udv|group

Что нового?

UDV NTA 2.0

2026

ОГЛАВЛЕНИЕ

ИИ-ассистент для аналитика сетевой безопасности

Главное обновление релиза — в UDV NTA появился UDV AI (ИИ — ассистент).
Он подключается к продукту как браузерное расширение аналитика ИБ и работает с данными Management.

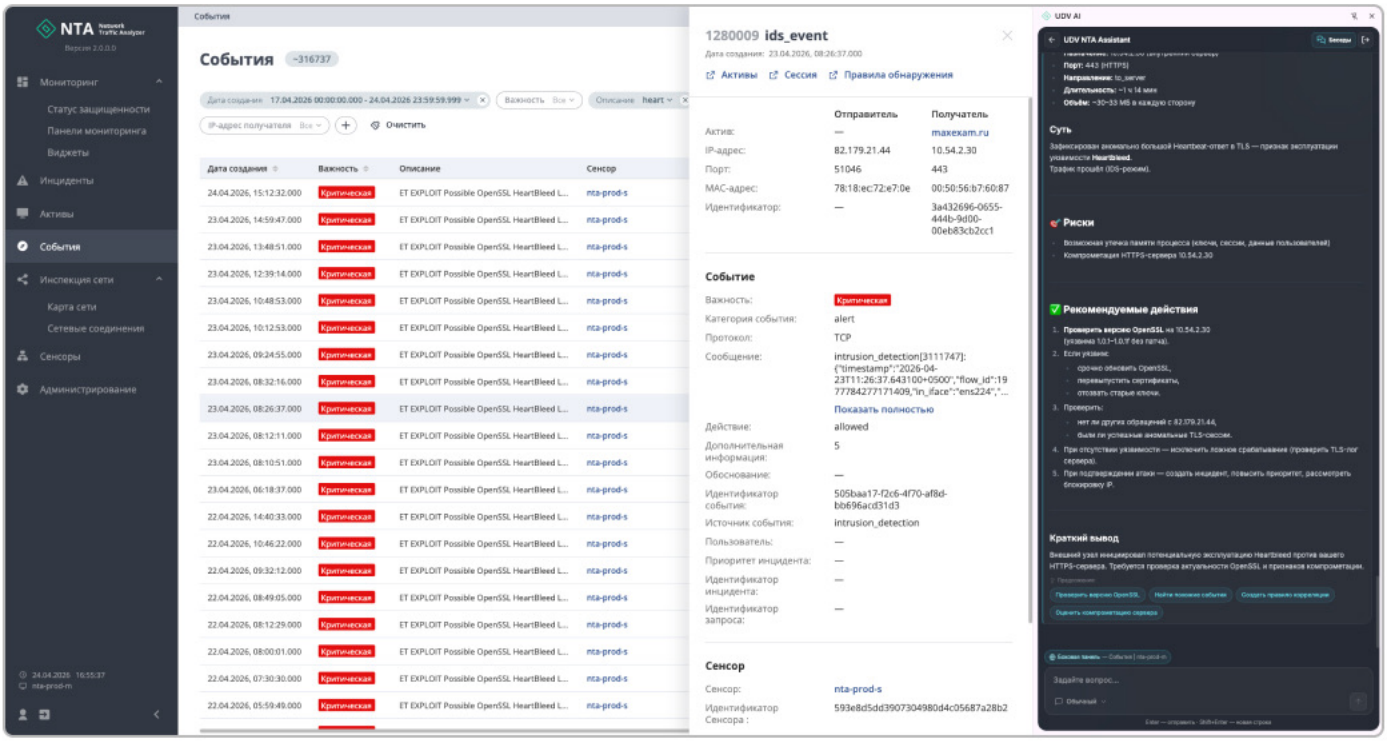

Рис. 1. ИИ-ассистент в интерфейсе продукта

Ассистент разбирает инцидент и сразу выдает рекомендации по реагированию с учетом контекста компании: регламентов, критичных активов и бизнес-процессов. Также по запросу он формирует отчет в нужном формате и объеме — от короткой сводки по инцидентам за смену до развернутого отчета по сетевой активности за месяц с разбивкой по протоколам, объемам трафика и приоритету расследования. Искать инструкцию или вручную сопоставлять событие с картой сети больше не нужно — ответ приходит за секунды.

За счет ассистента порог входа в анализ сетевого трафика снижается. С продуктом уверенно работает специалист без глубокой экспертизы в NTA, где ИИ помогает разобраться в событии и подсказывает следующий шаг.

