

УТВЕРЖДЕН
18678659.00001-03 32 02-ЛУ

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

Руководство администратора (системного программиста)

18678659.00001-03 32 02

2022 г.

АННОТАЦИЯ

Настоящий документ является руководством администратора 18678659.00001-03 32 02 Комплекса программных средств ретроспективного анализа сетевого трафика «Стетоскоп» версии 3.0 (далее - ПК Стетоскоп или изделие).

В руководстве даётся общее описание ПК Стетоскоп, приводится процедура установки ПК Стетоскоп, описываются подключение и настройка ПК Стетоскоп в информационную систему и указываются действия администратора по работе с программным обеспечением. Описывается инфраструктура ПК Стетоскоп, включая возможные схемы подключения.

<p><i>Все права защищены. Полное или частичное копирование материалов без письменного согласования с ООО «ЦСС-Безопасность» запрещено.</i></p>
--

СОДЕРЖАНИЕ

1. Общие сведения.....	5
1.1. Область применения.....	5
1.2. Назначение.....	5
1.3. Состав ПК Стетоскоп	6
2. Общие принципы работы ПК Стетоскоп	8
2.1. Общие положения	8
2.2. Условия выполнения ПК Стетоскоп	11
3. Установка на аппаратную платформу.....	14
3.1 Подготовка операционной системы и жестких дисков	14
3.2 Установка ПК Стетоскоп и добавление источника данных	16
3.3 Удаление источника данных	19
3.4 Удаление ПК Стетоскоп	19
4 Анализаторы	20
4.1 Анализатор пороговых значений	22
4.2 Анализатор подозрительных IP-адресов	24
5 Приложение 1. Примеры фильтров анализаторов	26
5.1 Пример фильтра анализатора пороговых значений	26
5.2 Пример фильтра анализатора подозрительных IP-адресов	29
6 Приложение 2. Сообщения анализаторов	30
6.1 Структура и поля сообщений порогового анализатора	30
6.2 Структура и поля сообщений анализатора подозрительных IP-адресов	37
7 Приложение 3. Перечень категорий подозрительных IP-адресов	43

8	Перечень принятых сокращений	44
---	------------------------------------	----

1. ОБЩИЕ СВЕДЕНИЯ

Настоящее руководство разработано в соответствии с ГОСТ 19.503-79 ЕСПД, ГОСТ 2.601-95 ЕСКД и распространяется на программный комплекс ретроспективного анализа сетевого трафика «Стетоскоп» версии 3.0, обозначаемый 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 «Анализатор»;
- 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

