VAS Experts ITG

СКАТ AntiDDoS

- Детекция
- Митигация
- Анализ

О компании VAS Experts

VAS Experts — разработчик программного обеспечения для контроля и анализа трафика. С 2013 года мы выполнили **более 2000 инсталляций** в России и по всему миру.

Наша команда имеет **более чем 25-летний** опыт разработки программного обеспечения и обширные знания в области телеком-технологий.

20M+

абонентов

Более

35 Тбит/с

Последние инсталляции:

- Россия и СНГ
- Европа
- Ближний Восток
- Латинская Америка
- Африка
- Юго-Восточная Азия

MTS Sarkor YOTA COM GhoFi connecting people Norte CableColor SKYTiC telecom

Наши продукты

Система контроля и анализа трафика (СКАТ) — мультифункциональная платформа для управления трафиком

Для интернет-провайдеров:

DPI

Управление трафиком на основе QoS, фильтрация по белым и черным спискам

BRAS

Гибкое и масштабируемое программное решение

AntiDDoS

Защита сети оператора от злоумышленников

Модуль аналитики QoE

Сбор статистики, оценка здоровья сети и качества услуг

CG-NAT

Прозрачная трансляция сетевых адресов на стандартном x86-сервере

VEOS

Операционная система

Наши продукты

Система контроля и анализа трафика (СКАТ) — мультифункциональная платформа для управления трафиком

Для мобильных операторов:

PGW

Интеллектуальный шлюз, обеспечивающий контроль трафика в рамках архитектуры EPC

PCEF

Гибкая тарификация на основе различных условий в соответствии с требованиями PCRF

EPDG

Решение для запуска Wi-Fi Calling (VoWiFi)

