

УТВЕРЖДЕН

18678659.00001-03 34 02-ЛУ

**ПРОГРАММНЫЙ КОМПЛЕКС
РЕТРОСПЕКТИВНОГО АНАЛИЗА СЕТЕВОГО ТРАФИКА
«СТЕТОСКОП» ВЕРСИИ 3.0**

Руководство оператора

18678659.00001-03 34 02

2022 г.

АННОТАЦИЯ

Настоящий документ является руководством оператора 18678659.00001-03 34 01 программного комплекса ретроспективного анализа сетевого трафика «Стетоскоп» версии 3.0, обозначаемый 18678659.00001-03 (далее - ПК Стетоскоп).

В руководстве описываются интерфейсы оператора по работе с ПК Стетоскоп с указанием их назначения, указываются действия оператора по работе с программным обеспечением и сообщения оператору. Описывается управление через встроенное WEB-приложение. Описываются форматы сообщений и управление службами захвата трафика, индексации и анализа.

Все права защищены. Полное или частичное копирование материалов без письменного согласования с ООО "ЦСС-Безопасность" запрещено.

СОДЕРЖАНИЕ

1. Общие сведения.....	4
1.1. Область применения.....	4
1.2. Назначение	4
1.3. Состав ПК Стетоскоп	4
2. Общие принципы работы ПК Стетоскоп	6
2.1. Общие положения.....	6
2.2. Условия выполнения ПК Стетоскоп.....	10
3. WEB-приложение	12
3.1. Общие сведения.....	12
3.2. Список интерфейсов.....	17
3.3. Дашборд статистики трафика	18
3.4. Список сессий статистики трафика	20
4. Политики анализа потоков сетевого трафика	Ошибка! Закладка не определена.
4.1. Типы анализаторов	Ошибка! Закладка не определена.
4.2. Формат и параметры политик анализаторов	Ошибка! Закладка не определена.
4.3. Формат и параметры событий ИБ анализаторов	Ошибка! Закладка не определена.
5. Сообщения оператору	Ошибка! Закладка не определена.
6. Сценарии использования	Ошибка! Закладка не определена.
Термины и определения	Ошибка! Закладка не определена.
Перечень принятых сокращений	28

1. Общие сведения

Настоящее руководство разработано в соответствии с ГОСТ 19.505-79 ЕСПД и распространяется на комплекс программных средств ретроспективного анализа сетевого трафика «Стетоскоп» версии 3, обозначаемого 18678659.00001-03.

1.1. Область применения

Областью применения ПК Стетоскоп является мониторинг сетевых потоков между компонентами информационных систем (далее – ИС) и сетью Интернет.

1.2. Назначение

ПК Стетоскоп, предустановленный на аппаратную платформу или гостевую виртуальную машину, образующий аппаратно-программный комплекс (далее – АПК), является системой мониторинга и анализа потоков сетевого трафика взаимодействия компонентов ИС Организации между собой и сетью Интернет. ПК Стетоскоп предназначен для захвата, записи и индексации потоков сетевого трафика, анализа передаваемых по сети данных с целью выявления атак и аномалий, сбора и визуализации статистики сетевых сессий и передаваемых данных, выявление используемых сетевых протоколов, форматов и служб, определение географической принадлежности IP-адресов сети Интернет и DNS-имен, взаимодействующих сетевых субъектов, экспорта по требованию оператора образцов сетевого трафика и перенаправления сетевого трафика на внешние анализаторы, перенаправление системных событий и событий информационной безопасности (далее – событий ИБ) на внешние системы анализа событий ИБ, системы мониторинга и управления ИБ и SIEM-системы.

1.3. Состав ПК Стетоскоп

В состав ПК Стетоскоп входят следующие программные средства (далее по тексту – ПС):

- ПС «Дампер»;
- ПС «Индексатор»;
- ПС «Клиент»;
- ПС «Ротатор»;
- ПС «База данных» (далее по тексту – ПС «БД»).

ПС «Дампер» предназначено для гарантированного захвата сетевых пакетов на скорости до 20 Гбит/с, записи их на диск и передачи для дальнейшей обработки ПС «Индексатор».

ПС «Индексатор» предназначено для обработки сетевых пакетов на скорости до 20 Гбит/с в режиме близком к реальному времени, записи информации о них в ПС «БД» и передачи информации о потоках сетевого трафика на дальнейшую обработку в ПС «Анализатор».

Обработка сетевых пакетов включает в себя следующие операции:

- объединение (склейка) сетевых пакетов в сетевые сессии;
- индексация сетевых пакетов и сетевых сессий по множественным атрибутам;
- расчет сетевой статистики по пакетам и сессиям;
- выявление протоколов, форматов и служб;
- определение географической принадлежности и DNS-имен по IP-адресам взаимодействующих сетевых субъектов;
- выявление отклонений от стандартов обмена (RFC) в обнаруженных сетевых протоколах.

ПС «Анализатор» предназначено для выполнения поиска по заданным правилам атак и аномалий в сетевом трафике различными методами, в том числе методами с применением машинного обучения. ПС «Анализатор», получая данные от ПС «Индексатор» и от ПС «БД» выполняет следующие виды анализа:

- анализ статистики трафика на предмет превышения порогов по различным метрикам и группировкам;
- анализ сетевых субъектов по IP-адресам или DNS-именам на

предмет их вхождения в особые («плохие») списки;

- Выявление запрещенных протоколов или выявление новых протоколов для контролируемой ИС;
- Выявление запрещенных или новых для контролируемой ИС серверных сетевых портов;
- Выявление новых IP-адресов для контролируемой ИС;

ПС «Клиент» предназначено для предоставления оператору средств управления и мониторинга работой ПК Стетоскоп и решения операторских задач по мониторингу трафика и событий ИБ.

ПС «БД» предназначена для хранения и выдачи по запросу образцов трафика, статистики трафика, посчитанной по записанным образцам трафика, системных событий, генерируемых ПС в процессе работы, и событий ИБ, генерируемых ПС «Анализатор» на основании заданных правил анализа.

ПС «Ротатор» предназначено для выполнения в автоматическом режиме задач управления свободным местом дискового пространства АПК. По заранее заданным конфигурационным параметрам ПС «Ротатор» на регулярной основе следит за оставшимся свободным местом и обеспечивает бесперебойную работу ПК Стетоскоп в режиме 24/7 без необходимости обслуживания АПК персоналом путем ротации и архивации накопленных данных.

2. Общие принципы работы ПК Стетоскоп

2.1. Общие положения

Исходными данными для ПК Стетоскоп являются потоки сетевого трафика. ПК Стетоскоп выполняет обработку потоков сетевого трафика путем индексации и анализа. Для решения задач индексации и анализа потоки сетевого трафика должны быть записаны в формате PCAP.