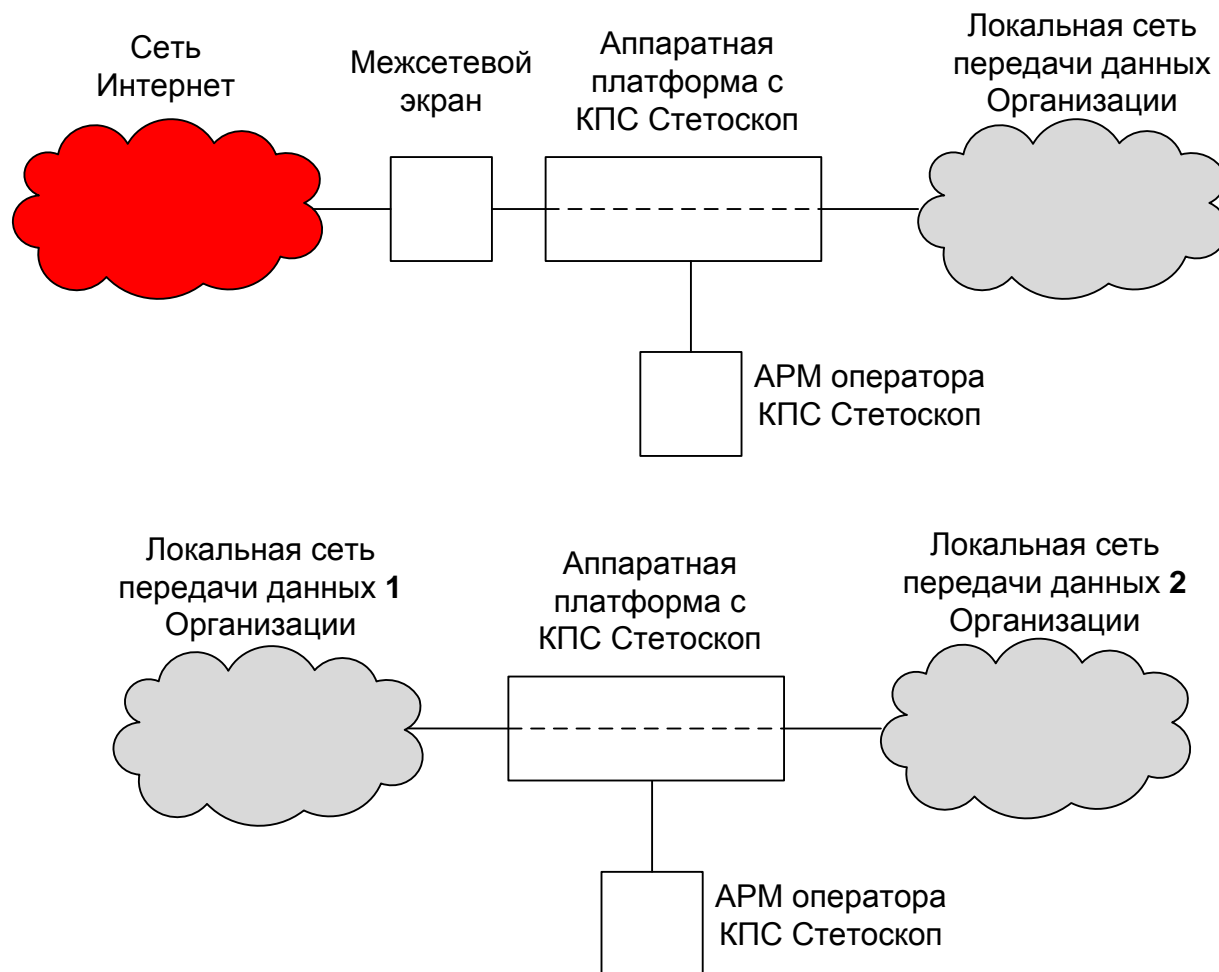
Исходными данными для ПК Стетоскоп являются потоки сетевого трафика. ПК Стетоскоп выполняет обработку потоков сетевого трафика путем индексации и анализа. Для решения задач индексации и анализа потоки сетевого трафика должны быть записаны в формате PCAP.

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.

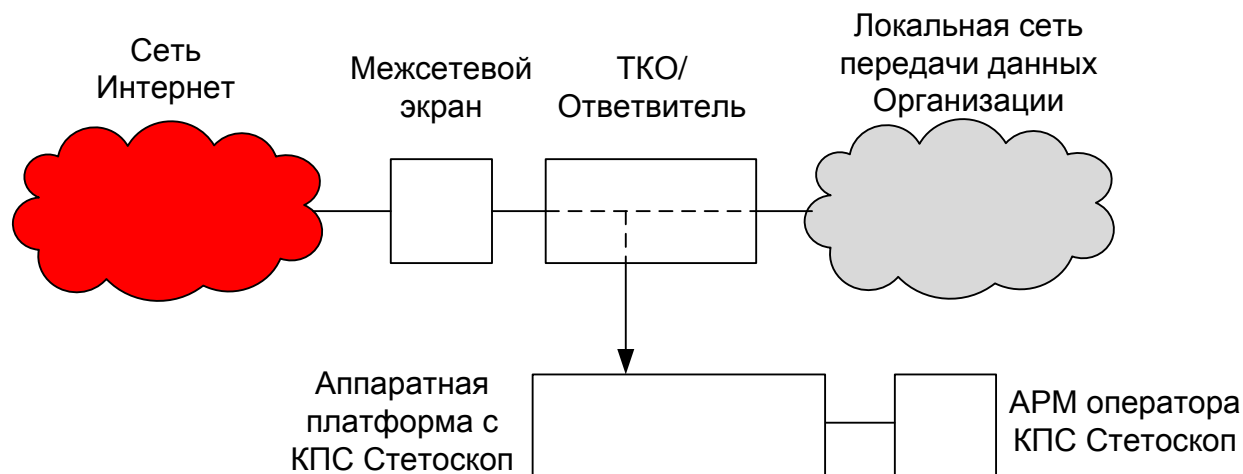
В процессе проброса сетевых пакетов между двумя сетевыми интерфейсами АПК, их копии захватываются ПК Стетоскоп и записываются на локальный диск АПК с последующим анализом. Данный режим при штатной работе АПК не оказывает влияние на линию связи, в которую он встроен. Для обеспечения отказоустойчивости 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.