Собственный DPI движок

История развития

2013 — DPI

2016 — CG-NAT

2017 — L3 BRAS Dual Stack IPv4/IPv6

2018 — COPM

2019 — L2 BRAS Dual Stack IPv4/IPv6

2020 — Поддержка мобильных сетей

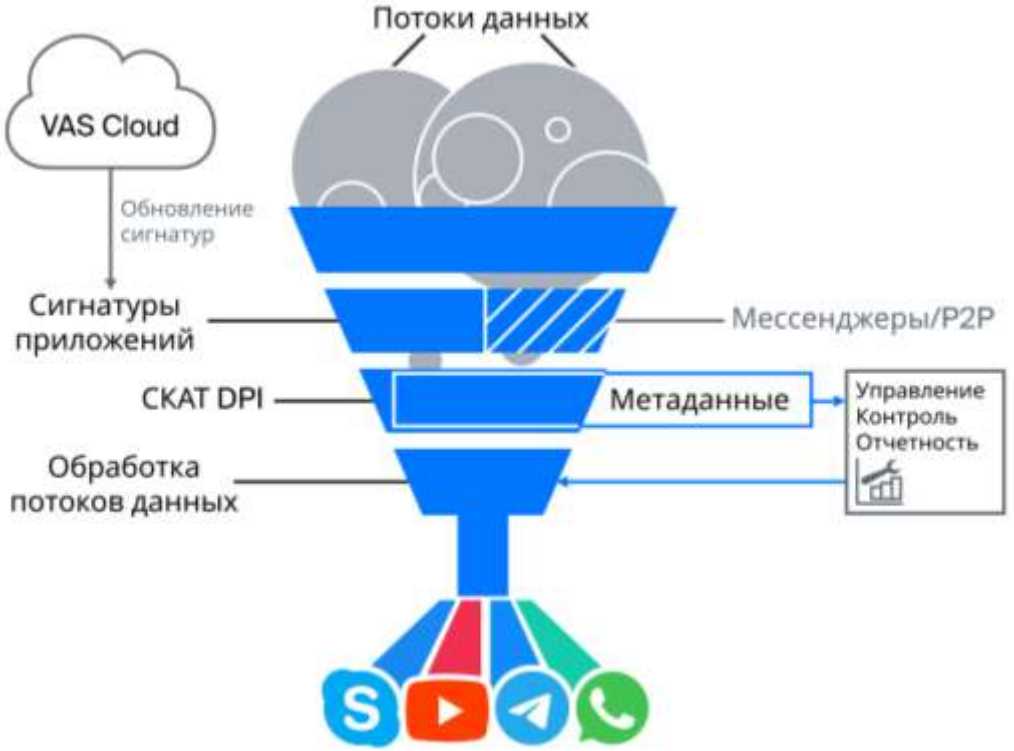
2021 — Border Router

2022 — VAS Services, LBS

2023 — VEOS, On-Stick, EPDG

2024 — PCEF, Diameter

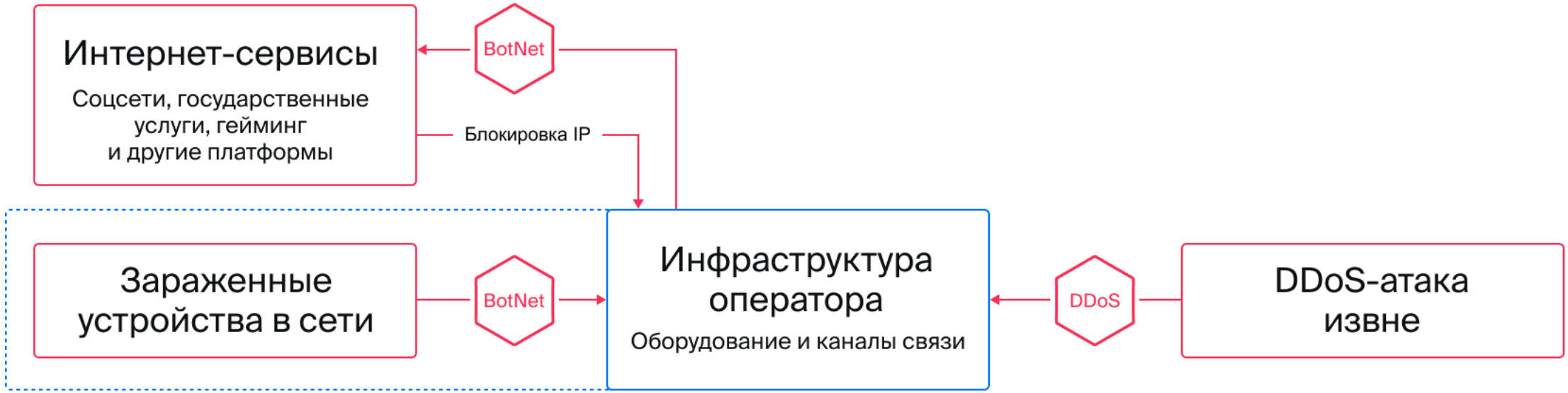
2025 — PGW, AntiDDoS



Замена решений

Sandvine	Cisco SCE	Cisco ASR	MikroTik	Ericsson SE
Allot	A10 Network	Juniper MX	Huawei NE	Nokia SR

Вызовы DDoS и BotNet для операторов



Участие в BotNet

- Повышенная нагрузка на оборудования
- Внесение публичных IP-адресов в черные списки, что влечет недоступность сервисов для абонентов

Перегрузка вышестоящего канала

- Невозможность оказывать услуги
- Жалобы абонентов и отток базы
- Финансовые и репутационные потери

Статистика DDoS-атак

2025 – рекордный год по объему и мощности DDoS-атак

47,1 миллиона DDoS-атак в 2025 году (вдвое больше, чем в 2024 году). Зафиксированный рекорд мощности – **31,4 Тбит/с;** в первом квартале – более 700 гиперобъемных атак, превышающих 1 Тбит/с (Cloudflare)

Телекоммуникации – постоянная цель атакующих

Финансовый и телекоммуникационный секторы составляют **60% всех целей в мире** (StormWall)

Рост числа атак в России и СНГ

На 83% увеличилось число DDoS-атак в первом полугодии 2025 года по сравнению с первым полугодием 2024 года (StormWall)