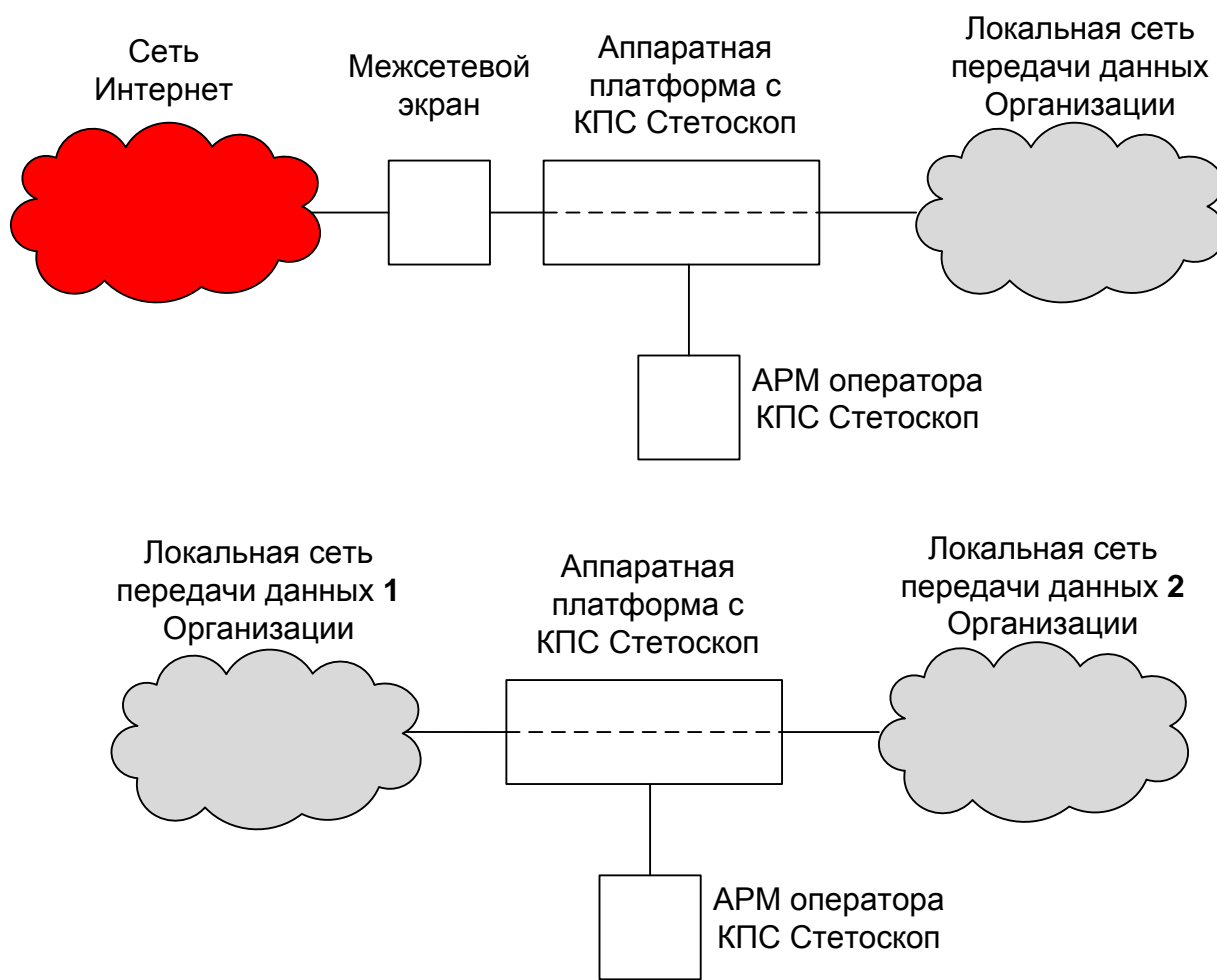
ПК Стетоскоп обладает собственным функционалом захвата и записи потоков сетевого трафика в формате PCAP. Для захвата потоков сетевого

трафика необходимо интегрировать АПК в действующую сеть передачи данных контролируемой ИС Организации. Для этого предусмотрены два режима встраивания: режим «мост» и режим «ответвитель».

Режим «мост» подразумевает встраивание АПК в разрыв действующей линии передачи данных контролируемой ИС Организации. В этом режиме используется два сетевых интерфейса АПК, которые разрывают действующую линию связи, и выполняется настройка АПК по пробросу (перекладыванию) входящих пакетов из одного интерфейса в другой. Типовая схема включения в режиме «мост» подразумевает установку АПК либо между двумя локальными сегментами сети передачи данных Организации, либо между локальным сегментом и сетью Интернет.

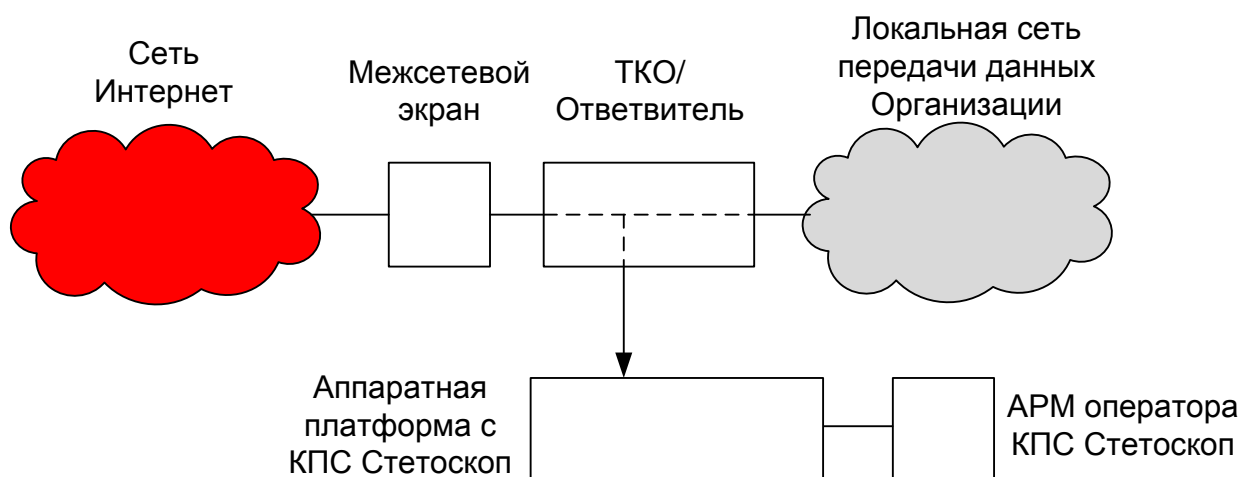
В процессе проброса сетевых пакетов между двумя сетевыми интерфейсами АПК, их копии захватываются ПК Стетоскоп и записываются на локальный диск АПК с последующим анализом. Данный режим при штатной работе АПК не оказывает влияние на линию связи, в которую он встроен. Для обеспечения отказоустойчивости линии связи к возможным аппаратным и/или программным сбоям АПК рекомендуется применять сетевые платы с функцией bypass. Пример встраивания АПК в действующую линию связи в режиме «мост» представлен на рисунке 1.

Рисунок 1. Схема применения режима встраивания «мост».



Режим «ответвитель» подразумевает встраивание АПК либо через устройство ответвления трафика (ТАР), либо через подключение к порту зеркалирования (port mirroring или span-порт) сетевого трафика используемого телекоммуникационного оборудования (далее – ТКО). В этом режиме ПК Стетоскоп захватывает копии сетевых пакетов, записывает их на локальный диск АПК с последующим анализом, не разрывая линию связи, а получая их с ТАР-устройства или с порта зеркалирования ТКО. В режиме «ответвитель» АПК Стетоскоп может захватывать сетевые потоки циркулирующие между двумя локальными сегментами сети передачи данных Организации, между локальным сегментом и сетью Интернет или между локальными узлами ИС Организации.

Рисунок 2. Схема применения режима встраивания «ответвитель».



В случае применения режима «ответвитель» путем настройки порта зеркалирования копирования входящих и исходящих сетевых пакетов с нескольких портов ТКО в один порт анализа необходимо учитывать емкость выбранного порта ТКО для подключения АПК, чтобы не превысить пропускную способность исходящих сетевых потоков, иначе могут быть потери сетевых пакетов на ТКО.

ПК Стетоскоп может выполнять анализ ранее записанных сетевых потоков в формате PCAP. Для этого необходимо выполнить копирование на АПК файлов в формате PCAP, ранее записанных сетевых потоков, и провести процедуру регистрации этих файлов в ПК Стетоскоп.

Независимо от способа получения PCAP-файлов (собственным механизмом захвата или копированием ранее записанного трафика) ПК Стетоскоп выполняет индексацию и анализ сетевых потоков, записанных в PCAP-файлах. Скорость индексации и анализа зависит от конфигурации АПК и сложности применяемых алгоритмов анализа. Используя рекомендованные параметры аппаратной платформы или гостевой виртуальной машины для исполнения ПК Стетоскоп скорость индексации и анализа должна быть не менее скорости записи потоков сетевого трафика.

Результатом анализа потоков сетевого трафика являются сообщения о событиях ИБ, которые записываются во встроенную базу данных (БД) и при

необходимости могут быть перенаправлены на внешних получателей событий ИБ по протоколу SYSLOG.

2.2. Условия выполнения ПК Стетоскоп

Для обработки сетевых потоков на скорости до 10 Гбит/с в каждом направлении (суммарно 20 Гбит/с) рекомендуются следующие параметры аппаратной платформы:

- сервер в корпусе 19”, монтируемом в стандартную коммуникационную стойку;
- центральный процессор с не менее 10 вычислительными ядрами с частотой не менее 2.0 ГГц;
- оперативная память не менее 256 ГБ;
- постоянно запоминающее устройство (далее - ПЗУ) №1 для операционной системы не менее 64 ГБ;
- ПЗУ №2 для хранения индекса и событий журналов аудита не менее 4 ТБ;
- ПЗУ №3 для хранения образцов записанного трафика суммарно не менее 120 ТБ (Расширение объема ПЗУ №3 позволит увеличить срок хранения образцов записанного трафика);
- поддержка ядра ОС Linux версии 4;
- один сетевой интерфейс, работающий на скорости не менее 1 Гбит/с, для реализации канала управления. Для реализации отказоустойчивого канала управления рекомендуется выделять два сетевых интерфейса;
- один и более сетевых интерфейсов с чипсетами Intel, работающих на скорости 10 Гбит/с для захвата сетевого трафика.