В основе ассистента — MCP-сервер. Он подключается к UDV NTA Management, обращается к REST API продукта и забирает данные по инцидентам, активам, сетевым соединениям и событиям - это материал для рекомендаций и отчетов ассистента.

АВТОМАТИЗАЦИЯ И СНИЖЕНИЕ НАГРУЗКИ

Ассистент опирается на два источника знаний: базу знаний самой компании-заказчика и экспертизу UDV Security. В платформе заранее сформированы датасеты с документацией и экспертными знаниями UDV Group, которые ускоряют внедрение решения и повседневную работу аналитика, отвечая на вопросы по возможностям продукта и трактовке событий прямо в чате. Архитектура ассистента LLM независима: его можно подключить к локально развернутой модели или обезличивать данные при работе с внешними моделями.

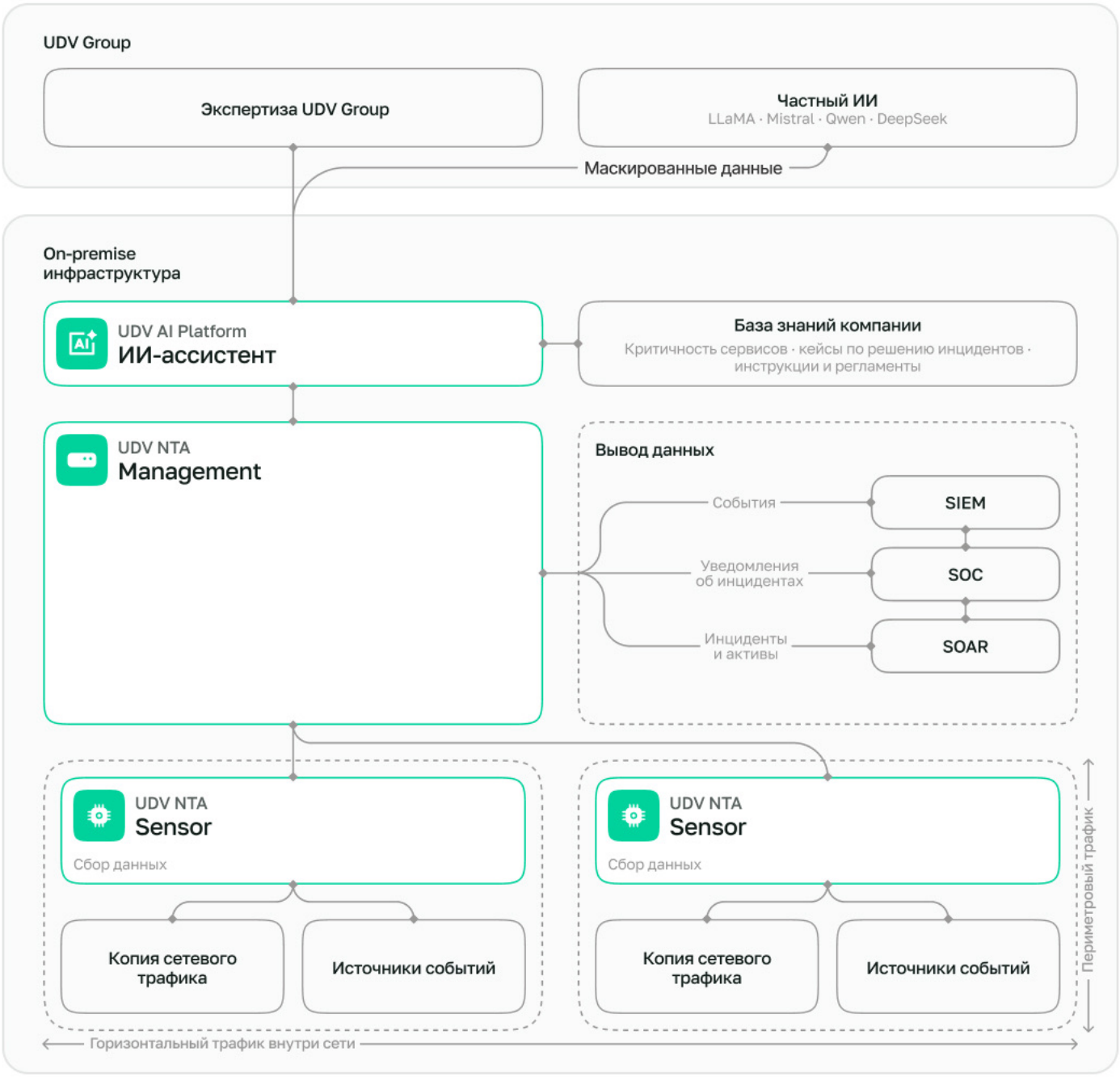

Рис. 2. Архитектура ИИ-ассистента в UDV NTA

Детектирование индикаторов компрометации по репутационным спискам

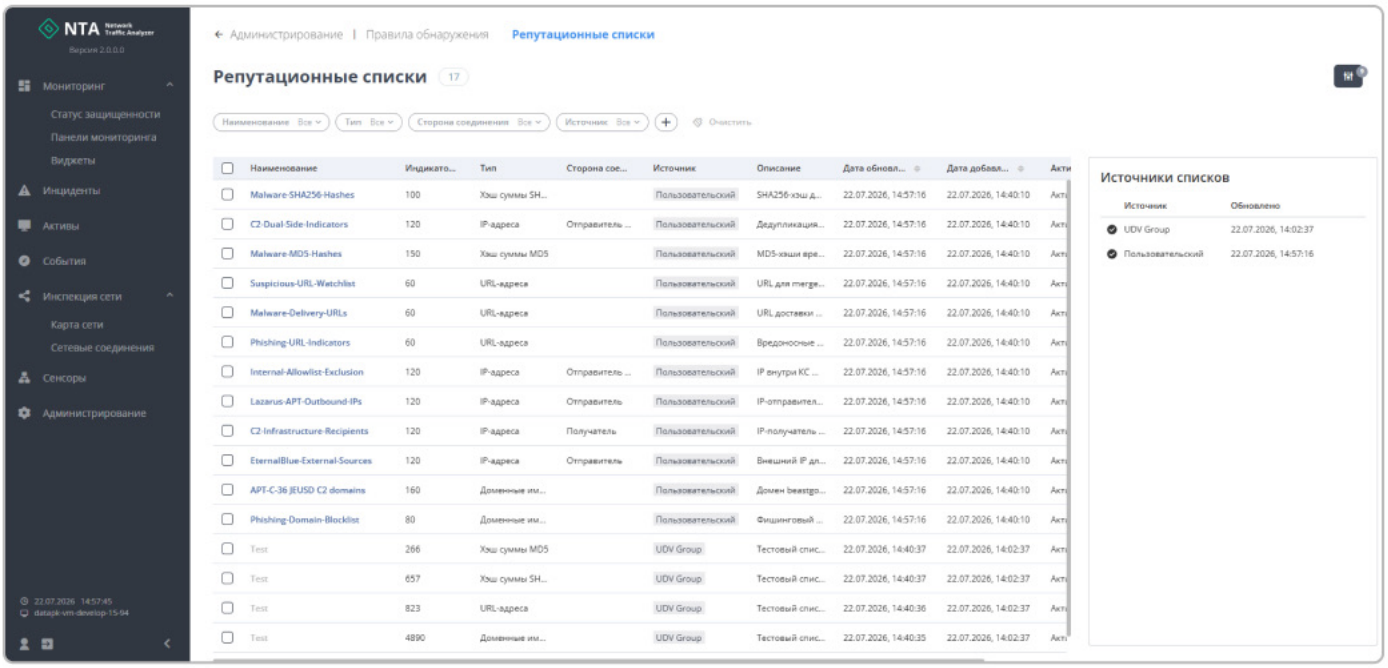

Рис. 3 Репутационные списки: пользовательские индикаторы и автообновляемый список от UDV Group