Проблема традиционных решений

Традиционная защита фокусируется на сервисах и сайтах

- Защищает сервисы и веб-сайты конечных пользователей
- Обеспечивает безопасность приложений, ориентированных на клиентов
- Осуществляет мониторинг структуры трафика абонентов

СКАТ AntiDDoS разработан для защиты интернет-провайдеров

- Защита входящего канала — смягчение атак до того, как они перегрузят пропускную способность сети
- Детальный анализ трафика по IPFIX fullflow обеспечивается механизмами DPI
- Детектор на основе алгоритмов машинного обучения формирует эталон здорового трафика и выявляет отклонения от нормы

Решение СКАТ AntiDDoS на базе QoE

Защита от распространённых форм атак на операторов связи

- Распределенная архитектура, обеспечивающая высокую отказоустойчивость
- Адаптивная защита и автоматическое обновление правил
- Нейросетевые алгоритмы и DPI обеспечивают глубокую аналитику трафика
- Решение гибко настраивается и поддерживает разные сценарии блокировки

Решение СКАТ AntiDDoS на базе QoE

Защита от распространённых форм атак на операторов связи

Переполнение входных каналов

- ✓ Amplification attacks (DNS, NTP, UDP flood и другие)
  Защита: blackhole атакуемых адресов или применение flowspec на аплинк канале. Другие способы защиты неэффективны
- ✓ BotNet attacks
  Защита: blackhole атакуемых адресов, flowspec на аплинк канале, создание списка адресов BotNet сети и их блокировка на СКАТ