Для обработки сетевых потоков на скорости до 1 Гбит/с в каждом направлении (суммарно 2 Гбит/с) рекомендуются следующие параметры аппаратной платформы:

- сервер в корпусе 19”, монтируемом в стандартную коммуникационную стойку или ПК или гостевая виртуальная машина;
- центральный процессор с не менее 4 вычислительными ядрами с частотой не менее 2.0 ГГц;
- оперативная память не менее 64 ГБ;
- постоянно запоминающее устройство (далее - ПЗУ) №1 для операционной системы не менее 64 ГБ;
- ПЗУ №2 для хранения индекса и событий журналов аудита не менее 256 ГБ;
- ПЗУ №3 для хранения образцов записанного трафика суммарно не менее 12 ТБ (Расширение объема ПЗУ №3 позволит увеличить срок хранения образцов записанного трафика);
- поддержка ядра ОС Linux версии 4;
- один сетевой интерфейс, работающий на скорости не менее 1 Гбит/с, для реализации канала управления. Для реализации отказоустойчивого канала управления рекомендуется выделять два сетевых интерфейса;
- один и более сетевых интерфейсов с чипсетами Intel, работающих на скорости 1 Гбит/с для захвата трафика.

Для работы с WEB-приложением ПК Стетоскоп на АРМ должна быть установлена программа браузер. Список поддерживаемых программ браузеров и их версий приведен в таблице 1. В программе браузер должна быть включена поддержка языка сценариев JavaScript.

Таблица 1. Поддерживаемые программы браузер для работы с ПК Стетоскоп.

Название программы браузер	Версия (не ниже)
Google Chrome	53
Mozilla Firefox	52
Microsoft Edge	40

Рекомендуемые параметры АРМ пользователя ПК Стетоскоп:

- персональный компьютер;
- оперативная память не менее 16 ГБ;
- постоянно запоминающее устройство не менее 128 ГБ;
- центральный процессор с не менее двумя вычислительными ядрами с частотой работы не менее 2.0 ГГц;
- монитор не менее 23” с разрешением не менее FullHD (1920x1080). Для комфортной работы рекомендуется разрешение 4К;
- сетевой интерфейс, работающий на скорости не менее 1 Гбит/с;
- предустановленная операционная система, поддерживающая исполнение программ браузеров из таблицы 1.

3. WEB-приложение

3.1. Общие сведения

ПС «Клиент» ПК Стетоскоп является WEB-приложением, построенным на базе клиент серверной архитектуры и разделяется на две части: серверная и клиентская. Серверная часть WEB-приложения выполняется на сервере, с предустановленным ПК Стетоскоп. Клиентская часть WEB-приложения передается в программу браузер при первом обращении к серверной части. Все дальнейшее взаимодействие, получение данных от серверной части, выполняется в фоновом режиме по технологии AJAX. Для управления ПК Стетоскоп и решения задач анализа сетевого трафика рекомендуется выделить одно или более автоматизированное рабочее место (далее - АРМ) пользователя. ПК Стетоскоп поддерживает одновременную работу нескольких операторов.

Для подключения к WEB-приложению пользователь ПК Стетоскоп должен воспользоваться программой браузером, установленной в операционной системе (далее – ОС) выделенного АРМ. Должна быть обеспечена сетевая связность на уровне протокола IP АРМ оператора и

сервера с предустановленным ПК Стетоскоп. В адресной строке браузера необходимо ввести IP-адрес или DNS-имя сервера, с предустановленным ПК Стетоскоп, и пройти процедуру аутентификации.

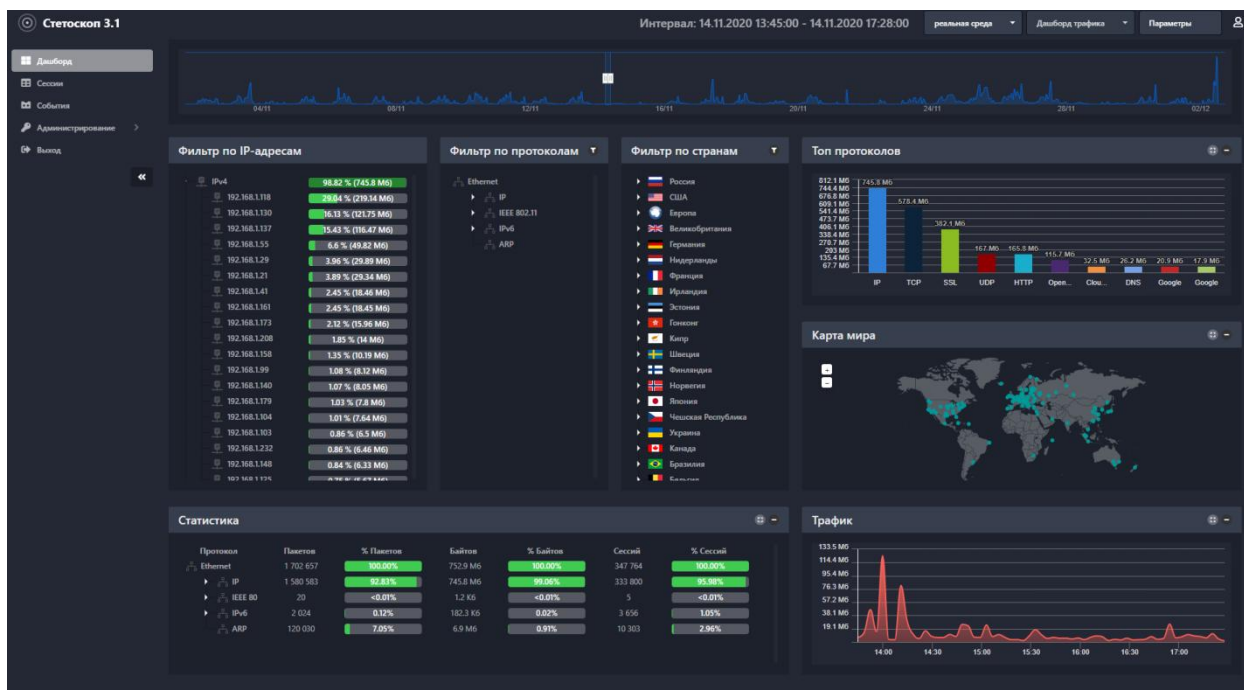
По умолчанию после установки ПК Стетоскоп имя пользователя и пароль имеют значение `admin` и `passwd` соответственно. После первого входа с именем пользователем и паролем по умолчанию необходимо сменить пароль пользователя. Пароль пользователя должен удовлетворять следующим требованиям безопасности (стойкости):

- не менее 10 символов;
- должна быть одна строчная и одна заглавная буква;
- должна быть хотя бы одна цифра;
- пароль не должен состоять из словарных слов;
- не должно быть более двух одинаковых повторяющихся символов.

После успешного прохождения процедуры аутентификации пользователь будет перенаправлен на WEB-страницу основного интерфейса WEB-приложения ПК Стетоскоп. Все случаи неправильной аутентификации регистрируются в журнале аудита системных событий ПК Стетоскоп.

Общий вид интерфейса представлен на рисунке 3.

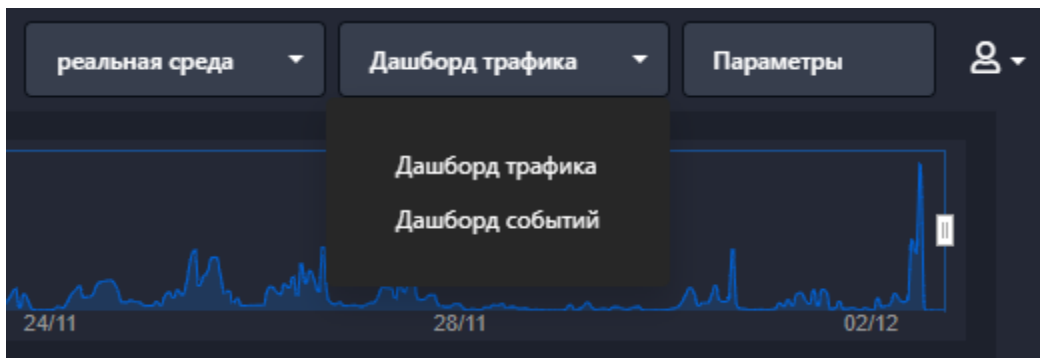
Рисунок 3. Общий вид WEB-интерфейса пользователя.



