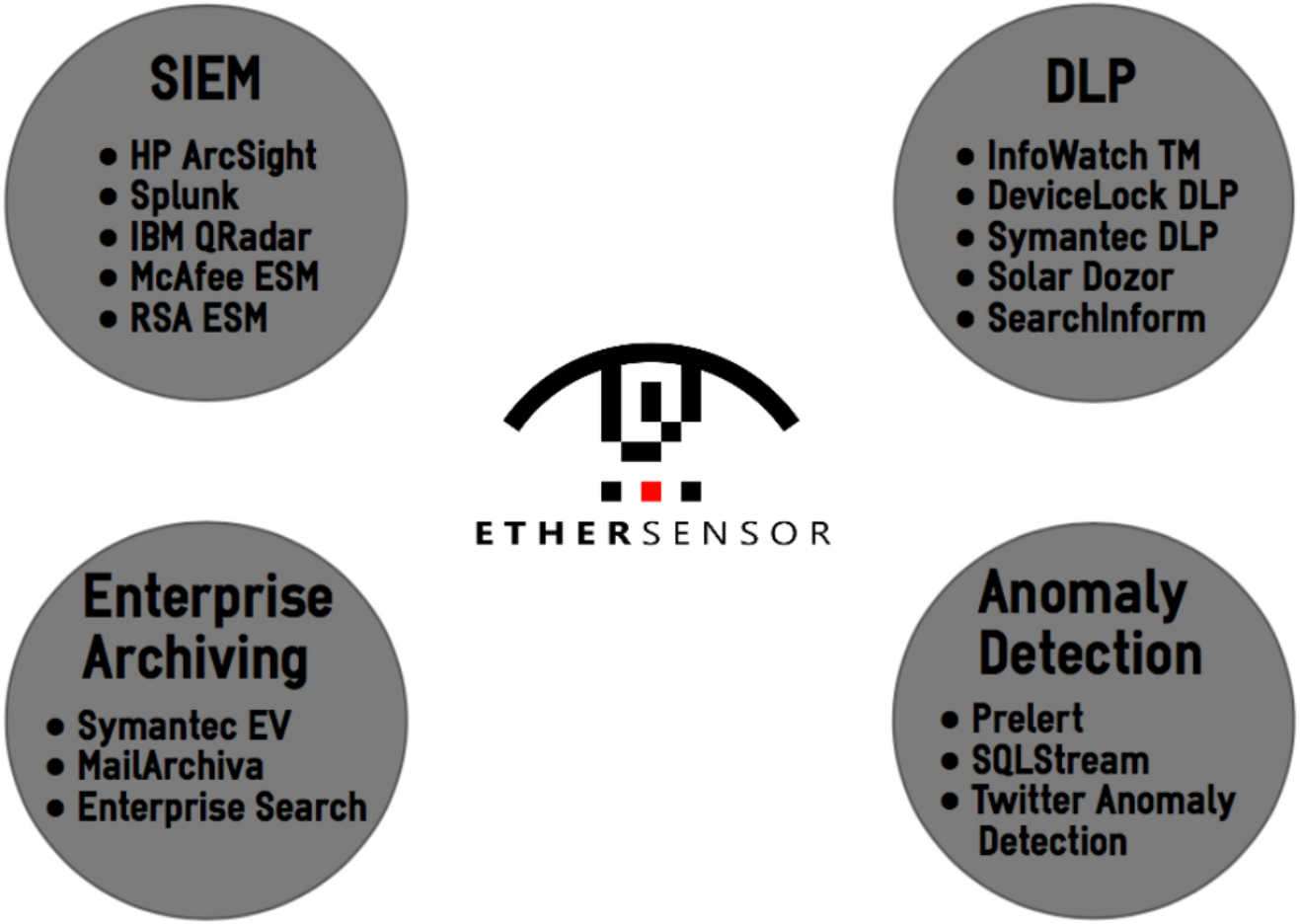
Комплекс программных продуктов Microolap для анализа сетевого трафика

Сергей Сурков
ss@microolap.ru
+7 (929) 927 3642

Распространенные задачи

- Анализ сетевого трафика в системах ИБ различных классов
- Повышение эффективности выявления утечек конфиденциальной информации
- Вскрытие SSL-трафика
- Визуализация сетевой статистики
- Анализ сетевых аномалий
- Построение аналитических отчетов

Где используется анализ сетевого трафика



EtherSensor – программная платформа анализа трафика

MICROOLAP

Принцип работы:

- **Получает** копию сетевого трафика (Mirror-порт, ICAP(S), интеграционные источники) в режиме реального времени
- **Извлекает** сообщения, метаданные, сетевые события
- **Анализирует**:
  - Пользовательские сообщения (текст)
  - Файлы (имя, тип, размер, хеш)
  - События (аутентификация, различные сетевые действия)
  - Метаданные (адресаты, IP, хосты)
- **Отправляет** результаты системам-потребителям

Потребители

- DLP – высокоуровневый анализ пользовательских событий, таких как сообщения, файлы, и другие события
- SIEM - низкоуровневый анализ и корреляция сетевых событий пользователей и систем
- eDiscovery – архивы для хранения различных данных, такие как электронная переписка, сетевые события и т.д.
- UEBA/UBA (User and Entity Behavior Analytics/User Behavior Analytics) – информация о сетевых соединениях и других событиях пользователей
- Anomaly Detection

Извлекаемые данные

MICROOLAP

Веб-почта, социальные сети, форумы

- Gmail, Mail.ru, Yandex, Yahoo, Live.com, Facebook, VK, Odnoklassniki, Сервисы поиска работы – **сотни сервисов**

Информация

- Аутентификация, регистрация
- Отправляемые сообщения и вложения
- Чтение входящих сообщений
- Списки контактов

Извлекаемые данные

MICROOLAP

Электронная почта

- Протоколы SMTP(S), POP3(S), IMAP4(S)
- Сообщения IBM Lotus Notes/Domino
- Microsoft OWA (Outlook Web Access)

Серверы электронной почты могут быть как корпоративными, так и внешними

Извлекаемые данные

MICROOLAP

Сервисы мгновенных сообщений - IM, SMS/MMS

- XMPP - Google Talk/Hangout, Yahoo …
- Microsoft Skype for Business (Lync)
- MRA - Mail.Ru Агент
- OSCAR – ICQ …
- Сервисы отправки SMS/MMS сообщений