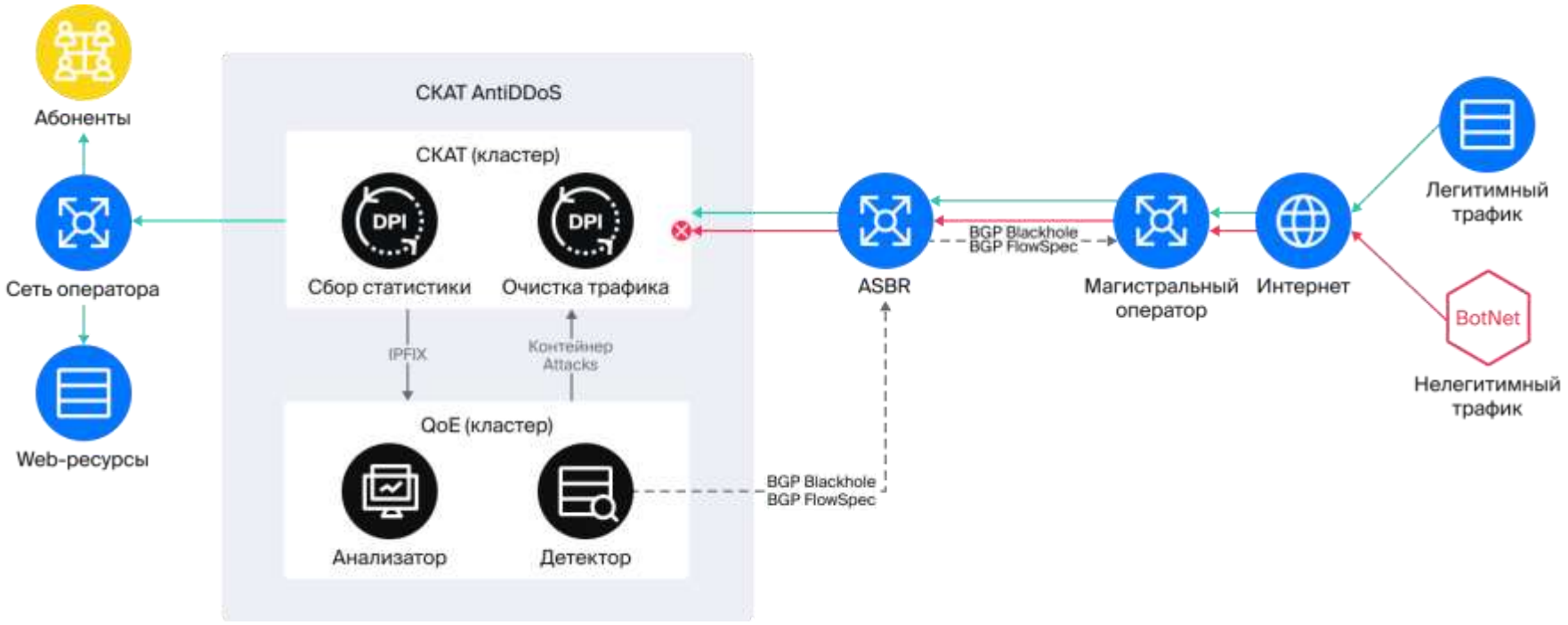
Атака высоким PPS

- ✓ Flood, SYN flood, обычно с подменой source IP
  Защита: перенаправление трафика на СКАТ для фильтрации или blackhole атакуемых адресов

Взлом элементов сети оператора

- ✓ Риск взлома определяется по сканированию сети адресов оператора
  Защита: детектирование таких сессий и их блокировка по внешнему адресу

Решение СКАТ AntiDDoS на базе QoE



Анализ

Детектирование

Очистка

Blackhole

FlowSpec

Принцип работы

1. Трафик проходит через СКАТ DPI, который направляет IPFIX Fullflow в модуль QoE для детального анализа
2. Модуль QoE создаёт эталонный профиль «здорового» трафика
3. Детектор выявляет отклонения от нормы, классифицирует угрозы и определяет их источники с помощью алгоритмов ML
4. При обнаружении атаки формируется контейнер Attacks, содержащий IP-адреса злоумышленников и используемые ими порты
5. В случае переполнения каналов применяется механизмы Blackhole и Flowspec