WEB-приложение состоит из нескольких областей, которые всегда сохраняют свое присутствие для обеспечения переключения интерфейсов представления данных и настроек ПК Стетоскоп:

- Вертикальное меню, расположенное слева экрана, где перечислены все интерфейсы,
- Горизонтальное меню, расположенное в верхней части экрана,
- График интенсивности потоков сетевого трафика или событий анализаторов, расположенный горизонтально под горизонтальным меню,
- Рабочая область отображения данных, расположенная по центру под графиком интенсивности, занимаемая большую площадь экрана – основной рабочий интерфейс, выбранный пользователем пункта вертикального меню.

Рисунок 4. Элементы горизонтального меню.



1. Реальная среда – переключатель режимов работы, позволяющий пользователю выбирать наборы данных, называемые источниками, для анализа. Пункты этого меню зависят от зарегистрированных источников в ПК Стетоскоп.

2. Дашборд трафика – переключатель между агрегированными отчетами по статистике трафика и агрегированными отчетами по событиям.

3. Параметры – диалоговое окно настроек общих критериев фильтрации отображаемых данных (см. рис. 5)

Рисунок 5. Диалоговое окно - Параметры

Параметры ✕

Период времени для анализа:

Начало:
01.11.2020 22:15:00 📅 ⌚

Окончание:
02.12.2020 22:15:00 📅 ⌚

Направление трафика для отображения на графиках:

☒ Общий ☐ Входящий ☐ Исходящий

Параметры трафика для отображения на графиках:

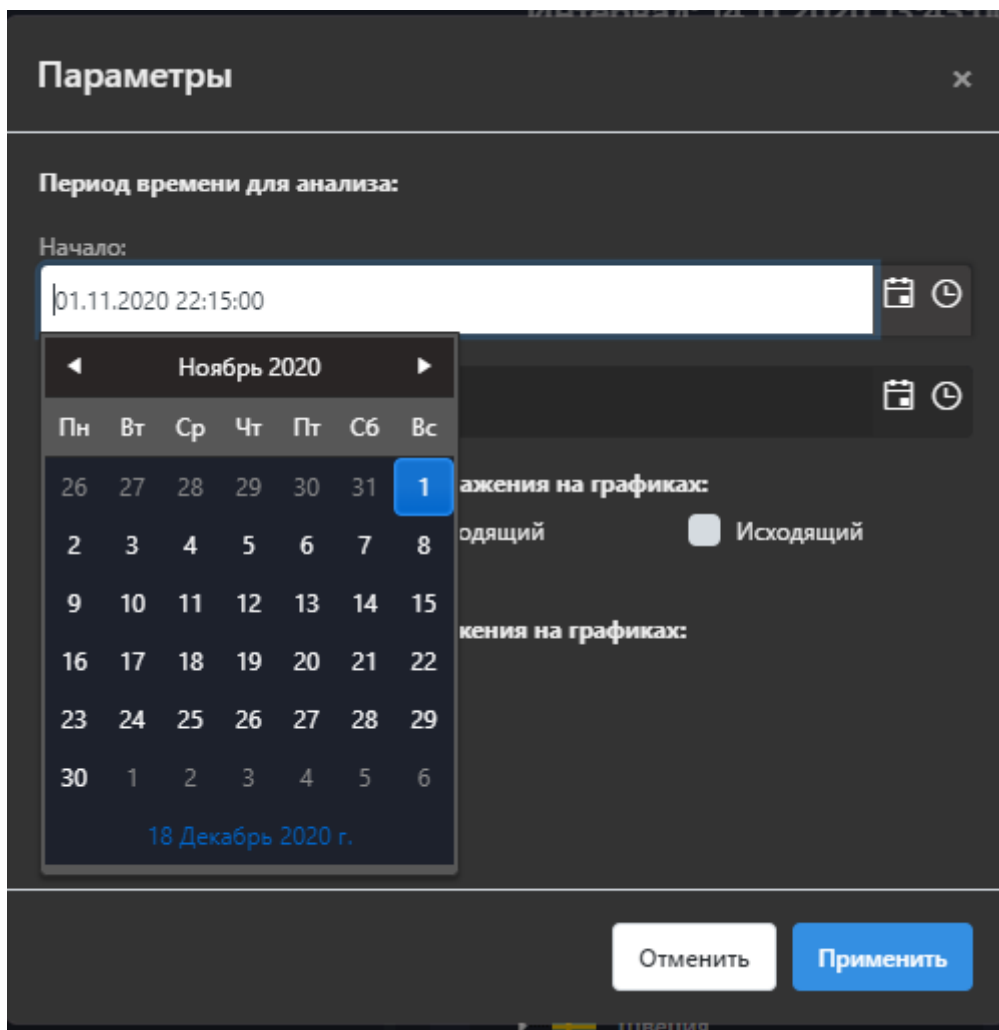
☒ Байты ☐ Пакеты ☐ Сессии

Отменить Применить

В диалоговом окне Параметры пользователь может указать диапазон времени и параметры, отображаемых на графике интенсивности значений агрегации и в представленных в рабочей области отображения данных отчетах.

Для дашборда списка сетевых сессий параметры включают в себя начало временного диапазон и окончание временного диапазона, ограничивая выборку данных по времени. Также можно указать сводная информация по каким параметрам сетевого трафика требуется для отображения: входящий трафик, исходящий трафик, байты, пакеты и сессии.

Рисунок 6. Диалоговое окно – Параметры – выбор дат и времени.



Указание даты и времени начала и окончания периода, отображаемых данных для анализа можно выполнять непосредственным введением значений в поле, а можно через открывающийся календарь и выпадающий список времени. Это позволяет оперативно изменять требуемый для анализа временной диапазон.

3.2. Список интерфейсов

1. «Дашборд статистики трафика»
2. «Список сессий статистики трафика»
3. «Дашборд и список событий»
4. «Администрирование»

3.3. Дашборд статистики трафика

Дашборд статистики трафика отображает агрегационную информацию по локальным IP-адресам, обнаруженным сетевым протоколам до прикладного уровня, включая сервисы и по географической принадлежности внешних IP-адресов. Данные окна расположены в левой верхней части экрана и обладают свойством фильтрации. Выбирая в них требуемые элементы автоматически применяется фильтр для остальных элементов дашборда статистики трафика.

Дашборд статистики трафика содержит распределение по протоколам – окно «Топ протоколов», отображение на карте мира распределение источников трафика – окно «Карта мира», элемент в правом нижнем углу с укрупненным представлением выбранного локального интервала в графике интенсивности – окно «Трафик» и детальную статистику по обнаруженным сетевым протоколам – окно «Статистика» (см. рис. 7)

Рисунок 7. Дашборд статистики трафика



Элементы пользовательского интерфейса «Трафик» и «Карта мира» поддерживают раскрытие на полный экран в отдельном окне, что может быть удобно при наличии отдельного монитора или для возможности детальной

проработке пользователем элементов, отображаемых в этих интерфейсах (см. рис. 8 и рис. 9).