Список поддерживаемых и рекомендованных сетевых чипсетов Intel для захвата сетевого трафика: i350, 82580EB, 82580DB, XL710, X550, X710, 82599ES, X540, XXV710, FM10420.

В случае применения в качестве аппаратной платформы среду виртуализации, рекомендуется использовать эмуляцию сетевых драйверов семейства «e1000», «e1000e», «igb», «ixgbe», «i40e».

Для работы с интерфейсом WEB-приложения 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. УСТАНОВКА НА АППАРАТНУЮ ПЛАТФОРМУ

3.1 Подготовка операционной системы и жестких дисков

1. Установить операционную систему (далее – ОС) Linux Ubuntu в исполнении «server» без графического интерфейса релиз версии 18.04.5 LTS (Версия ядра ОС Linux Ubuntu 4.15.0-144-generic). В процессе установки выбрать только один дополнительный пакет для установки – «OpenSSH-server».

Примечание. Версия поддерживаемого ПК Стетоскоп ядра ОС указана в названии директории в файле-архиве с дистрибутивом (например, stet-3.0.9424_4.15.0-144-generic). Версия должна совпадать полностью, в противном случае установка или корректная работа ПК Стетоскоп не гарантируется.

2. Разбиение жестких дисков требует:

- размещения ОС на отдельном выделенном разделе отдельно жесткого диска (предпочтительно использовать тип диска SSD),
- выделение отдельного раздела и отдельно жесткого диска для базы данных статистики сетевого трафика (предпочтительно использовать тип диска SSD),

Далее приведен пример создания отдельного раздела на отдельном жестком диске для базы данных статистики сетевого трафика.

Примечание. Использование команд из этого примера удалит все данные на используемых жестких дисках. Для использования команд из примера необходимо иметь полномочия суперпользователя в ОС.

Исходные данные:

- количество дисков: 1,
- названия дисков в ОС: /dev/nvme0n1,
- тип файловой системы нового раздела: ext4,

- директория подключения нового раздела: /ch

Команды создания раздела:

а. Команды создания LVM-раздела

- `sudo pvcreate /dev/nvme0n1`

- `sudo vgcreate -s 32M vch /dev/nvme0n1`

- `sudo lvcreate -n lch -l 100%FREE vch`

б. Команда создания раздела с новой файловой системы на созданном массиве «`sudo mkfs.ext4 /dev/vch/lch`».

в. Команда создания директории подключения нового раздела «`sudo mkdir -p /ch`».

г. Команда добавления подключения нового раздела при загрузке ОС «`sudo sh -c "echo '/dev/vch/lch /ch ext4 defaults 0 2' >> /etc/fstab"`»

д. Команда подключения нового раздела в текущей сессии загрузки ОС «`sudo mount -a`».

- выделение массива жестких дисков большого объема с отдельным разделом файловой системы для размещения файлов записанного сетевого трафика (диски предпочтительно объединить в массив типа RAID0 для обеспечения требуемой скорости записи на них).

Далее приведен пример создания массива типа RAID0 встроенными средствами в ОС Linux для размещения файлов записанного сетевого трафика.

Примечание. Использование команд из этого примера удалит все данные на используемых жестких дисках. Для использования команд из примера необходимо иметь полномочия суперпользователя в ОС.

Исходные данные:

- количество дисков: 10,

- названия дисков в ОС: /dev/sdb /dev/sdc /dev/sdd /dev/sde /dev/sdf /dev/sdg /dev/sdh /dev/sdi /dev/sdj /dev/sdk,

- на момент создания нового массива в системе нет других массивов,

- имя создаваемого массива: md0,
- тип файловой системы нового раздела из массива: ext4,
- директория подключения нового раздела из массива: /data

Команды создания раздела:

а. Команда создания массива «`sudo mdadm --create --verbose /dev/md0 --level=0 --raid-devices=20 /dev/sdb /dev/sdc /dev/sdd /dev/sde /dev/sdf /dev/sdg /dev/sdh /dev/sdi /dev/sdj /dev/sdk`».

б. Команда создания раздела с новой файловой системой на созданном массиве «`sudo mkfs.ext4 -F /dev/md0`».

в. Команда создания директории подключения нового раздела «`sudo mkdir -p /data`».