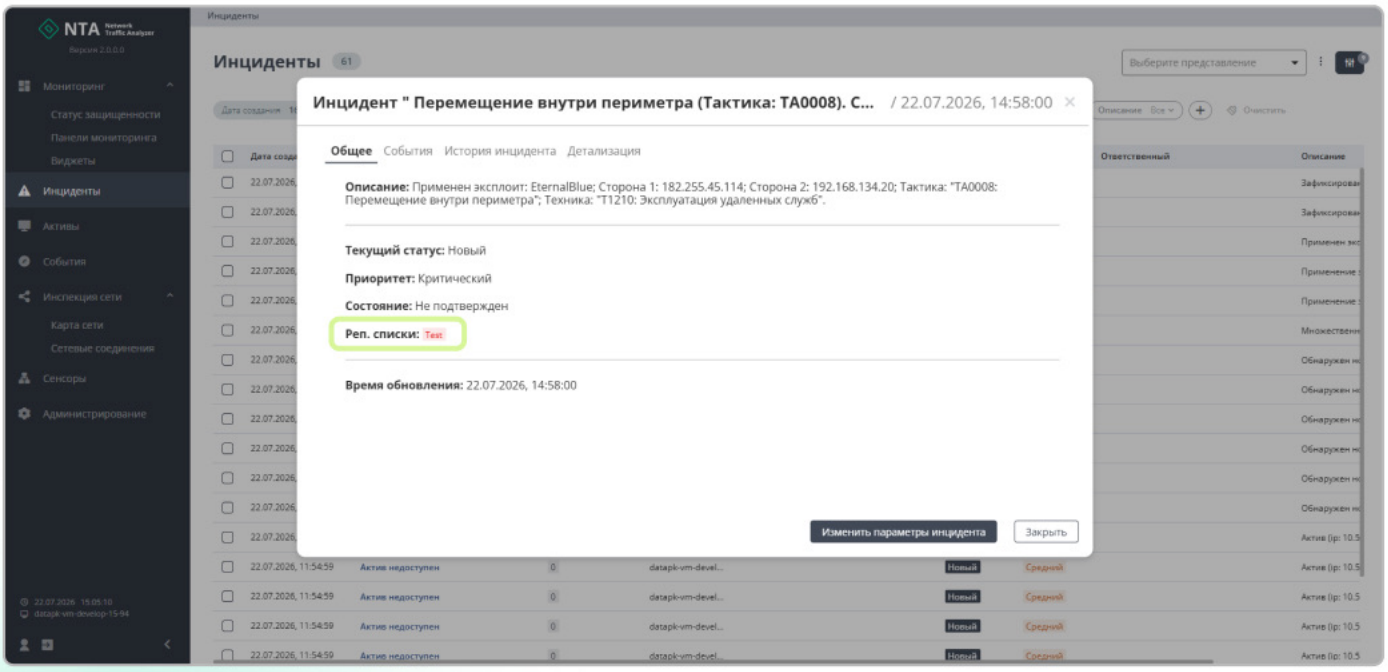

Рис. 4. Совпадение с репутационным списком отображается прямо в карточке инцидента

В релизе UDV NTA 2.0 добавлена проверка трафика по репутационным спискам. Всем клиентам с действующей лицензией на продукт становится доступна автообновляемая экспертиза вендора - UDV Threat Intelligence. Также возможно подключение собственной базы индикаторов компрометации.

ТОЧНОСТЬ ОБНАРУЖЕНИЯ УГРОЗ

Продукт сверяет с репутационными списками IP-адреса участников соединений, доменные имена из DNS-запросов, URL из HTTP-запросов и хеши извлеченных из трафика файлов (MD5, SHA-256). Проверка учитывает направление взаимодействия: к активу или от актива, и сравнивает его с направлением, заданным для индикатора при загрузке списка. При совпадении по значению индикатора и направлению формируется событие ИБ. Учет направления резко снижает количество ложных срабатываний и помогает аналитику быстрее приоритизировать реагирование.

На ранних этапах атаки злоумышленники используют известную инфраструктуру и типовые инструменты — так дешевле, даже если канал управления зашифрован и содержимое недоступно для инспекции. Обращение к серверу из репутационного списка выдает атакующего. Проверка хешей файлов позволяет обнаружить известное вредоносное ПО, опираясь на многолетнюю экспертизу UDV Group в выявлении угроз для крупных российских предприятий.

Новые методы детекторов: рост точности обнаружения

1. Сигнатурный анализ теперь учитывает направление в решающих правилах обнаружения вторжений: оно формируется автоматически из заданных в продукте границ контролируемой сети. Правила срабатывают с учетом положения узла — внутри защищаемой инфраструктуры или за ее пределами. Раньше правила применялись ко всему трафику без разбора, и это порождало поток срабатываний, не имеющих отношения к реальным угрозам.
2. Переработана логика выявления эксфильтрации данных через DNS-туннели — один из самых доступных каналов скрытой передачи данных, поскольку DNS-трафик разрешён практически в любой сети. Точность детектирования туннелирования повышена: меньше ложных событий в потоке для аналитика и избыточных записей в хранилище.

Вместе оба механизма кратно снижают количество ложных срабатываний, поэтому теперь аналитик разбирает меньше нерелевантных событий и быстрее доходит до реальных угроз.

Обнаружение эксплуатации уязвимости Heartbleed

Расширен перечень выявляемых сетевых атак: добавлено обнаружение эксплуатации уязвимости Heartbleed (CVE-2014-0160) в библиотеке OpenSSL.

Несмотря на возраст уязвимости, в корпоративных сетях продолжают работать необновленные системы, особенно во внутренних сегментах и на встраиваемом оборудовании. Продукт своевременно оповестит аналитика о попытке эксплуатации.

