

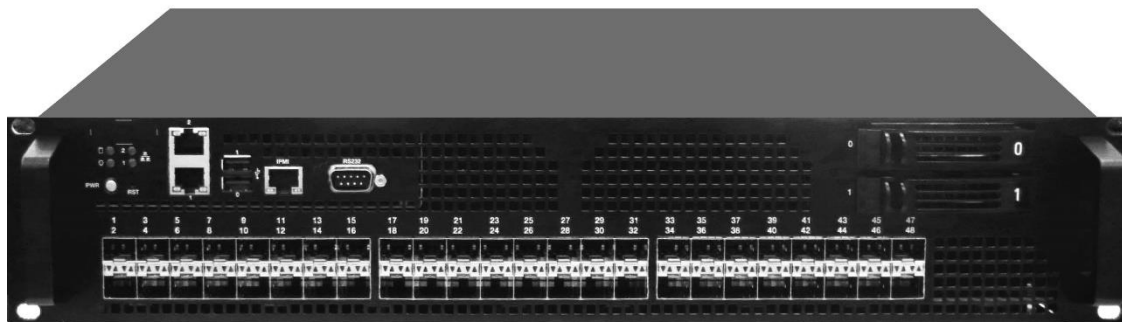
# Leo<sup>L7 DPI</sup>

## Устройство многоуровневого анализа и фильтрации трафика

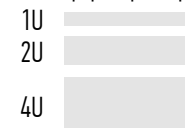
LEO – аппаратно-программный комплекс мониторинга и фильтрации IP-трафика на каналах со скоростями до 100 Гбит/сек:

- в соответствии с заданными правилами,
- в режиме реального времени,
- без потерь.

LEO используется для решения широкого спектра сетевых задач, может расширять свой функционал, масштабируясь до систем типа IPS и съёмника COPM3.



форм-фактор



## LEO эффективно решает задачи трех основных типов

Агрегация и балансировка

Анализ трафика

Фильтрация трафика

- Анализирует трафик в сети оператора:
  - выявляет узкие места, нагруженные протоколы, распределение трафика по странам и т. п.;
  - записывает данные на диск;
  - определяет часы-пик по входящему / исходящему трафику и т. д.;
  - проводит мониторинг в режиме on-line.
- Блокирует нежелательные виды трафика.
- Перенаправляет трафик на другие сетевые интерфейсы для дополнительного анализа.

⚠ Для правильной работы LEO должен в полном объеме получать пакеты, содержащие контентный трафик и служебные управляющие сообщения.

До 64 GbE портов, каждый из которых может независимо работать на приём /RX/ и передачу /TX/.

## matching / критерии для правил

критерии фильтрации	тип приложения
	геолокация
	сигнатура
	регулярные выражения
	IP-адрес, IP-IP, подсети /IP + Mask/
	порт, диапазон портов
	подсеть, подсеть-подсеть
	URL
	логин на сервере авторизации
	IMSI

## действия

блокировка	блокировка используется при установке LEO «в разрыв» для фильтрации из выходного потока нежелательных типов трафика
запись	запись определённого вида трафика в файл для дальнейшего анализа
перенаправление трафика	возможность выделить из основного потока часть трафика и отправить его в свободный сетевой интерфейс  например, для обхода фильтрации или подачи на устройство мониторинга
DocExtractor	извлечение и экспорт из потока данных документов
Traffic Shaping	ограничение полосы канала  позволяет управлять скоростью отправки пакетов в интерфейс во избежание перегрузки линка

# LEO - многофункциональный сетевой фильтр

LEO

Правила

Добавить правило | Удалить все правила

ID	Правило	Действие	Истекает	Скорость
7	<input checked="" type="checkbox"/> Логин Lanister	↓ Записать файлы: 0	05.01.2018 15:16	0 бит/с 0 %
6	<input checked="" type="checkbox"/> Порт 53	⊗ Блокировать	28.12.2017 15:14	160,4 Кбит/с < 1 %
5	<input checked="" type="checkbox"/> Сигнатура / список IP 127.0.0.1 + Challenge Handshake Authentication Protocol (0xc223)	⊗ Блокировать	30.12.2017 15:10	0 бит/с 0 %
4	<input checked="" type="checkbox"/> Сигнатура / тип трафика AVI + ESP/IPSEC 03	✓ Пропустить	07.01.2018 15:08	0 бит/с 0 %
3	<input checked="" type="checkbox"/> Страна Арулько	⊗ Перенаправить	28.12.2017 15:07	0 бит/с 0 %
1	<input type="checkbox"/> Тип трафика HTTP	DocExtractor	∞	0 бит/с 0 %
2	<input checked="" type="checkbox"/> Тип трафика WhatsApp	⊗ Блокировать ↓ Записать файлы: 0 ✓ Пропустить	31.12.2017 14:35	0 бит/с 0 %

LEO

Мониторинг

Процессор использовано 56 % температура 55 °C | Память занято 99 % 31,0 Гб из 31,3 Гб | HDD занято 37 % 41,4 Гб из 110,8 Гб | Сеть вход 376,6 Мбит/с выход 376,6 Мбит/с | Потери сетевых пакетов 0