- Обычный **Skype**
  - Без агентов, на канале

Информация

- Сообщения
- Контакт-листы
- Файлы, документы

Извлекаемые данные

MICROOLAP

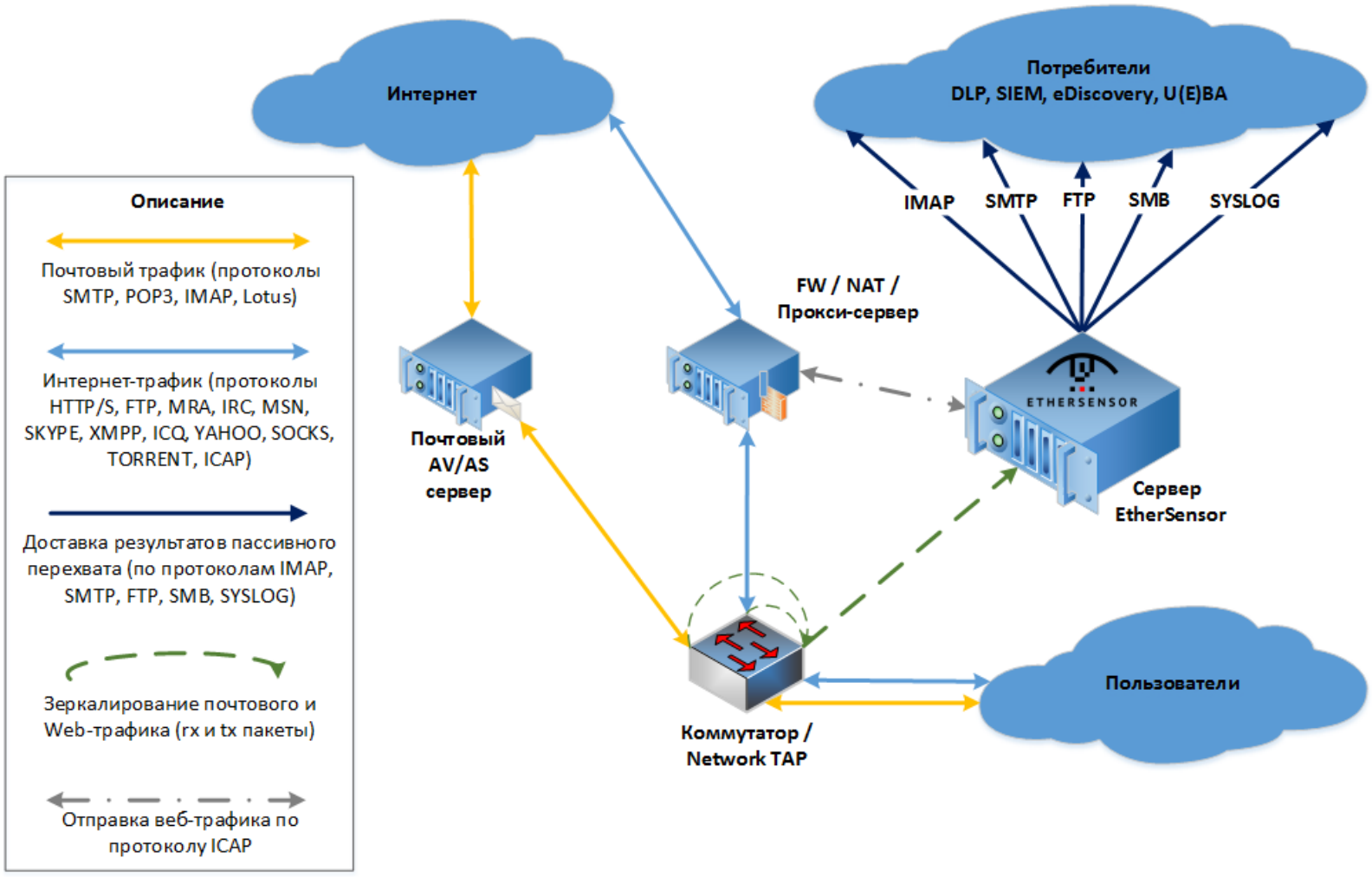
Отправка/загрузка файлов

- Через веб-браузер - HTTP(S)
- Сервис мгновенных сообщений
- Протоколов FTP(S), WebDAV(S)

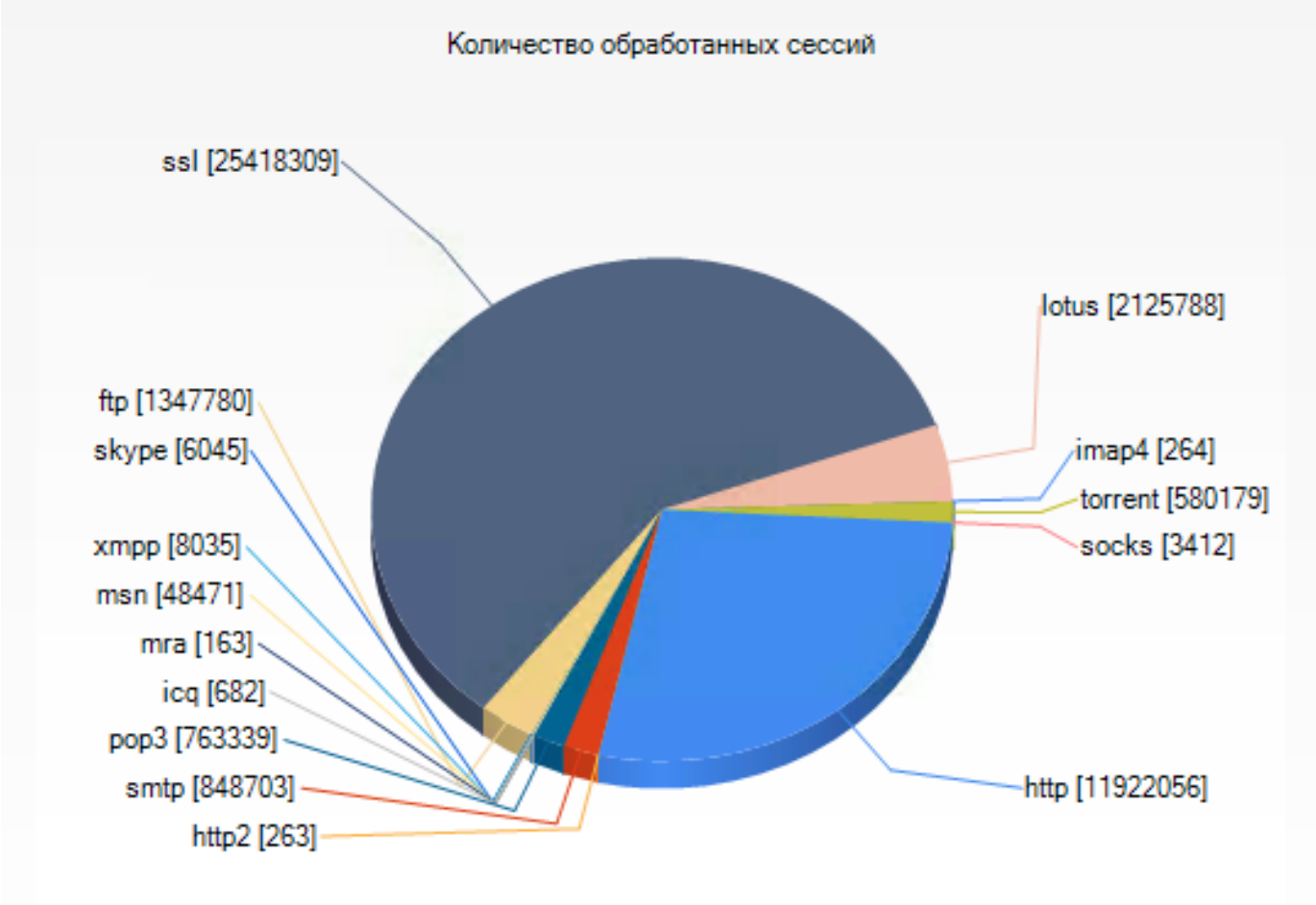
Поисковые запросы

- Google
- Yandex
- Yahoo
- Rambler
- Bing
- Wikipedia.org ...