г. Команда добавления подключения нового раздела при загрузке ОС «`sudo sh -c "echo '/dev/md0 /data ext4 defaults 0 2' >> /etc/fstab"`»

д. Команда подключения нового раздела в текущей сессии загрузки ОС «`sudo mount -a`».

3.2 Установка ПК Стетоскоп и добавление источника данных

1. Разместить архив с дистрибутивом на файловой системе аппаратной платформы (далее – сервер). Архив поставляется в виде файла на компакт диске и имеет название «stet-3.0.<версия КПС>_<версия ОС>.tar.gz». Где <версия КПС> - минорная версия релиза ПК Стетоскоп, <версия ОС> - версия ядра ОС Linux Ubuntu.

Примечание. Аппаратная платформа, с установленной ОС, должна быть подключена к сети Интернет для выполнения установки требуемых пакетов общего программного обеспечения и ОС.

2. Раскрыть архив командой «`tar xzf stet-3.0.<версия КПС>_<версия ОС>.tar.gz`». И выполнить вход в директорию дистрибутива «stet-3.0.<версия КПС>_<версия ОС>» командой «`cd stet-3.0.<версия КПС>_<версия ОС>`».

3. Находясь в директории с файлами дистрибутива выполнить установку системной части ПК Стетоскоп. Для этого с правами суперпользователя ОС необходимо выполнить команду «`sudo stetinstallsystem.sh`». В процессе выполнения команды будет выдан запрос пароля суперпользователя СУБД ClickHouse. Необходимо нажать «Enter», таким образом оставив его пустым.

```
Enter password for default user:
Password for default user is empty string. See /etc/clickhouse-server/users.xml and /etc/clickhouse-server/users.d to change it.
```

В случае успешной установки системной части в конце журнала установки должны быть выданы следующие сообщения:

«Considering dependency socache_shmcb for ssl:

Module socache_shmcb already enabled

Module ssl already enabled

ALTER ROLE».

4. Выполнить установку базовой части ПК Стетоскоп. Для этого с правами суперпользователя ОС необходимо выполнить команду «`sudo ./stetinstallcommon.sh`». В случае успешной установки базовой части в конце журнала установки должны быть выданы следующие сообщения:

«Created symlink /etc/systemd/system/multi-user.target.wants/stet_rotator.service → /usr/local/bin/stet_rotator.service.

Created symlink /etc/systemd/system/stet_rotator.service → /usr/local/bin/stet_rotator.service.

Created symlink /etc/systemd/system/multi-user.target.wants/stet_report.service → /usr/local/bin/stet_report.service.

Created symlink /etc/systemd/system/stet_report.service → /usr/local/bin/stet_report.service.»

5. Далее необходимо выполнить регистрацию источника данных. Для этого необходимо выбрать его уникальное имя, которое в последствии будет отображаться в интерфейсе управления, а также перечень сетевых интерфейсов аппаратной платформы для захвата трафика. Пример имени

источника – «src1». Для просмотра списка сетевых интерфейсов аппаратной платформы, доступных из ОС, необходимо выполнить команду «ip a». Для регистрации источника ПК Стетоскоп необходимо с правами суперпользователя выполнить команду «sudo ./stetaddsrc.sh src1 "ens7 ens8"», где ens7 и ens8 – имена сетевых интерфейсов в ОС, которые будут использоваться для захвата сетевых потоков.

Успешная регистрация источника должна сопровождаться следующими сообщениями журнала регистрации:

```
«Created                               symlink                               /etc/systemd/system/multi-
user.target.wants/stet_anlz_threshold.service                               →
/usr/local/bin/stet_anlz_threshold.service.
Created      symlink      /etc/systemd/system/stet_anlz_threshold.service      →
/usr/local/bin/stet_anlz_threshold.service.».
```

Примечание. ПК Стетоскоп выполняет монопольный захват указанных сетевых интерфейсов. Совместное их использование с другим СПО невозможно. Последующий вызов команды «ip a» не покажет эти интерфейсы в списке сетевых интерфейсов ОС. Для возврата выбранных сетевых интерфейсов под управление ОС необходимо остановить службу захвата ПК «Дампер» командой «sudo systemctl stop stet_dmpr_src1.service», где src1 - выбранное название источника в ПК Стетоскоп. При повторном запуске сервиса, сетевые интерфейсы будут опять исключены из стека ОС. Следствием этого строго не рекомендуется выбирать сетевые интерфейсы управления ПК Стетоскоп на которых назначены IP-адреса. Аппаратная платформа перестанет быть доступной по этим IP-адресам.