СКАТ DPI осуществляет очистку трафика

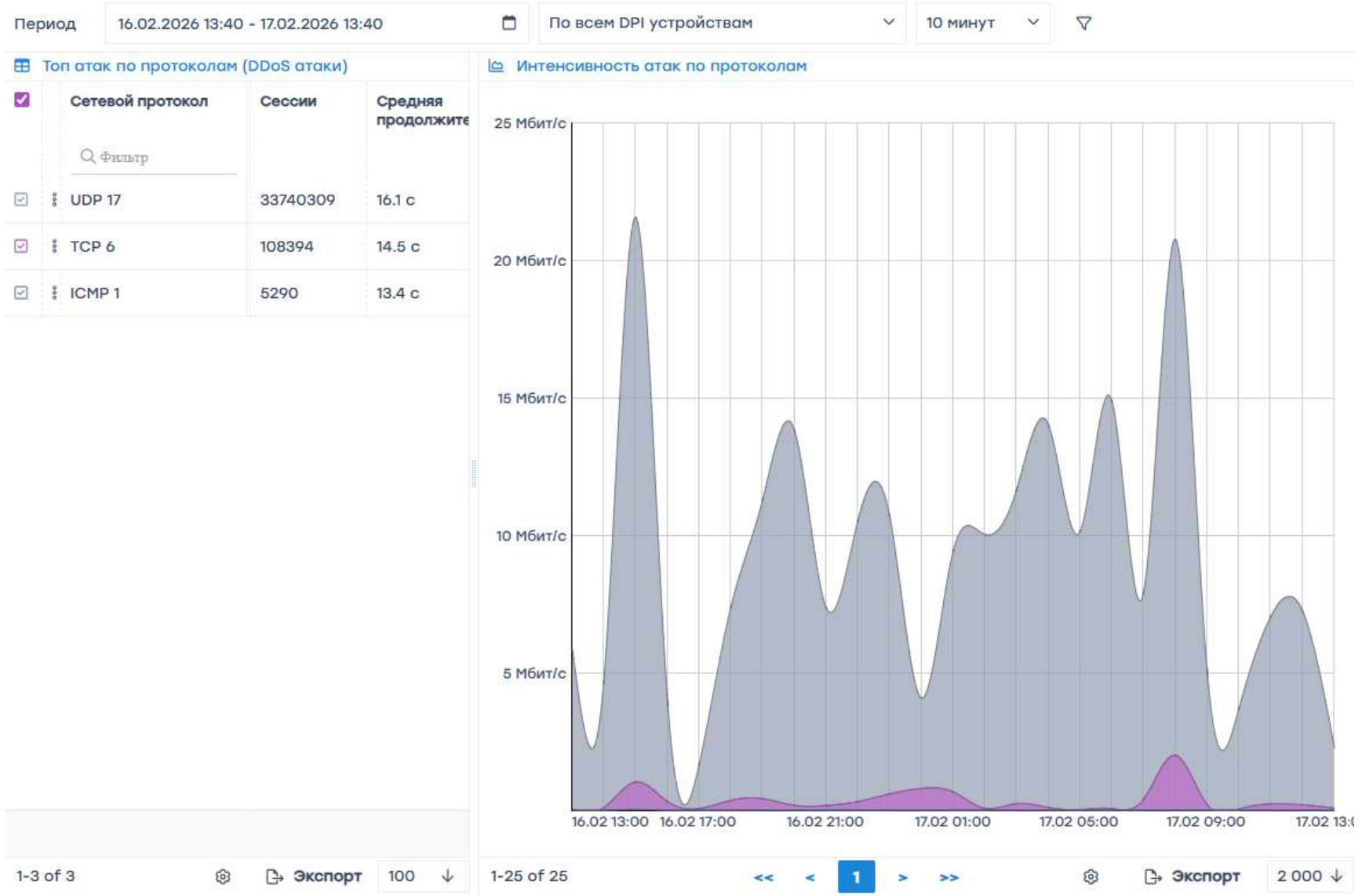
Топ DDoS-атак

Период 16.02.2026 13:42 - 17.02.2026 13:42 | По всем DPI устройствам | 10 минут

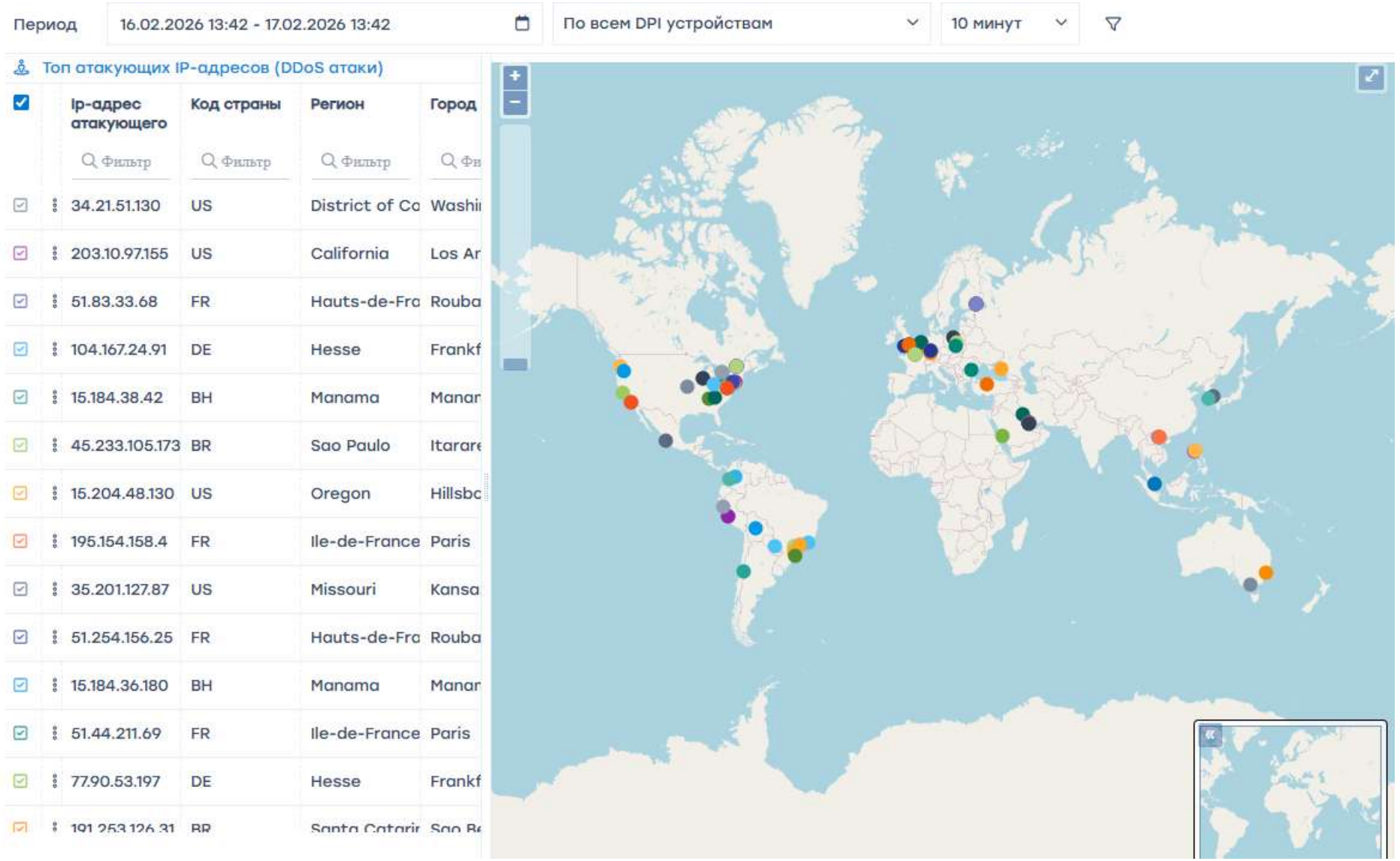
Топ атак (DDoS атаки)