Схема интеграции



В среднем SSL-трафик составляет от 50% до 75%



SSLSplitter

Описание:

Программное MITM-решение, расшифровывает SSL-соединения, отдает данные в Mirror-интерфейсы, подключенные к EtherSensor.

Отличия от других решений:

- Не нужно платить за неиспользуемый функционал (VPN, FW, DHCP, и т.д.)
- Не только HTTPS и FTPS, а все протоколы Over SSL
- Поддержка шифрования ГОСТ
- Поддержка TLS 1.3
- Функционирует в режимах L2 (bridge) и L3 (router)
- Проще в обслуживании

SSLSplitter

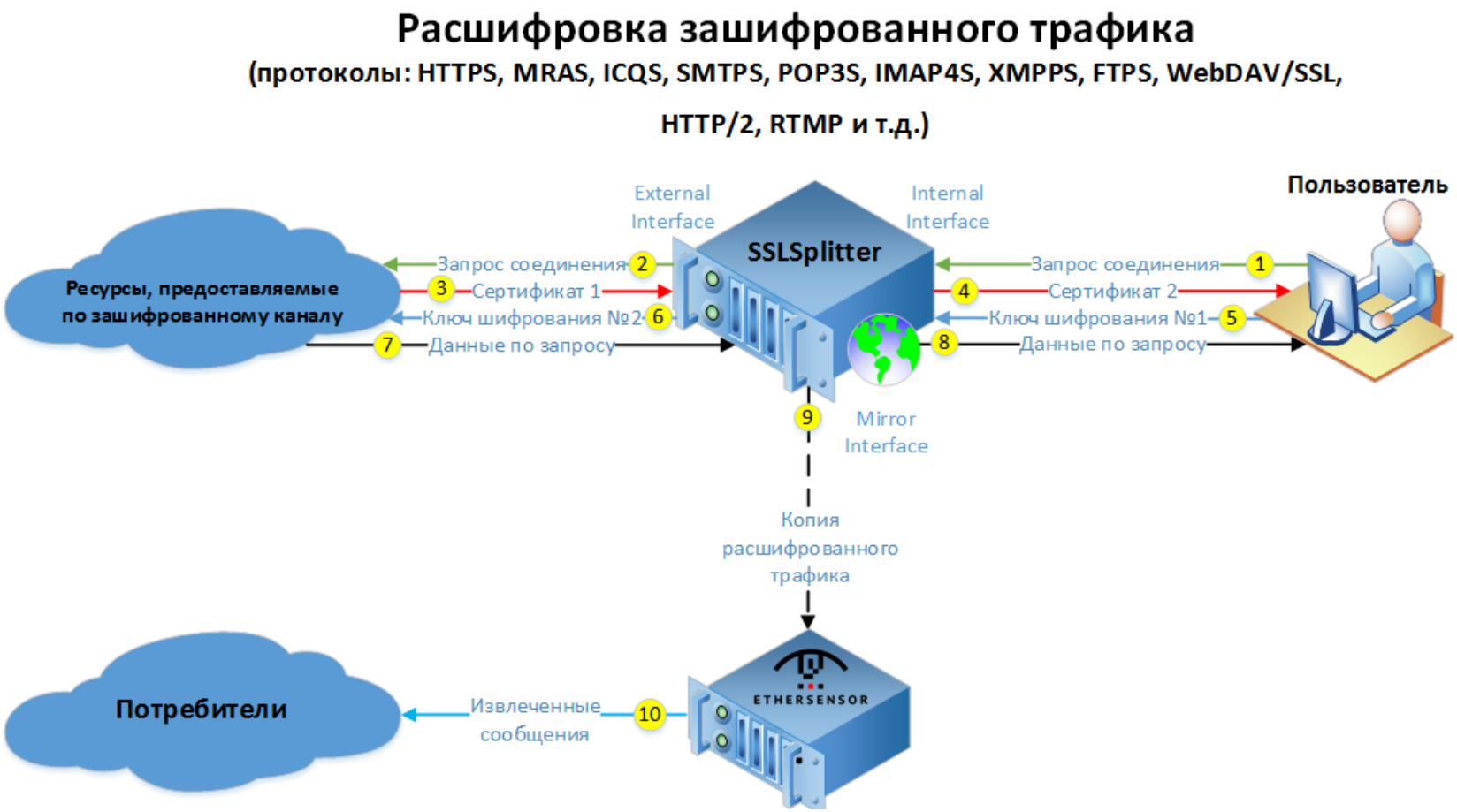
Возвращает ИБ контроль над ситуацией в организации:

- Интернет-трафик, мессенджеры, веб-почта, соц. сети, передача файлов, сетевые события и т.д.

Новые возможности анализа:

- детектирование VPN
- Skype на канале
- облачные хранилища
- SIP
- детекторы сервисов удаленного управления

Схема работы SSLSplitter



EtherStat

Программная система хранения и анализа статистики, генерируемой платформой **EtherSensor**.

Основное назначение системы – хранение, обработка, анализ и построение отчетности о деятельности пользователей в корпоративной сети.

EtherStat

Возможности:

- Мониторинг сетевой активности
- Привязка сетевого трафика к конкретным пользователям и их устройствам
- Выявление несанкционированных действий в сети
- Предоставление дополнительной информации о событиях
- Формирование отчетов о сетевых событиях

EtherStat

MICROOLAP

Позволяет строить отчеты следующих типов:

- топ самых активных пользователей
- топ посещаемых веб-доменов с возможностью углубления до конкретных веб-сервисов
- разбивка сетевого трафика по категориям (при интеграции с категоризатором)
- новые устройства в сети за период
- хосты, с которых работает множество пользователей (помогает находить в сети несанкционированно установленные коммутаторы и Wi-Fi точки доступа)
- история изменений в Active Directory
- проблемы в структуре Active Directory
- поиск по тексту поисковых запросов
- поиск по посещаемым URL (помогает осуществить отслеживание прохождения документов в сети Интернет при поиске инсайдеров)

EtherStat

Принцип работы:

1. Получает статистику о TCP-соединениях, веб-запросах и поисковых запросах пользователей
2. Сохраняет данные в БД
3. Определяет устройство и пользователя, сгенерировавших трафик
4. На основании полученных данных строятся различные отчеты, позволяющие определить сетевую активность пользователей и их устройств
5. Интегрируется со сторонними системами для получения дополнительной информации о событиях

EtherStat

Обогащение данных:

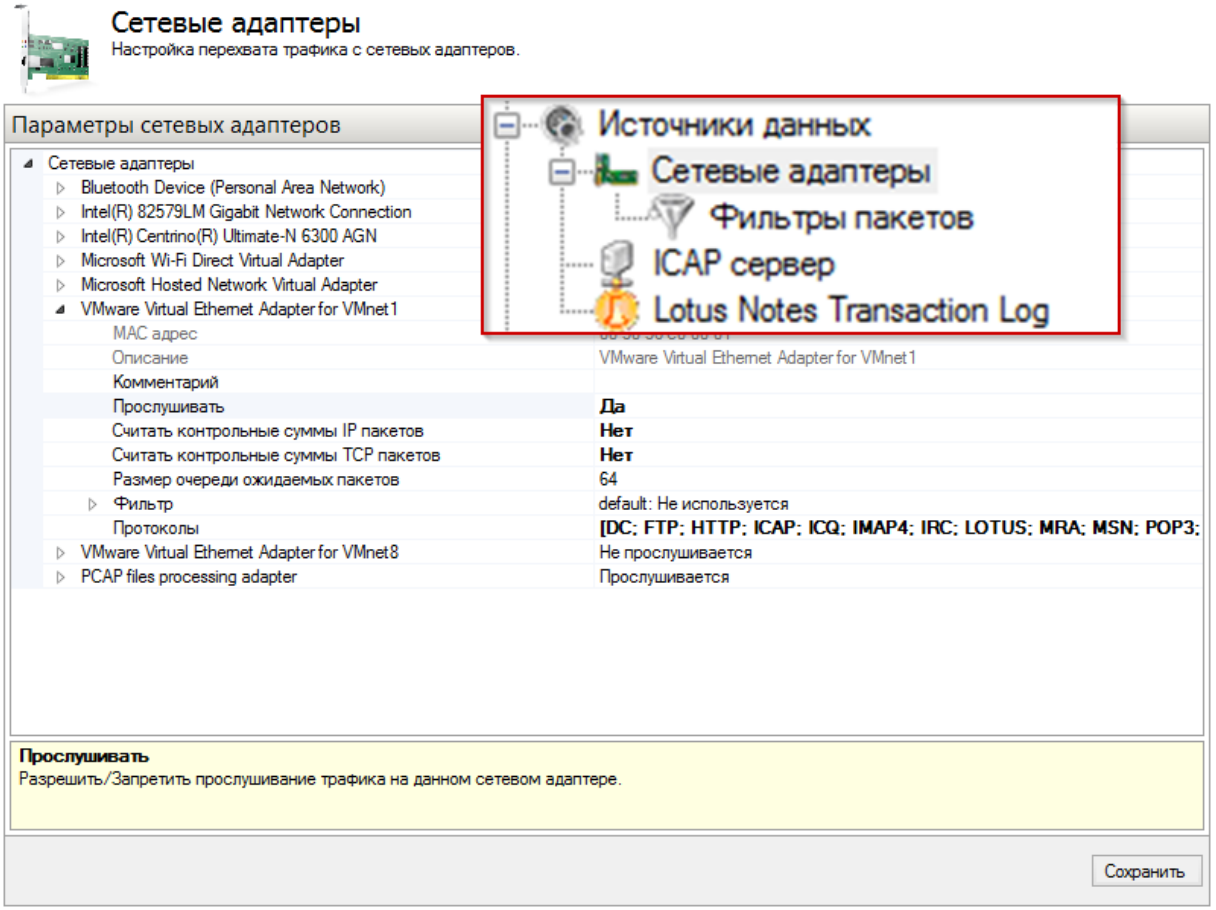
- Active Directory
- DHCP-журналы
- Windows Logs (Security)
- Категоризаторы (Entensys, SimilarWeb, …)

В будущей версии (июнь 2017):

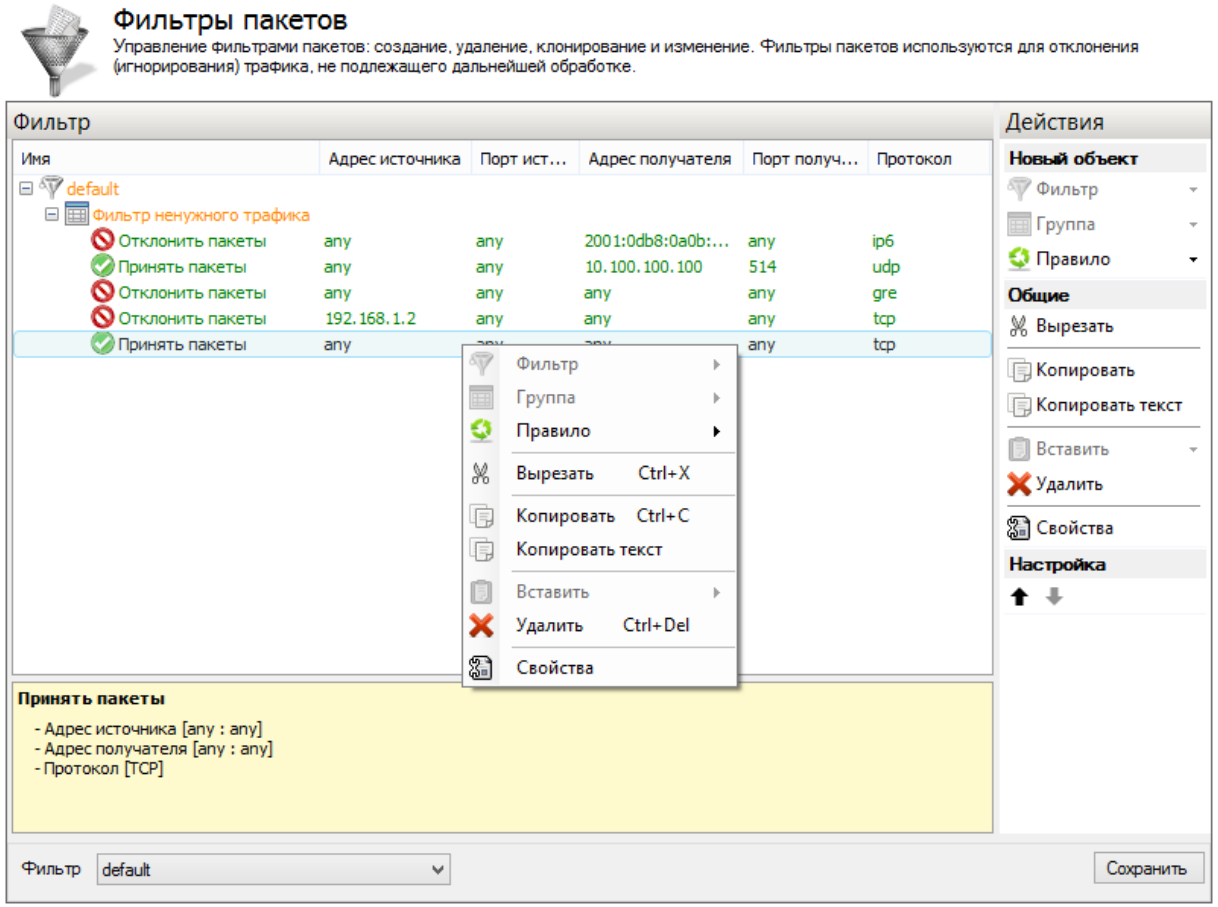
- Внешние источники (IBM X-Force Exchange)
- NMAP-сканирование сети
- Агенты Microolap

