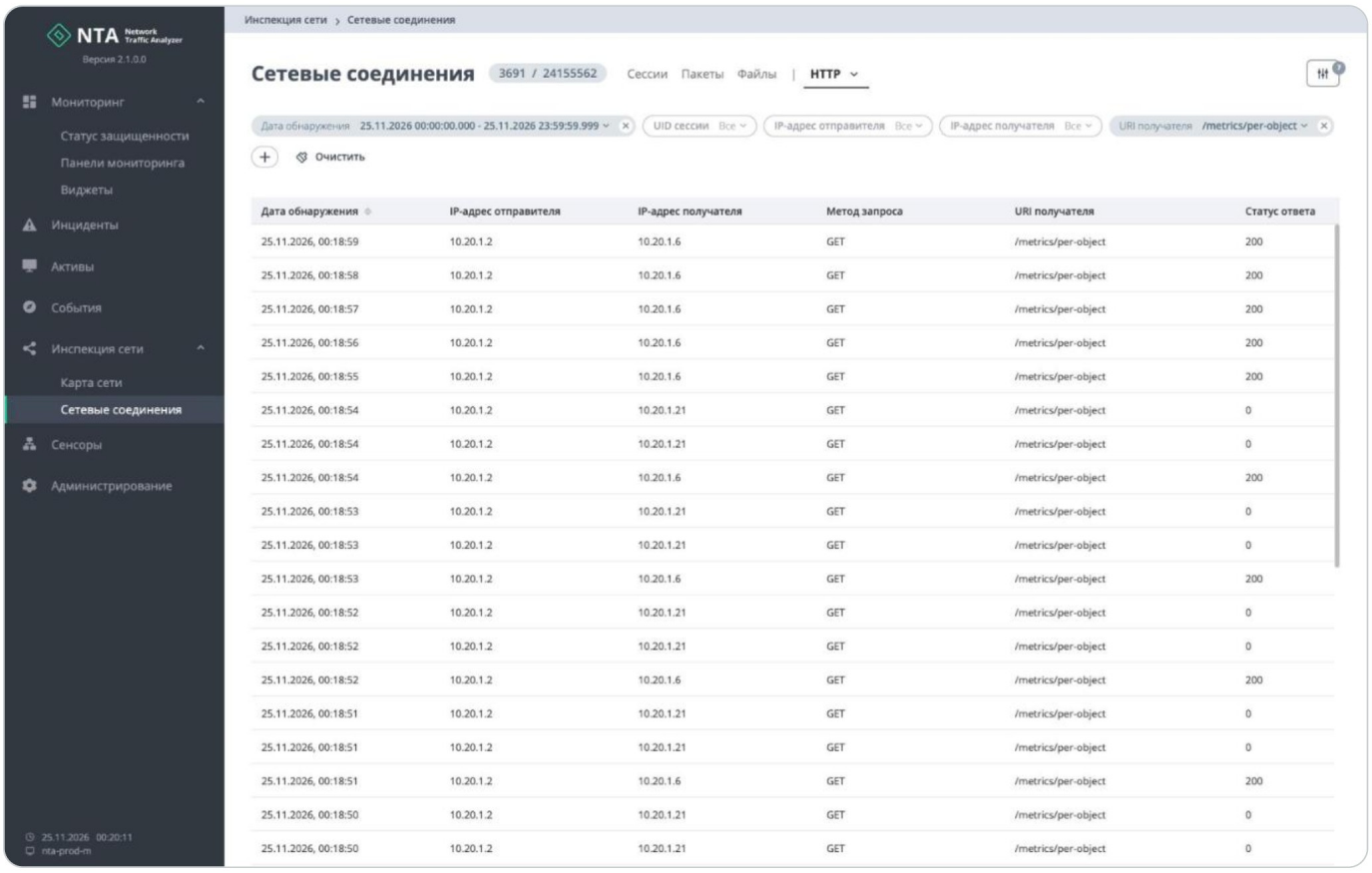

Рис. 4. Фильтр по полю «URI получателя» для протокола HTTP

Откуда узлы берут время?

В 2.1 появился разбор протокола NTP. От точного времени зависят доменная аутентификация и корреляция журналов, поэтому полезно видеть узлы, которые синхронизируются мимо корпоративного сервера времени.