IP-адрес цели	Количество атак	Количество типов атак	Сессии	Средняя продолжител	Скорость трафика	Скорость потока
Фильтр						
10.29.239.214	1	1	1845855	20.3 с	806.5 Кбит/с	183 Пак/с
10.9.98.57	1	1	1482102	15.4 с	1.8 Мбит/с	243 Пак/с
10.25.16.48	1	1	1353470	17.4 с	2.4 Мбит/с	289 Пак/с
10.25.7.247	1	1	1346479	19.4 с	1.8 Мбит/с	293 Пак/с
10.253.25.211	1	1	1289163	14.4 с	6.2 Мбит/с	690 Пак/с
10.248.70.208	1	1	849233	8.7 с	1 Мбит/с	139 Пак/с
10.9.87.239	1	1	831991	15.7 с	1.3 Мбит/с	359 Пак/с
10.138.5.221	1	1	772650	12 с	2.8 Мбит/с	298 Пак/с
10.29.234.6	1	1	772433	17.8 с	477.4 Кбит/с	52 Пак/с
10.25.244.181	1	1	754541	12.2 с	1.4 Мбит/с	176 Пак/с
10.24.233.6	1	1	701596	6.4 с	1.6 Мбит/с	525 Пак/с
10.18.161.0	1	1	675812	11.8 с	1 Мбит/с	119 Пак/с
10.3.17.239	1	1	661379	17.7 с	1.7 Мбит/с	273 Пак/с
10.31.95.216	1	1	613803	13.5 с	1.4 Мбит/с	149 Пак/с

Топ атак
по протоколам



Топ атакующих IP-адресов (локация)