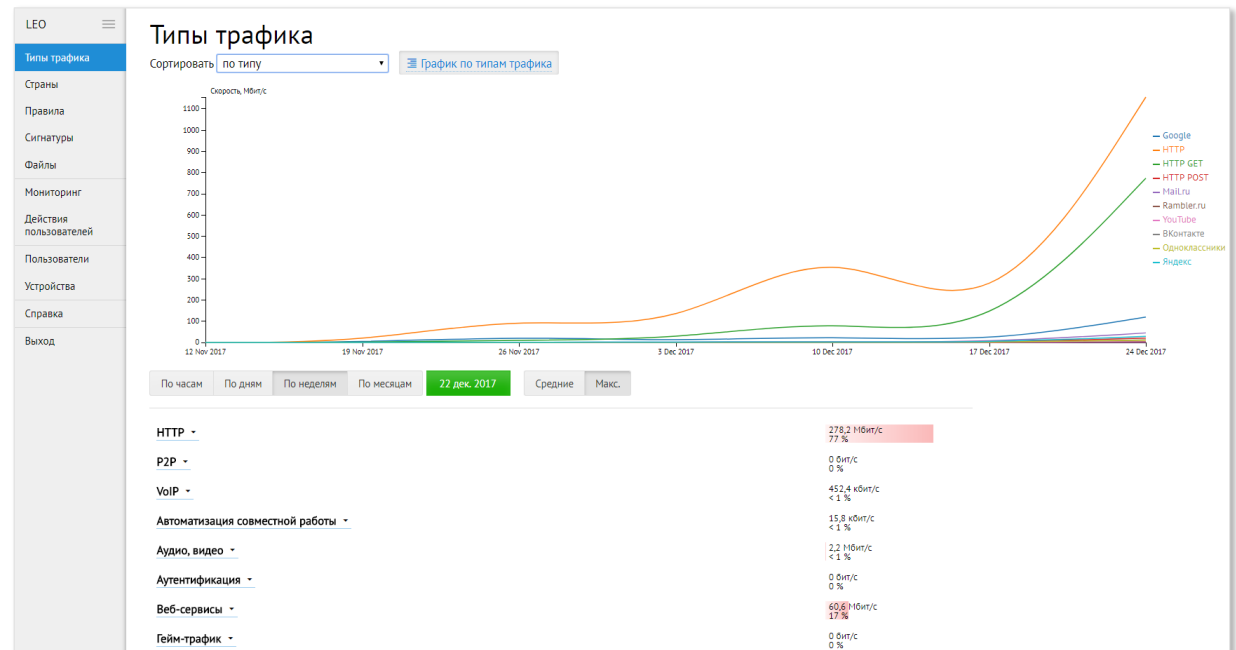
Загрузка CPU | Температура CPU | Память | HDD | Сеть | Потери

По часам | По дням | По неделям | По месяцам | ← 21 дек. | 22 дек. 2017 | Средние | Макс.

## классификатор приложений

HTTP	HTTP, HTTP ActiveSync, HTTP GET, HTTP POST, HTTP Proxy
P2P	Aimini, AppleJuice, BitTorrent, Direct Download Link, DirectConnect, Edonkey, FileTopia, Gnutella, iMESH, Kazaa/Fasttrack, OFF, OpenFT, PANDO, Soulseek, StealthNet, Thunder, WinMX
мессенджеры / VoIP	Cisco skinny, FaceTime и iMessages, H.323, IAX, MGCP, RTP, SIP, Skype, TeamSpeak, Truphone, Viber, Oscar, WathsApp, IRC, Jabber, meebo, MMS, MSN, OSCAR, Popo, QQ
автоматизация совместной работы	CitrixOnline/GoToMeeting, Lotus Notes, WebEx
аудио- и видеопотоки	Adobe Flash, Apple iTunes, AVI, Feidian, Grooveshark, Icecast, Last.fm, MPEG, Netflix, OGG, QuickTime, RealMedia, RTSP, RuTube, Spotify, WebM, Windowsmedia, YouTube
аутентификация	Kerberos, LDAP, RADIUS, XDMCP
веб-сервисы	Google, Google Maps, Mail.ru, Rambler.ru, Yahoo!, Яндекс
игровые сервисы / гейм-трафик	Armagetron, Battlefield, Crossfire, Dofus, Fiesta, Florensia, GTP, GuildWars, Halfife2, MapleStory, Quake, Steam, WARCRAFT 3, World of Kung Fu, World of Warcraft, XBOX
интернет ТВ	PPLive, PPStream, QQLive, SHOUTCast, SopCast, TVAnts, TVUplayer, VeohTV, Zattoo
корпоративные сервисы	Kontiki, SAP, Vmware