Скриншоты

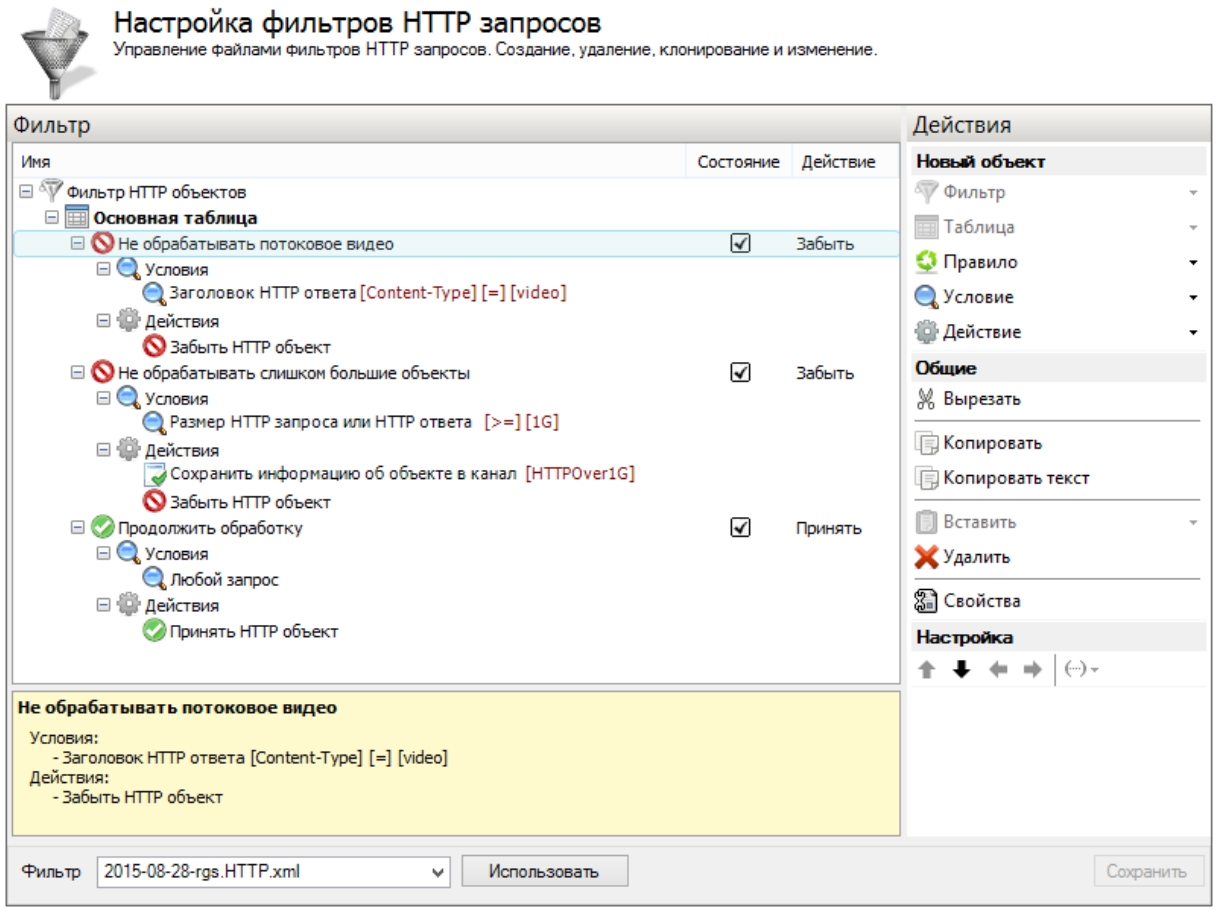
EtherSensor: Источники данных



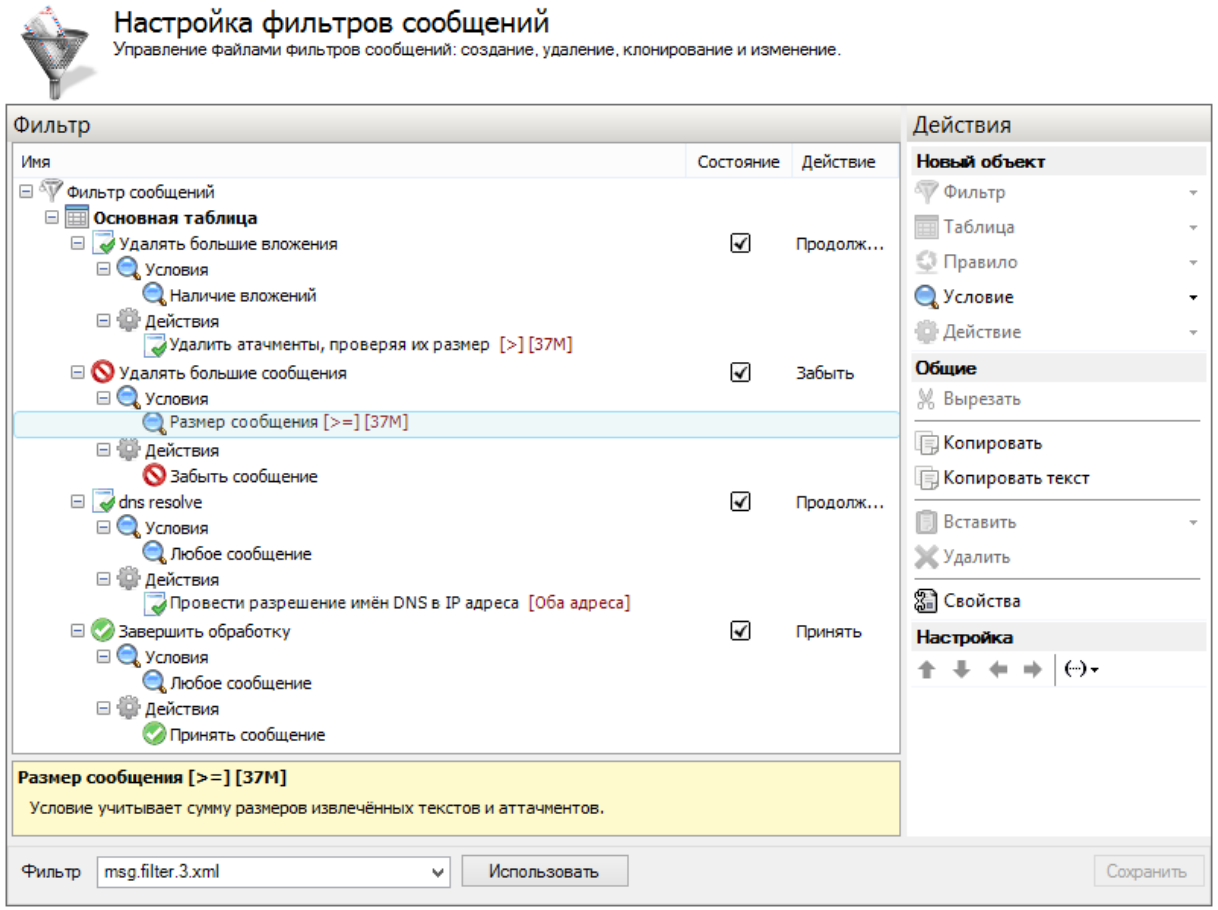
EtherSensor: BPF-фильтрация