Рисунок 8. Отдельное окно анализа распределения источников трафика на географической карте мира

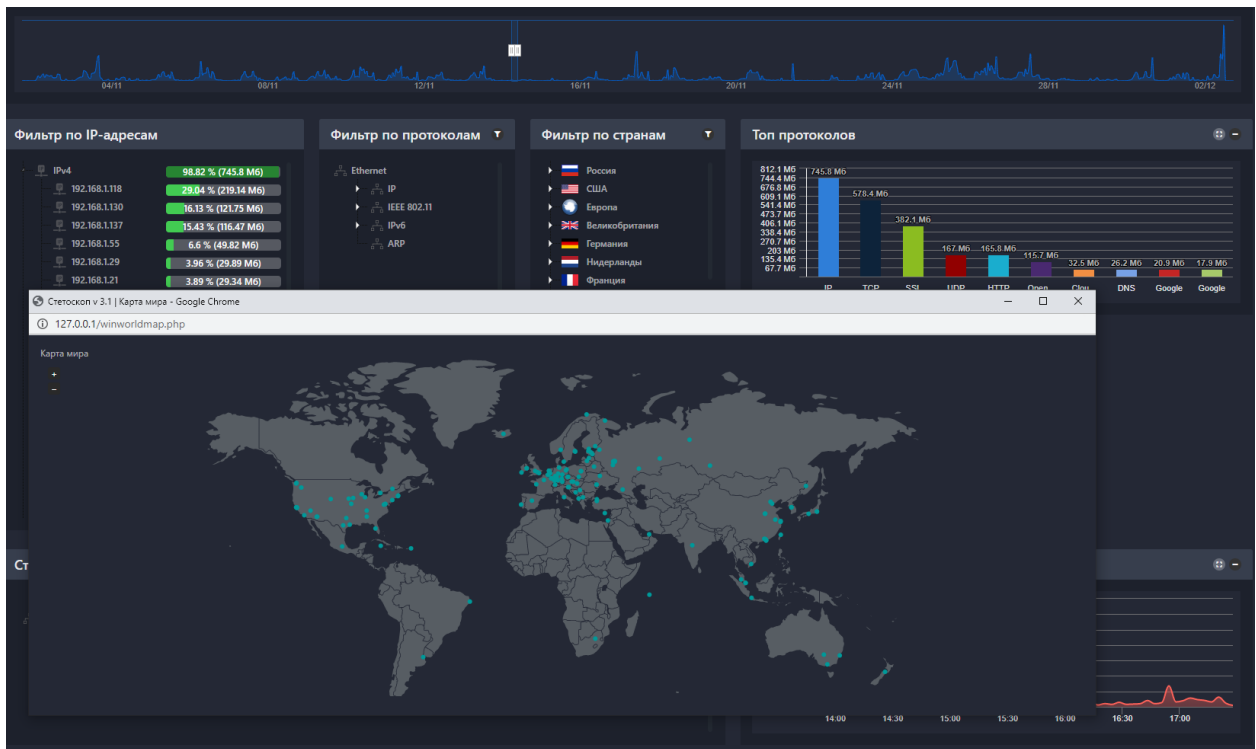
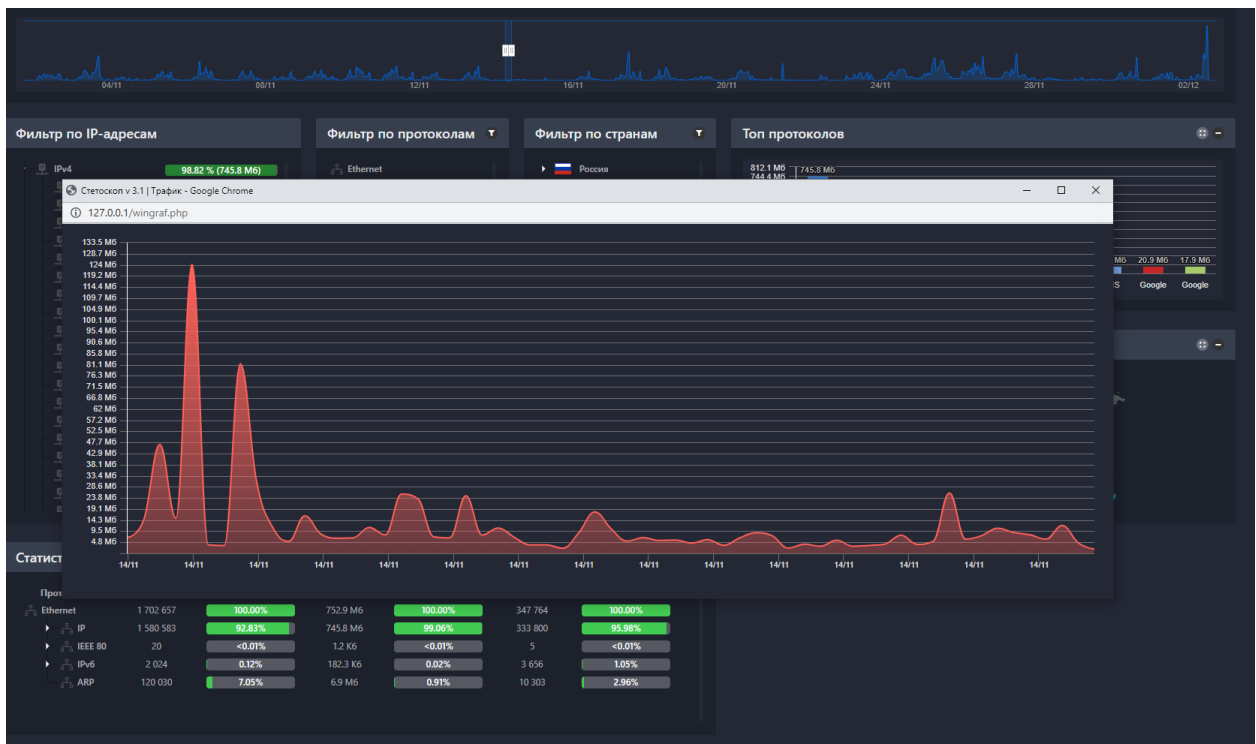


Рисунок 9. Отдельное окно анализа интенсивности трафика

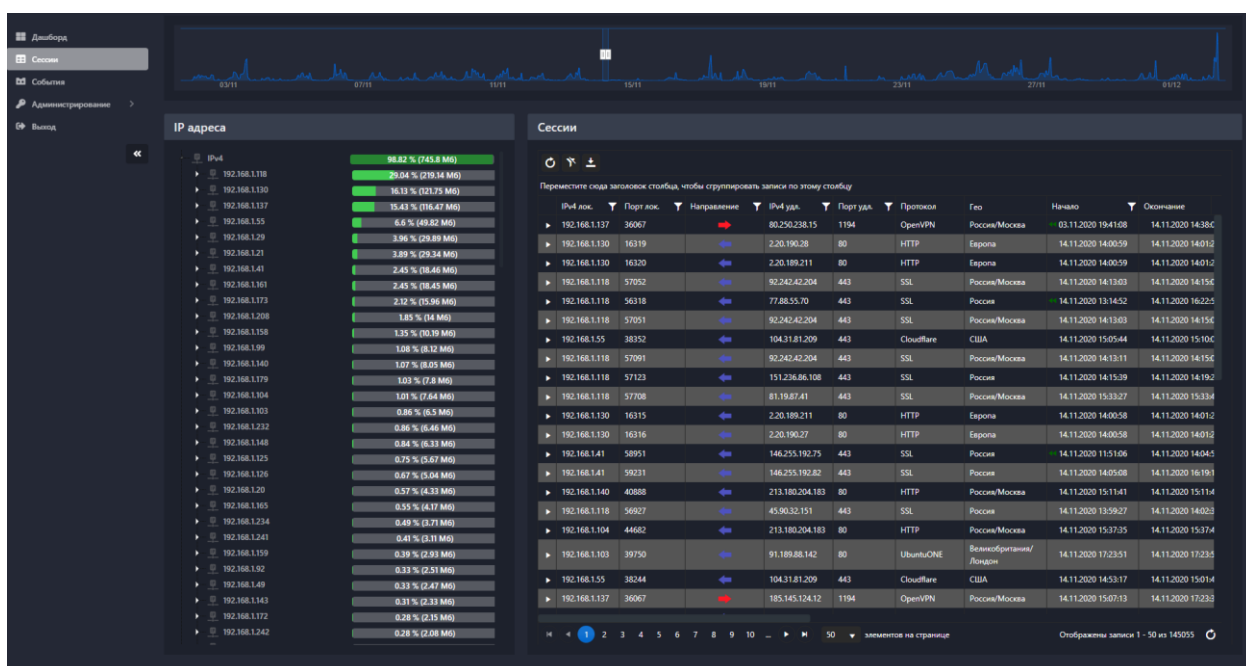


3.4. Список сессий статистики трафика

Рабочая область списка сессий статистики сетевого трафика представлена на рисунке 10 и состоит из следующих частей:

- область фильтра по времени - выбора интересующего временного диапазона,
- область фильтра по IP-адресам и протоколам,
- область списка сессий.