Топ атак по прикладным протоколам

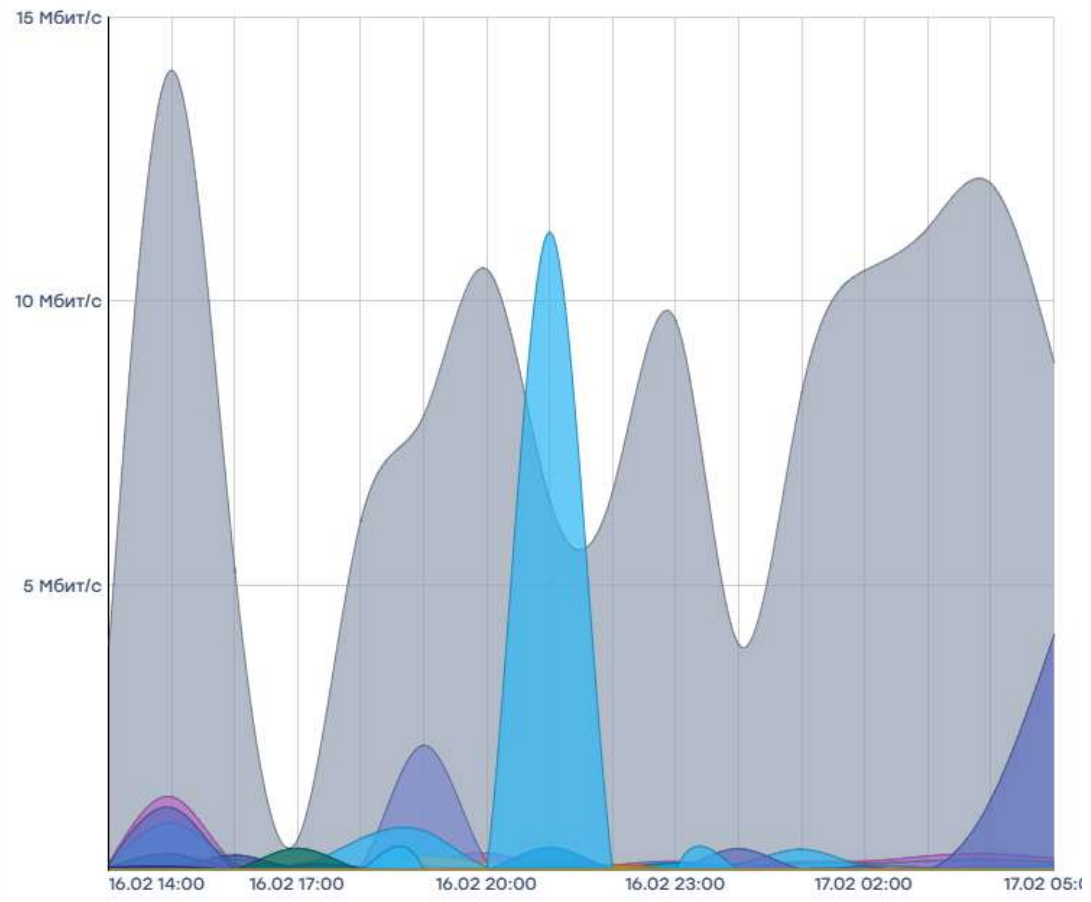
Период 16.02.2026 13:49 - 17.02.2026 13:49 | По всем DPI устройствам | 10 минут

Топ атак по прикладным протоколам (DDoS атаки)

Прикладной протокол	Сессии	Средняя продолжите
udp unknown 65041	19826612	35 с
rtp 49202	267160	3.6 с
skype 49216	185185	3.7 с
viber_vstreams 49233	92491	15.8 с
dns 53	31261	885.4 мс
tcp unknown 65030	28299	6.9 с
http 80	17015	16 с
https 443	9900	16.7 с
google_meet 49284	7817	35.3 с
ms-wbt/rdp 3389	4269	3.4 с
tiktok_cl 54351	4084	33.9 с
http-alt 591	3517	4.5 с
icmp 65025	3399	17.3 с
mysql 3306	3177	3.9 с

1-100 of 4775 | Экспорт | 100

Интенсивность атак по прикладным протоколам



1-16 of 16 | << < 1 > >> | Экспорт | 2 000

Характеристики решения

- Время реакции менее 1 минуты
- Обработка до 600 млн пакетов/сек
- Емкость фильтрации до 5 Тбит/с
- Защита от 100+ одновременных атак

Требования и начало работы

Для работы СКАТ AntiDDoS необходимы:

- QoE и GUI последней версии;
- Лицензия QoE AntiDDoS приобретается отдельной опцией;
- СКАТ лицензии BASE / COMPLETE / BRAS с опциями mark и channels;
- QoE устанавливается на отдельный сервер или виртуальную машину.

Отправьте запрос на персональную демонстрацию и тестирование решения через Личный кабинет

Контакты

dpi@vas.expert

vasexperts.ru