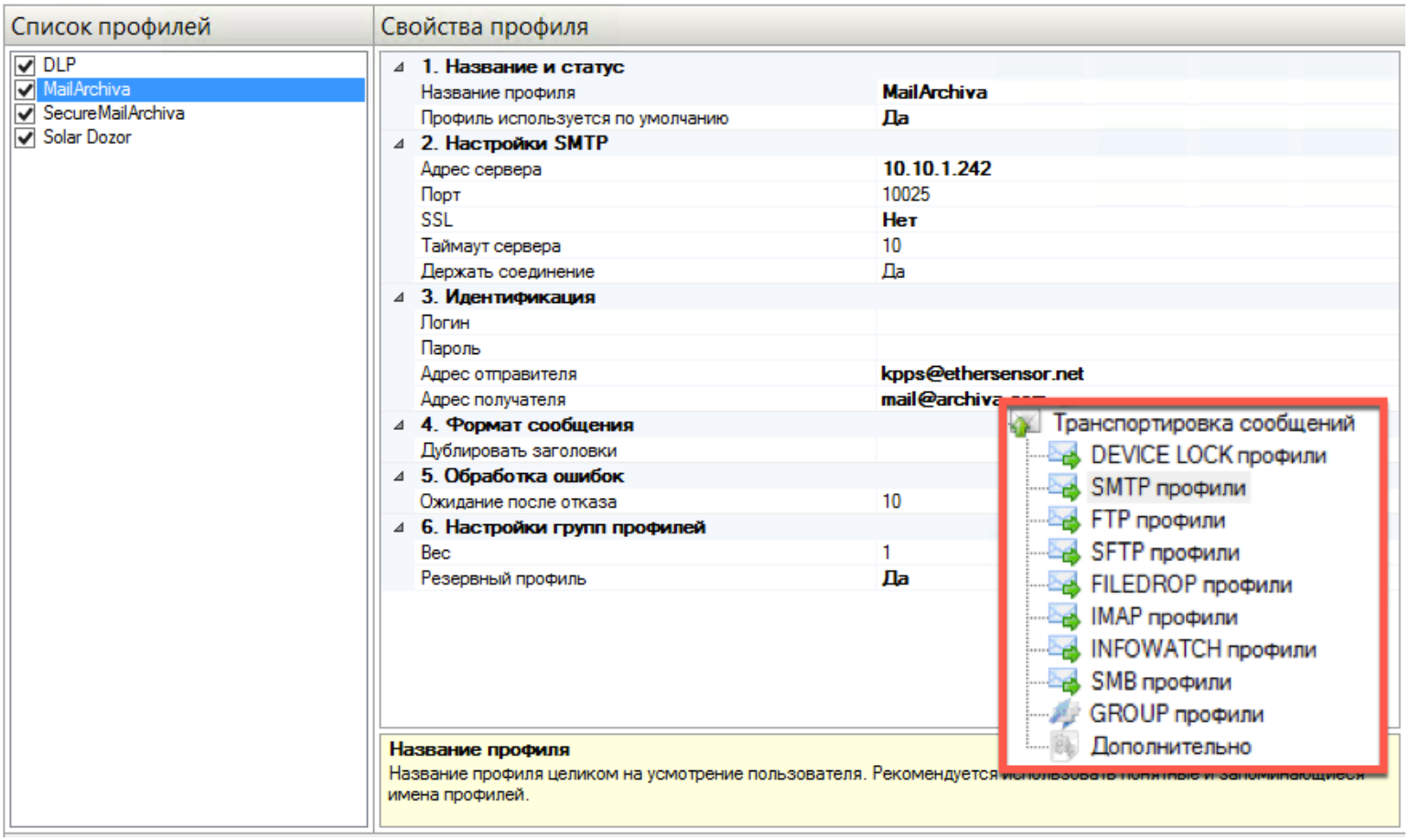
EtherSensor: HTTP-фильтрация



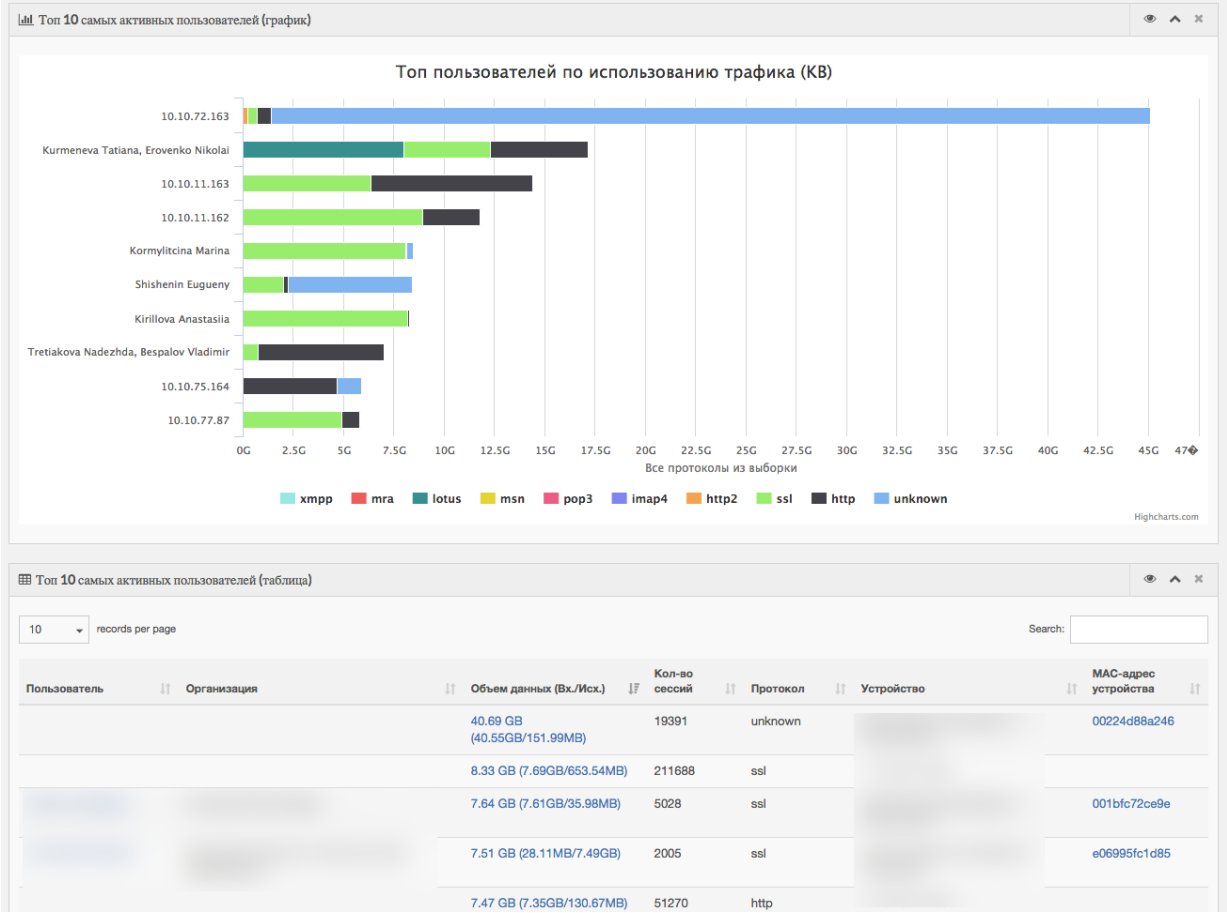
EtherSensor: Фильтры сообщений