Рисунок 10. Список сессий статистики трафика

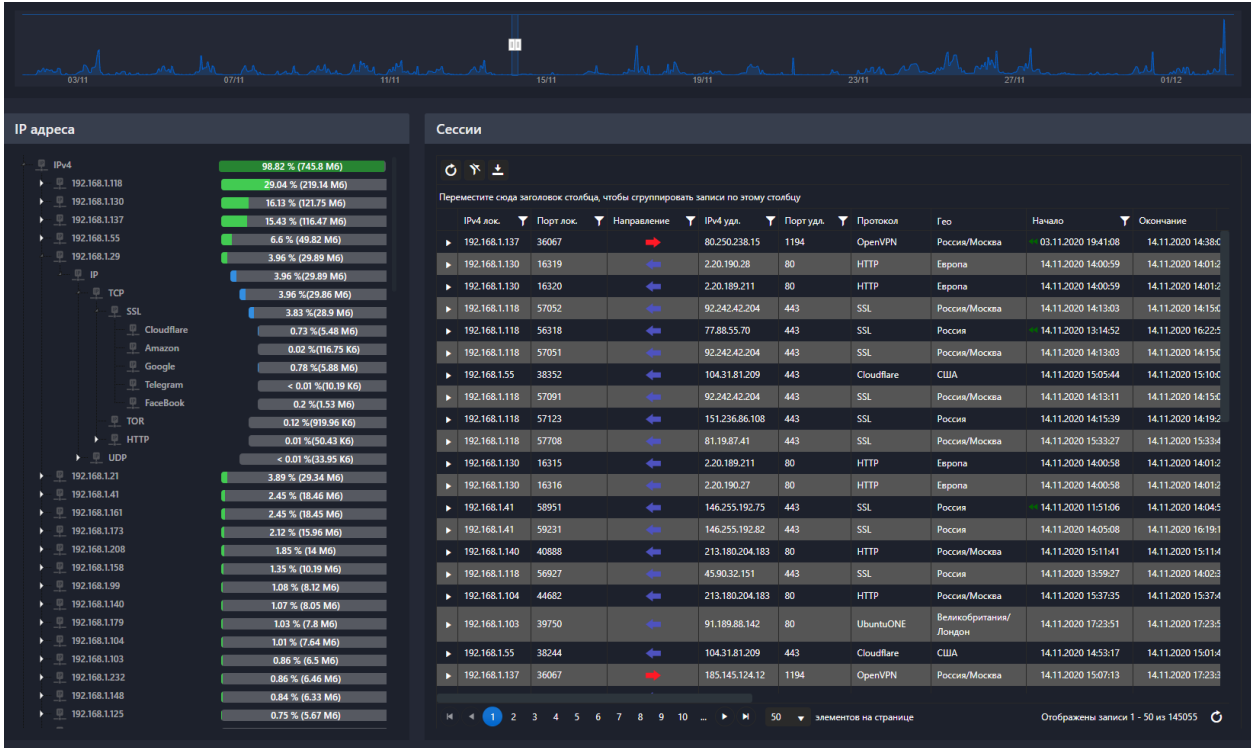


Задание временного диапазона влияет на данные, отображаемые в области фильтра по IP-адресам и протоколам – список IP-адресов и протоколов выводится с учетом данных о сетевых сессиях в ПС «БД» за заданный интервал времени.

Область фильтра по IP-адресам и протоколам представлена в виде элемента пользовательского интерфейса «дерево». В левой части отображаются IP-адреса и протоколы, а в правой статистика трафика. Корневыми узлами отображаются типы IP-адресов: IP версии 4, IP версии 6 и узел, агрегирующий остальной не IP-трафик (трафик не содержащий уровень протокола IP). Эти узлы содержат списки IP-адресов соответствующих

типов, отсортированные в порядке убывания размера объема трафика используемого хостом с указанным IP-адресом. Узел каждого IP-адреса может быть раскрыт и будет выведен иерархический список протоколов, используемых хостом с указанным IP-адресом. Пример раскрытого одного узла IP-адреса представлен на рисунке 11.

Рисунок 11. Иерархия элементов области фильтра по IP-адресам и протоколам.



Если в области фильтра по IP-адресам и протоколам пользователь ничего не выбирает, то в области списка сессий отображаются все сессии за указанный временной интервал.

Если пользователь выбирает в области фильтра по IP-адресам и протоколам интересующие его значения, то в области списка сессий отображаются только те сессии, которые удовлетворяют заданному временному диапазону, заданному IP-адресу и/или протоколу.

Область фильтра по IP-адресам и протоколам организована в виде двухуровневого дерева, где первый уровень – список IP-адресов, а второй уровень - список протоколов, соответствующих IP-адресу первого уровня.

Т.е. раскрыв необходимый узел первого уровня пользователь получает информацию о списке протоколов общения заданного IP-адреса за заданный интервал времени.

Область фильтра по IP-адресам и протоколам содержит дополнительную статистику по сессиям, байтам и пакетам для каждого отображаемого IP-адреса и протокола. Управление выбором отображаемого параметра производится в окне настроек текущего отображения интерфейса, вызываемого в правой верхней части окна WEB-приложения.

Область списка сессий представляет собой таблицу, в каждой строке которой отображается информация об одной сессии. В колонках таблицы отображены основные параметры сессии, такие как:

- уникальный идентификатор сессии – GUID,
- дата и время начала сессии,
- дата и время окончания сессии,
- количество байт сессии,
- количество пакетов сессии,
- стек протокол сессии.

Для получения дополнительной (расширенной информации) по сессии необходимо вызвать карточку сессии двойным нажатием мыши на строку требуемой сессии. Карточка выбранной сессии отображается в виде расширения ее строки областью снизу. Данная область содержит те же данные, что и в колонках строки сессии, а также следующие данные:

- кнопку отображения контента сессии,
- кнопку экспорта пакетов сессии в формате PCAP.

По нажатию на кнопку отображения контента сессии пользователю выводится текст сессии, полученный склеиванием содержимого транспортных и прикладных протоколов сетевых пакета, относящихся к сессии. Данные выводятся в режиме пригодном для чтения пользователем. Непечатаемые символы кодируются шестнадцатеричным представлением.

По нажатию на кнопку экспорта сессии в формате PCAP формируется файл в формате PCAP, содержащий пакеты выбранной сессии, который штатными средствами WEB-браузера сохраняется на АРМ пользователя. Данный файл пригоден для дальнейшей обработки программными средствами работы с PCAP-файлами, например WireShark, tcpreplay и т.п.

Для экспорта в PCAP-формате сетевых пакетов нескольких сетевых сессий необходимо выделить несколько строк сетевых сессий и нажать кнопку «Экспорт в PCAP», расположенную в верхней части таблицы со списком сессий.

Каждая сессия отображается в списке сессий одной строкой. В заголовке столбцов таблицы списка сессий отображается значек текущей выбранной колонки по данным в которой выполняется сортировка и признак возможности осуществления фильтрации по данным соответствующей колонки (см. рис. 12).

Рисунок 12. Фильтр списка сессий

Переместите сюда заголовок столбца, чтобы сгруппировать записи по этому столбцу

IPv4 лок.	Порт лок.	Направление	IPv4 удл.	Порт удл.	Протокол	Гео	Начало	Окончание
▶ 192.168.1.161	60913	←	17.253.39.201			Швеция/Киста	26.11.2020 23:29:12	26.11.2020 23:48:3
▶ 192.168.1.161	61035	←	93.184.221.133			Великобритания/Лондон	25.11.2020 17:17:52	25.11.2020 18:38:1
▶ 192.168.1.161	50301	←	94.247.111.11			Россия/Гурьевск	26.11.2020 18:27:41	26.11.2020 19:42:0
▶ 192.168.1.161	61871	←	188.126.94.86			Дания/Копенгаген	24.11.2020 11:30:53	24.11.2020 14:06:3
▶ 192.168.1.161	60782	←	198.27.219.132	29175	TCP	США	26.11.2020 1:43:07	26.11.2020 11:23:2
▶ 192.168.1.161	61653	←	94.25.26.58	4433	STUN	Россия/Москва	26.11.2020 13:02:26	27.11.2020 14:53:4
▶ 192.168.1.161	51231	←	198.27.219.132	29175	TCP	США	24.11.2020 18:26:11	25.11.2020 7:45:4

Над заголовками таблицы списка сессий есть область группировки сессий по параметрам сессий (см. рис 13).

Рисунок 13. Группировка в списке сессий.