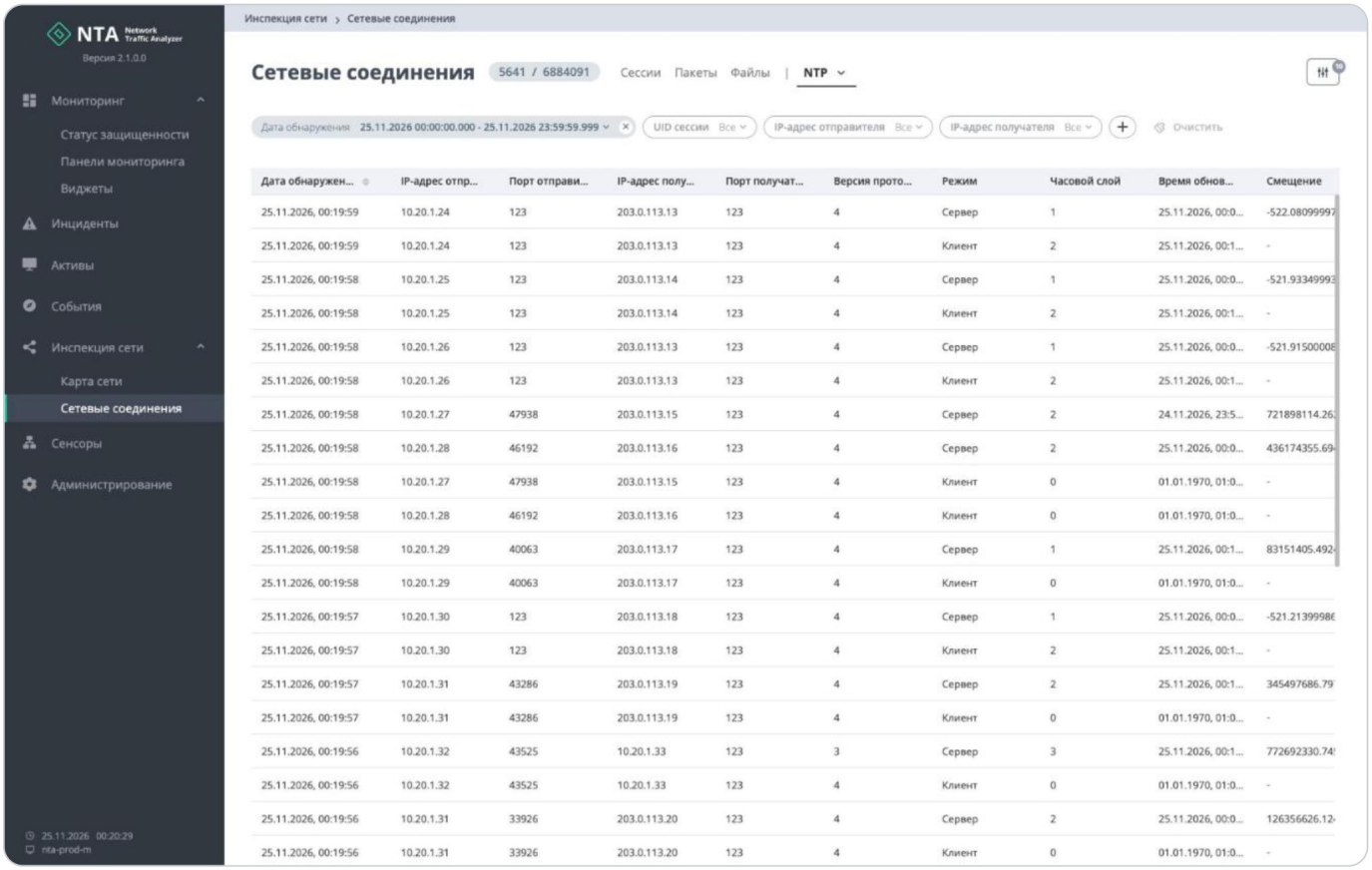

Рис. 5. Обращения узлов к серверам времени в разборе протокола NTP

КАК ПЕРЕЙТИ НА 2.1

- Обновление входит в действующую техническую поддержку.
- Обновиться можно с версий 1.1 и 2.0, порядок описан в документации.
- Активы сохранят свои наименования, а их адреса станут первыми признаками для новой логики.
- В документацию добавлены установка через мастер, новые методы API, работа с активами и подключение TI-платформ.

Чтобы обсудить переход на UDV NTA 2.1 или договориться о демонстрации, напишите нам.

Контакты
zapros@udv.group
8-800-333-04-65

Сайт продукта
nta.udv.group

Телеграм
@udv_group

Адрес
620100, г. Екатеринбург,
ул. Сибирский тракт, 12,
строение 7, этаж 4

udv|group

2026