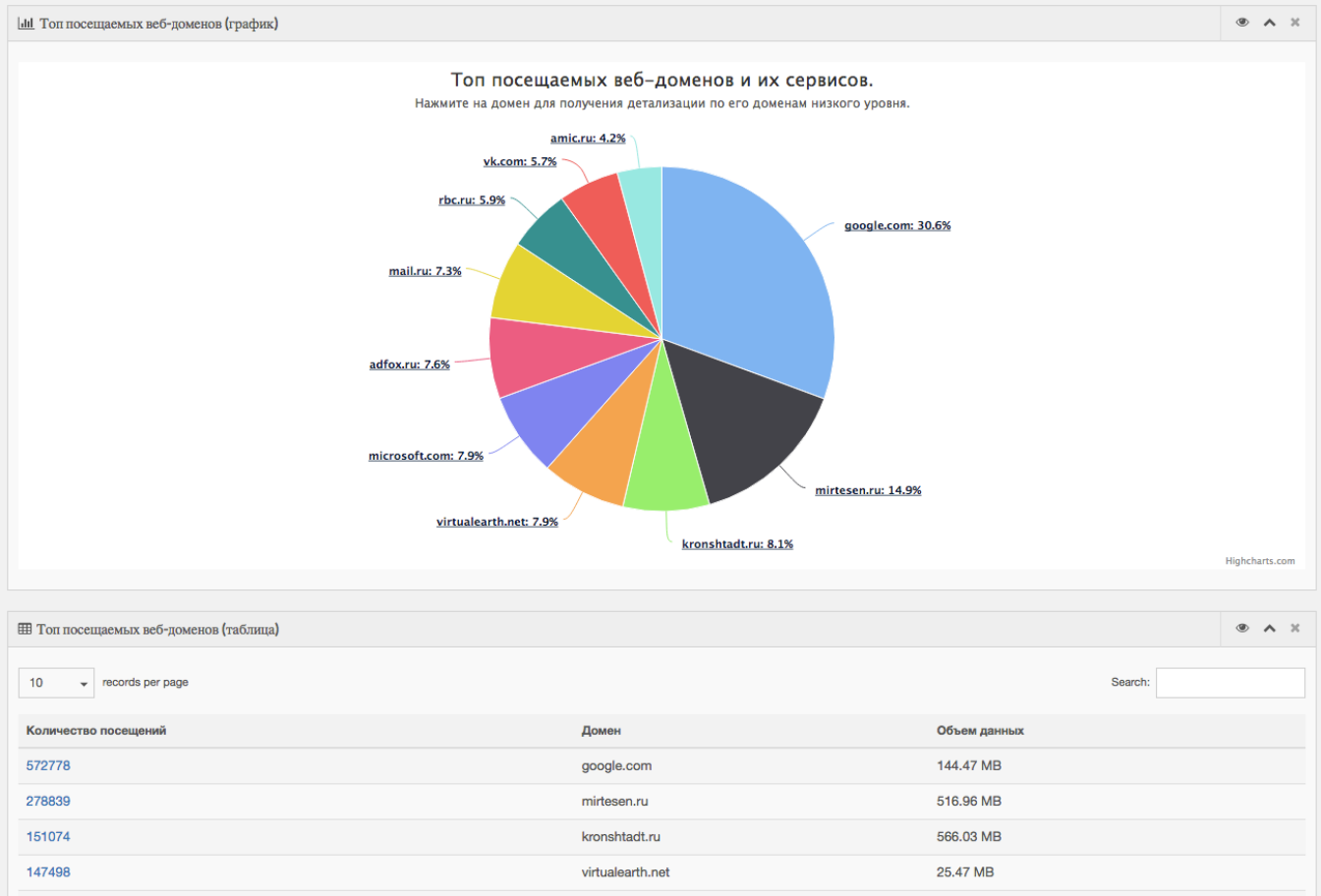
EtherSensor: Транспорт результатов



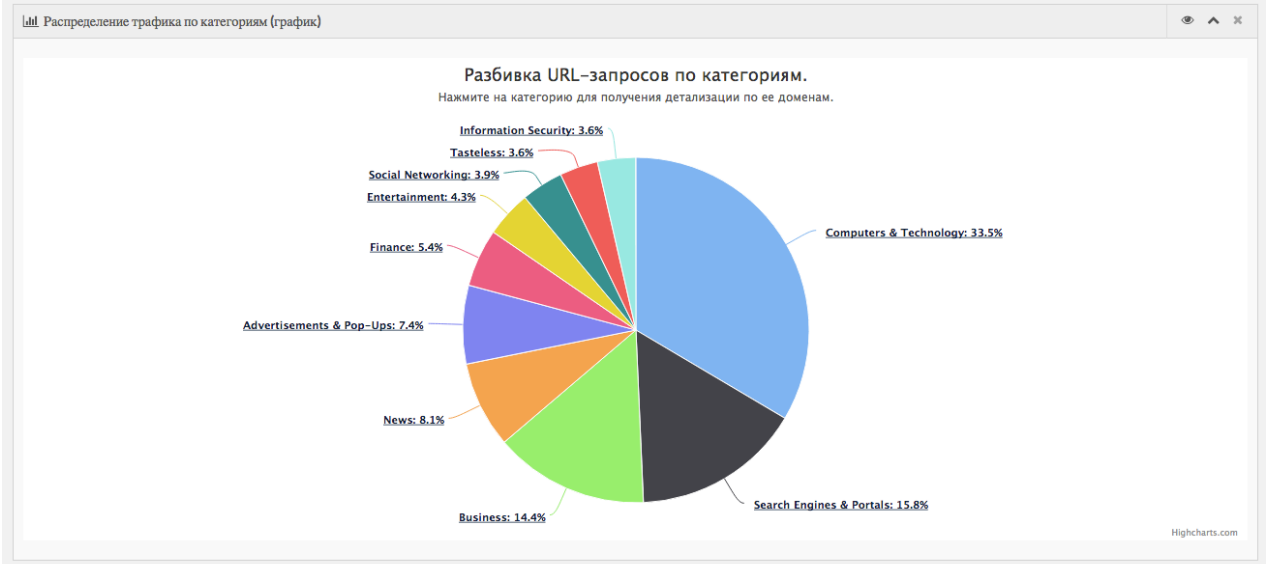
EtherStat: Отчет об использовании трафика