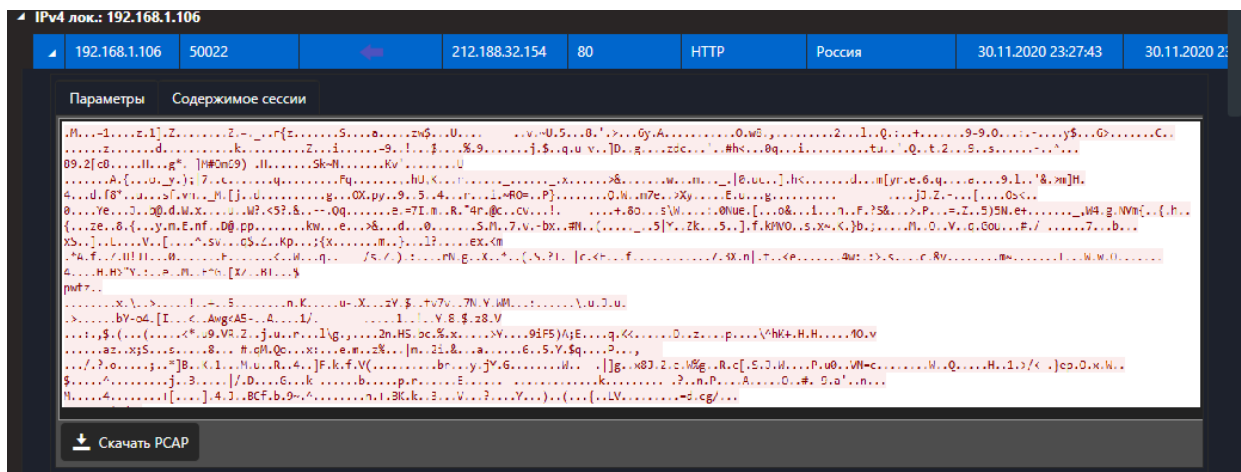
IPv4 лок.	Порт лок.	Направление	IPv4 удл.	Порт удл.	Протокол	Гео	Начало	Окончание
IPv4 лок.: 192.168.1.161								
▶ 192.168.1.161	60913	←	17.253.39.201	80	Apple	Швеция/Киста	26.11.2020 23:29:12	26.11.2020 23:29:12
▶ 192.168.1.161	61035	←	93.184.221.133	80	HTTP	Великобритания/Лондон	25.11.2020 17:17:52	25.11.2020 17:17:52
▶ 192.168.1.161	50301	←	94.247.111.11	443	SSL	Россия/Гурьевск	26.11.2020 18:27:41	26.11.2020 18:27:41
▶ 192.168.1.161	61871	←	188.126.94.86	8080	UDP	Дания/Копенгаген	24.11.2020 11:30:53	24.11.2020 11:30:53
▶ 192.168.1.161	60782	←	198.27.219.132	29175	TCP	США	26.11.2020 1:43:07	26.11.2020 1:43:07
▶ 192.168.1.161	61653	←	94.25.26.58	4433	STUN	Россия/Москва	26.11.2020 13:02:26	27.11.2020 13:02:26
▶ 192.168.1.161	51231	←	198.27.219.132	29175	TCP	США	24.11.2020 18:26:11	25.11.2020 18:26:11
▶ 192.168.1.161	52780	←	159.69.60.50	51754	BitTorrent	Германия	24.11.2020 18:43:01	25.11.2020 18:43:01
▶ 192.168.1.161	56604	←	94.25.26.58	4433	STUN	Россия/Москва	30.11.2020 14:11:54	01.12.2020 14:11:54
▶ 192.168.1.161	50802	←	94.25.26.58	4433	STUN	Россия/Москва	27.11.2020 17:03:47	28.11.2020 17:03:47
▶ 192.168.1.161	61359	←	37.193.189.84	49644	TCP	Россия/Новосибирск	27.11.2020 23:55:34	28.11.2020 23:55:34
▶ 192.168.1.161	65237	←	82.140.232.226	38827	TCP	Россия/Тверь	28.11.2020 6:30:15	28.11.2020 6:30:15
▶ 192.168.1.161	63431	←	185.21.217.56	32808	TCP	Нидерланды	25.11.2020 17:35:22	26.11.2020 17:35:22
▶ 192.168.1.161	60021	←	176.113.74.37	31404	TCP	Канада/Montreal	25.11.2020 2:13:28	25.11.2020 2:13:28

Каждая сессия содержит значек открытия карточки в начале соответствующей сессии строке. Нажатие на него открывает карточку с расширенной информацией о сессии и область просмотра контента сессии, включая кнопку экспорта в формате PCAP пакетов выбранной сессии (см. рис. 14 и рис. 15)

Рисунок 14. Карточка сетевой сессии

Параметры		Содержимое сессии	
Локальный IP:	192.168.1.161	Гео:	Великобритания/Лондон
Локальный порт:	61035	Начало:	25.11.20 14:17:52
Удаленный IP:	93.184.221.133	Конец:	25.11.20 15:38:12
Удаленный порт:	80	Длительность:	01:20:20
Протокол:	HTTP	Байты:	4 748 621 662
Локальный MAC-адрес:	D1:1E:66:F3:8B:58	Исходящие байты:	4 652 590 644
Удаленный MAC-адрес:	1F:0C:E6:19:8E:C8	Пакеты:	4 576 197
		Исходящие пакеты:	3 073 049
		Входящие байты:	96 031 018
		Входящие пакеты:	1 503 148
		Направление:	←
		Статус сессии:	закрыта

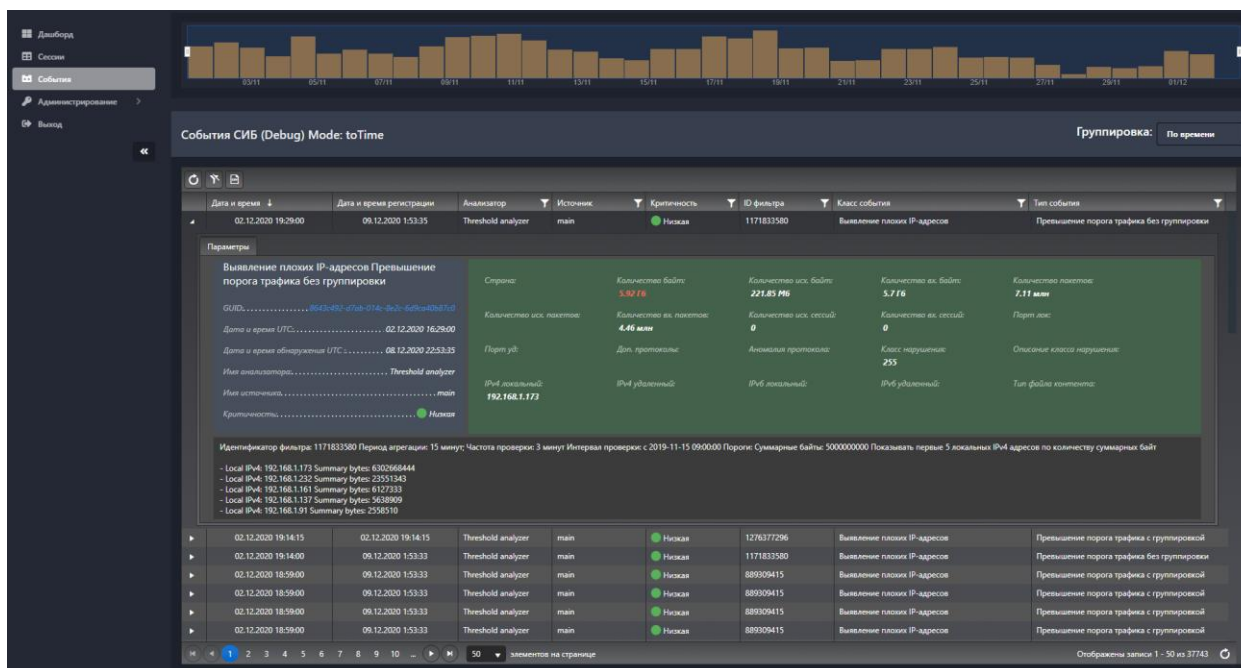
Рисунок 15. Контент сетевой сессии в карточке



3.5. Дашборд и список событий

В верхней части экрана дашборда и списка событий (см. рис. 16) отображается интенсивность событий за выбранный в параметрах (кнопка горизонтального меню в верхней части экрана) диапазон времени.