*Heartbleed (CVE-2014-0160) — это уязвимость в библиотеке OpenSSL, позволяющая злоумышленнику читать память сервера и похищать закрытые ключи, учётные данные и содержимое сессий.

Проактивный поиск угроз — кратный рост скорости в новой версии

В UDV NTA 2.0 переработана архитектура хранения и получения данных о сессиях. Активные и завершенные сессии разделены на уровне хранения, а запрос данных подстроен под новую схему.

Ускорение особенно заметно на высоконагруженных инсталляциях: там, где трафик измеряется десятками гигабит в секунду, а число сессий — десятками миллионов в сутки. Список сессий теперь загружается в десятки раз быстрее, а подсчет их количества по фильтру — на 20% быстрее. Утилизация RAM при проактивном поиске угроз снизилась в 2 раза и перестала зависеть от числа одновременно работающих аналитиков.

Продукт обрабатывает растущий объем трафика без роста затрат на серверную инфраструктуру, а специалисты SOC проводят расследования и проактивный поиск угроз по разобранным данным без задержек, даже при параллельной работе нескольких аналитиков.

Фильтрация по частичному совпадению домена в протоколе DNS

В фильтре по доменному имени добавлен поиск по частичному совпадению — по аналогии с фильтром «Приложение клиента» в протоколе HTTP.

Вредоносные домены и DNS-туннели часто меняют только один из уровней доменного имени. Поиск по полному совпадению в таких случаях не работал: аналитику приходилось перебирать варианты вручную. Теперь достаточно указать неизменную часть домена, чтобы увидеть всю связанную активность.

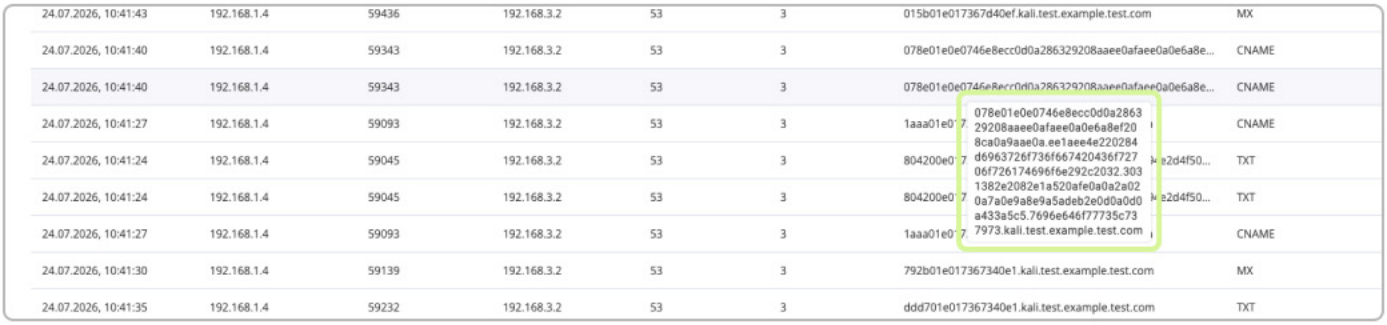

Рис. 5. Все запросы DNS-туннеля видны по одной неизменной части домена

Расширена индикация протоколов

В новой версии добавлено распознавание протоколов, важных для контроля промышленных и корпоративных сетей:

- Modbus RTU over TCP - к уже поддерживаемому разбору Modbus добавлена индикация его инкапсуляции внутри TCP. Наличие в сети этого варианта протокола указывает на нестандартную схему подключения АСУ ТП-оборудования и риск некорректного сегментирования сети;
- Regul - добавлен разбор команд управления Start, Stop, Load, что позволяет фиксировать в трафике операции запуска, остановки программы и загрузки программы на контроллере;
- SSDP, mDNS, LLMNR - эти протоколы обнаружения устройств злоумышленники используют для перехвата учетных данных (LLMNR/NBT-NS poisoning), а их видимость помогает найти неучтенные устройства в сети: принтеры, IoT-оборудование, медиаплееры, которые обычно не проходят инвентаризацию;
- RTSP - контроль видеопотоков, обнаружение камер и регистраторов в неожиданных сегментах сети;
- PTP - видимость трафика точной синхронизации времени в промышленных и телеком-сетях;
- Zabbix (agent, trapper) - контроль трафика систем мониторинга и выявление нелегитимных подключений под видом служебного трафика.

Скучный СТА пропустите — а вот пилотный проект новой версии пропускать не стоит

Контакты
zapros@udv.group
8-800-511-65-51

Сайт
udv.group

Телеграм
@udv_group

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

udv|group

2026