## LEO. Встроенный классификатор на 180 типов приложений



нераспознанное	TCP unknown, UDP unknown, Нераспознанное
облачные хранилища	Apple iCloud, Dropbox, Ubuntu One
почта	Gmail, IMAP, POP3, SkyFile Rudics, SkyFile постоплатный, SkyFile предоплатный, SMTP
служебные протоколы	BGP, DCE/RPC, DHCP, DHCPv6, DNS, EGP, GRE, i23v5, ICMP, ICMPv6, IGMP, IP in IP, IPP, LLMNR, MDNS, MOVE, NETBIOS, NetFlow, NOE, NTP, OSPF, PPTP, RemoteScan, SCTP, sFlow, SNMP, Socrates, SSDP, STUN, Syslog, UPnP, VRRP

социальные сети	facebook, Tuenti, Twitter, ВКонтакте, Одноклассники
СУБД	MSSQL, MySQL, Oracle, PostgreSQL, TDS
удаленный доступ	Citrix, PcAnywhere, RDP, TeamViewer, TELNET, VNC
файлы	AFP, FTP, NFS, Rsync, SMB, TFTP, Usenet, Windows Update
шифрованные протоколы	CiscoVPN, Cobra, HTTP Connect (SSL over HTTP), IPSEC, OpenVPN SSH, SSL, SSL без сертификата, Tor
классификатор может быть расширен под специфические требования заказчика	

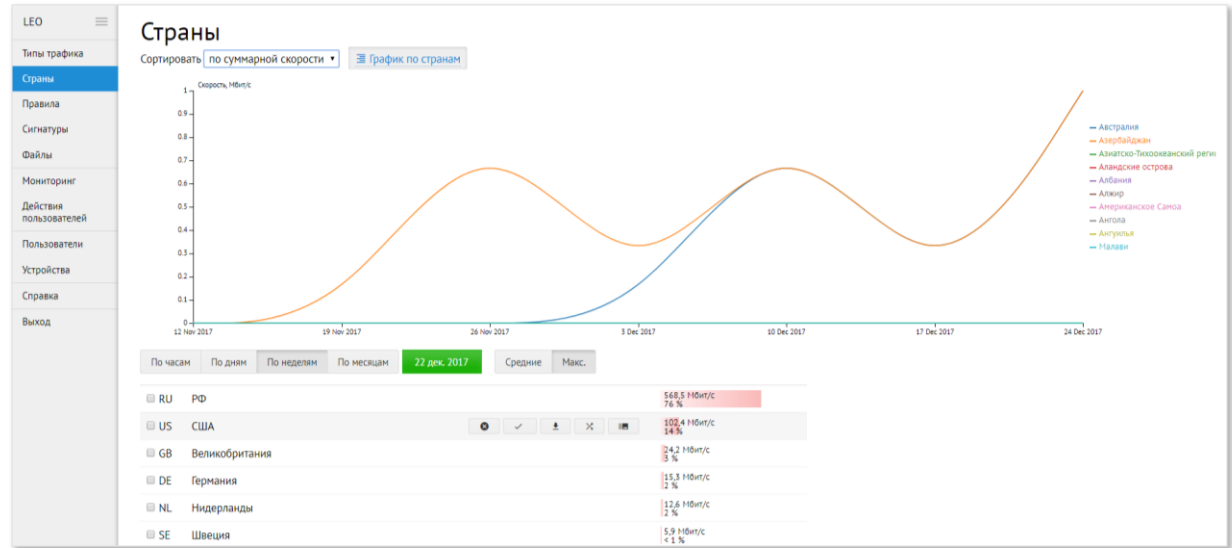
# LEO. Классификатор стран. Мониторинг и статистика

## классификатор стран

встроенный классификатор стран на основе базы данных геолокации

классификация входящего трафика на страну

классификация исходящего трафика на страну



## МОНИТОРИНГ И СТАТИСТИКА

мониторинг в реальном времени

долговременное накопление и агрегация статистики

статистика по типам трафика / странам

журнал действий пользователя

система управления правами доступа

Дата	Событие	Пользователь
22.12.2017 14:35	Создано новое правило Тип трафика WhatsApp	admin
19.12.2017 14:02	Создано новое правило Тип трафика HTTP	admin
22.12.2017 15:07	Создано новое правило Страна Арулько	supervisor
22.12.2017 15:09	Создано новое правило Сигнатура / тип трафика AVI + ESP/IPSEC 03	supervisor
22.12.2017 15:11	Создано новое правило Сигнатура / список IP 127.0.0.1/24,192.168.0.1 + ESP/IPSEC 02	supervisor
22.12.2017 15:14	Создано новое правило Порт 53	petrov
22.12.2017 15:16	Создано новое правило Логин Lanlister	petrov
22.12.2017 15:03	Создана учетная запись пользователя supervisor	admin
22.12.2017 15:13	Создана учетная запись пользователя petrov	admin
22.12.2017 15:19	Правило Тип трафика WhatsApp отредактировано	petrov
22.12.2017 15:17	Правило Тип трафика WhatsApp отредактировано	petrov
22.12.2017 15:16	Правило Тип трафика WhatsApp отредактировано	petrov
21.12.2017 19:50	Правило Тип трафика HTTP деактивировано	admin
22.12.2017 14:27	Попытка неавторизованного доступа.	nobody
21.12.2017 16:35	Попытка неавторизованного доступа.	nobody