Рисунок 16. Дашборд и список событий.

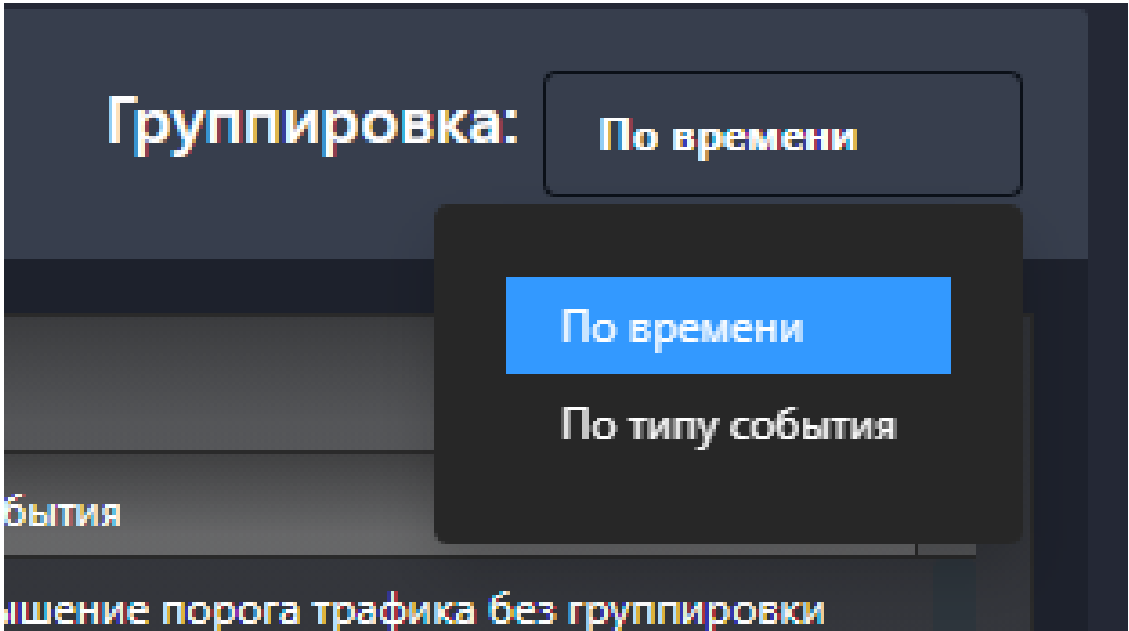


В центральной части представлен список событий, удовлетворяющих заданному пользователем фильтру и представлению.

Представление списка событий меняется переключателем «Группировка:» расположенному в правой верхней части экрана над списком событий. Представление списка событий реализовано в двух вариантах –

линейное, когда все события представлены в едином списке – элемент меню «По времени» и группированное, когда все события сгруппированы по типу – элемент меню «По типу события» (см. рис. 17)

Рисунок 17. Выбор представления списка событий.



Каждое событие в списке представлено одной строкой. В верхней части списка в названиях колонок отображается значек сортировки, выставленный на текущей выбранной колонке по данным из которой выполнять сортировку, и значки фильтрации. Нажатие на значек фильтра соответствующей колонки позволяет пользователю выполнить фильтрацию списка событий по дополнительным требуемым условиям (см. рис. 18).

Рисунок 18. Дополнительные фильтры списка событий.

ции	Анализатор	Источник	Критичность	ID фильтра	Класс события
5	Threshold analyzer	Строки со значениями равно фильтровать ОЧИСТИТЬ	изкая	1171833580	Выявление плохих IP-адресов
15	Threshold analyzer		изкая	1276377296	Выявление плохих IP-адресов
3	Threshold analyzer		изкая	1171833580	Выявление плохих IP-адресов
3	Threshold analyzer		изкая	889309415	Выявление плохих IP-адресов
3	Threshold analyzer		изкая	889309415	Выявление плохих IP-адресов
3	Threshold analyzer		изкая	889309415	Выявление плохих IP-адресов
3	Threshold analyzer	main	Низкая	889309415	Выявление плохих IP-адресов

Каждое событие в соответствующей строке содержит кнопку открытия карточки с расширенной информацией (см. рис. 19).

Рисунок 19. Карточка события.

▶	02.12.2020 18:59:00	09.12.2020 1:53:33	Threshold analyzer	main	Низкая	889309415	Выявление плохих IP-адресов	Превышение порога трафика с группировкой
▶	02.12.2020 18:59:00	09.12.2020 1:53:33	Threshold analyzer	main	Низкая	889309415	Выявление плохих IP-адресов	Превышение порога трафика с группировкой
▶	02.12.2020 18:59:00	09.12.2020 1:53:33	Threshold analyzer	main	Низкая	889309415	Выявление плохих IP-адресов	Превышение порога трафика с группировкой
▶	02.12.2020 18:59:00	09.12.2020 1:53:33	Threshold analyzer	main	Низкая	889309415	Выявление плохих IP-адресов	Превышение порога трафика с группировкой

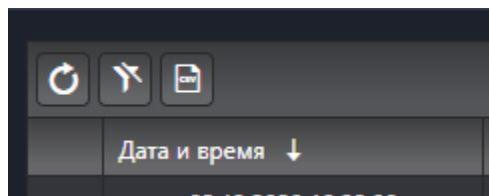
Параметры Выявление плохих IP-адресов Превышение порога трафика с группировкой GUID.....bc23b4ab-2b80-9442-9b7f-49072537887 Дата и время UTC.....02.12.2020 15:59:00 Дата и время обнаружения UTC.....08.12.2020 22:53:33 Имя анализатора.....Threshold analyzer Имя источника.....main Критичность.....Низкая		Страна: Количество исх. байт: 330 6 Количество исх. пакетов: 0 Порт uid: Доп. протоколы: ssh IPv4 локальный: 192.168.1.92 IPv4 удаленный: IPv6 локальный: IPv6 удаленный:					Количество исх. байт: 330 6 Количество исх. сессий: 0 Аномалия протокола: 255 Класс нарушения: Описание класса нарушения:		Количество вх. байт: 0 6 Количество вх. сессий: 0 Порт лог: Тип файла контента:	
---	--	---	--	--	--	--	--	--	---	--

Идентификатор фильтра: 889309415 Период агрегации: 60 минут Частота проверки: 15 минут Интервал проверки: с 2019-11-15 09:00:00 Пороги: Суммарные байты: 1 Фильтруемые протоколы: ssh Группировать по локальным IPv4 адресам
 - Local IPv4: 192.168.1.92

▶	02.12.2020 18:59:00	09.12.2020 1:53:33	Threshold analyzer	main	Низкая	889309415	Выявление плохих IP-адресов	Превышение порога трафика с группировкой
▶	02.12.2020 18:59:00	09.12.2020 1:53:33	Threshold analyzer	main	Низкая	889309415	Выявление плохих IP-адресов	Превышение порога трафика с группировкой

В верхней части над списком событий располагается панель инструментов (см. рис. 20).

Рисунок 20. Панель инструментов.



Описание кнопок панели инструментов слева направо:

- кнопка обновления списка событий,
- кнопка сброса всех заданных фильтров в заголовков столбцов таблицы списка сессий,
- кнопка экспорта списка сессий в формате CSV на APM оператора.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

ARP	– Address Resolution Protocol (протокол разрешения адресов) – процедуры и сообщения в коммуникационном протоколе, которые определяют физический адрес по IP-адресу.
EMAIL	– Electronic mail – электронная почта.
ftp	– File Transfer Protocol – протокол передачи данных.
ICMP	– Internet Control Message Protocol — межсетевой протокол управляющих сообщений.
IDS	– Служба обнаружения компьютерных атак.
MTU	– Maximum Transmission Unit – максимальный передаваемый модуль данных.
NTP	– Network Time Protocol – протокол синхронизации времени в сети.
OSI	– Open Systems Interconnection.
SMTP	– Simple Mail Transfer Protocol— простой протокол передачи почты.
SYSLOG	– Системные сообщения.
UDP	– прозрачный протокол в группе протоколов Internet. UDP, подобно TCP, использует IP для доставки; однако, в отличие от TCP, UDP обеспечивает обмен дейтаграммами без подтверждения или гарантий доставки.
АИС	– Автоматизированная информационная система.
БД	– База данных.
ОС	– Операционная система.

Лист регистрации изменений

[illegible]