EtherStat: Топ посещаемых веб-доменов



EtherStat: Топ посещаемых категорий веб-доменов

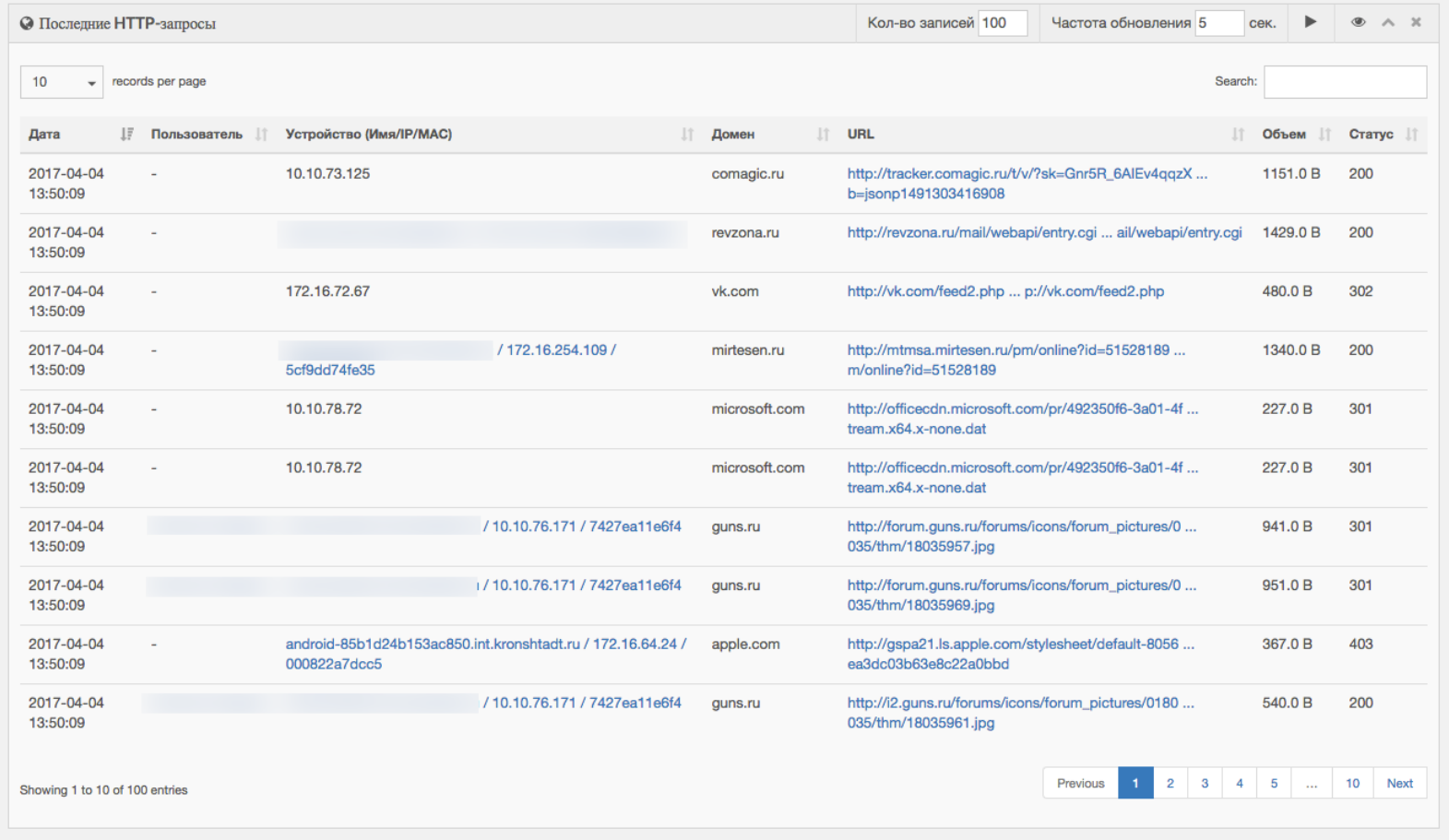


Распределение трафика по категориям (таблица)

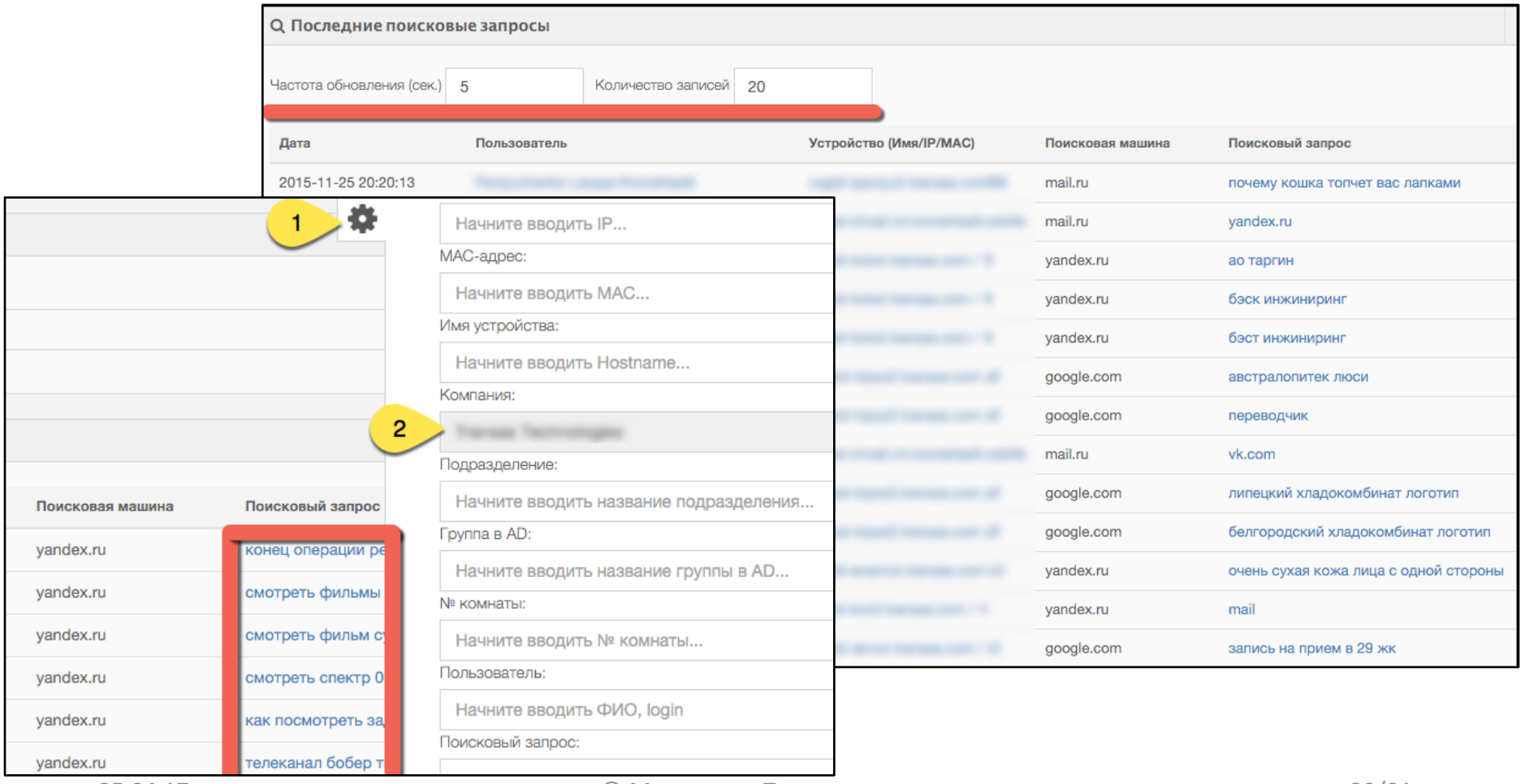
10 records per page Search:

Количество посещений	Домен	Объем данных
629253	Computers & Technology	589.59 MB
296089	Search Engines & Portals	290.27 MB
270869	Business	427.6 MB
151621	News	120.17 MB
137912	Advertisements & Pop-Ups	136.67 MB
101746	Finance	82.45 MB

EtherStat: Мониторинг веб-запросов



EtherStat: Мониторинг поисковых запросов



Спасибо!

Сергей Сурков

ss@microolap.ru

Будем рады Вашим вопросам!

+7 (929) 927 36 42