6. Установка успешно завершена, источник захвата трафика зарегистрирован, интерфейс WEB-приложения должен быть доступен по IP-адресу управления аппаратной платформы, заданного при установке ОС. Логин по умолчанию для входа в интерфейс WEB-приложения – «admin», пароль по умолчанию – «passw0rd». После успешного первого входа в

интерфейс WEB-приложения строго рекомендуется сменить пароль по умолчанию пользователя «admin».

3.3 Удаление источника данных

Находясь в директории с файлами дистрибутива выполнить с правами суперпользователя ОС команду «sudo ./stetsrcdel.sh <название источника>», где название источника – это название переданное ранее в команде добавления источника «stetsrcadd.sh». В примере выше это название – «src1».

Примечание. В результате выполнения этой команды будут полностью удалены все данные источника, включая записанный трафик и его статистика. Если необходимо сохранить исходный записанный трафик, то перед выполнением команды необходимо предварительно сделать его резервную копию.

3.4 Удаление ПК Стетоскоп

Удаление ПК Стетоскоп не предусмотрено по причине внесения существенных изменений в настройки и модули ядра ОС и для выполнения удаления необходимо воспользоваться процедурой переустановки ОС.

4 АНАЛИЗАТОРЫ

ПК Стетоскоп содержит набор анализаторов. Анализаторы позволяют в автоматическом режиме выявлять различные признаки атак и аномалий. Архитектура программного комплекса позволяет расширять набор анализаторов, подключать новые анализаторы. Новые анализаторы разрабатываются ООО «ЦСС-Безопасность». По мере выхода новых анализаторов их установка производится в рамках обновления комплекса программ согласно с условиями лицензионного договора.

Анализаторы используют данные о захваченном трафике, которые состоят из исходных данных пакетов и сессий, а также из статистики трафика, полученной в результате первичной обработки. Для работы анализатора необходимо задать конфигурацию и фильтры. Фильтр – это в терминах КП Стетоскоп атомарное правило выявления аномалии или атаки. Каждый анализатор может иметь несколько независимых фильтров. Каждый фильтр содержит набор параметров. После изменения конфигурации или фильтров требуется перезапуск анализатора. Конфигурационные файлы и файлы фильтров анализаторов расположены в директории «*/etc/stet-3.0*».

Выходными данными анализаторов являются сообщения пользователю программного комплекса, которые регистрируются во внутренней базе данных, а также опционально регистрируются в системном журнале операционной системы (SYSLOG-журнал). По умолчанию регистрация в системном журнале ОС включена. Формат сообщений, регистрируемых в системном журнале, описан в Приложении 2.

Анализаторы регистрируют сообщения в SYSLOG-журнале, указывая в заголовке SYSLOG-сообщений следующие параметры:

- priority (facility | level) – тип программы и критичность,
- дата и время,
- tag – название программы,

- PID – идентификатор процесса.

Значение параметра типа программы (tag) указывает название анализатора. Точное значение для каждого анализатора указывается в разделе соответствующего анализатора ниже. Анализаторы используют два значения типа программы (facility):

- LOCAL0 – для системных сообщений анализатора, которые содержат информацию о предупреждениях и ошибках анализатора,

- LOCAL1 – для сообщений безопасности анализатора, которые возникают в процессе обработки заданных фильтров.

В составе дистрибутива КП Стетоскоп содержится файл конфигурации штатного демона «rsyslogd» («51-stet.conf») для выделения сообщений анализаторов в отдельные файлы по типу программы. Этот файл содержит пример перенаправления данных сообщений на требуемый IP-адрес коллектора SYSLOG-сообщений. Содержание файла конфигурации:

```
local0.*           /var/log/stet0.log
local1.*           /var/log/stet1.log
#local0,local1.*   @192.168.69.30
```

При установке ПК Стетоскоп файл «51-stet.conf» размещается по пути «/etc/rsyslog.d/». Для перенаправления SYSLOG-сообщений на внешний SYSLOG-коллектор необходимо в этом файле указать необходимый IP-адрес, убрать символ комментария «#» в начале строки и применить конфигурацию «rsyslogd» командой «systemctl restart rsyslog» с правами суперпользователя.

Примечание: В сообщении SYSLOG поля разделяются символом «|» (hex 7C - ASCII).

4.1 Анализатор пороговых значений

Анализатор пороговых значений реализует логику выявления превышения или недостижения заданных значений статистики захваченного сетевого трафика:

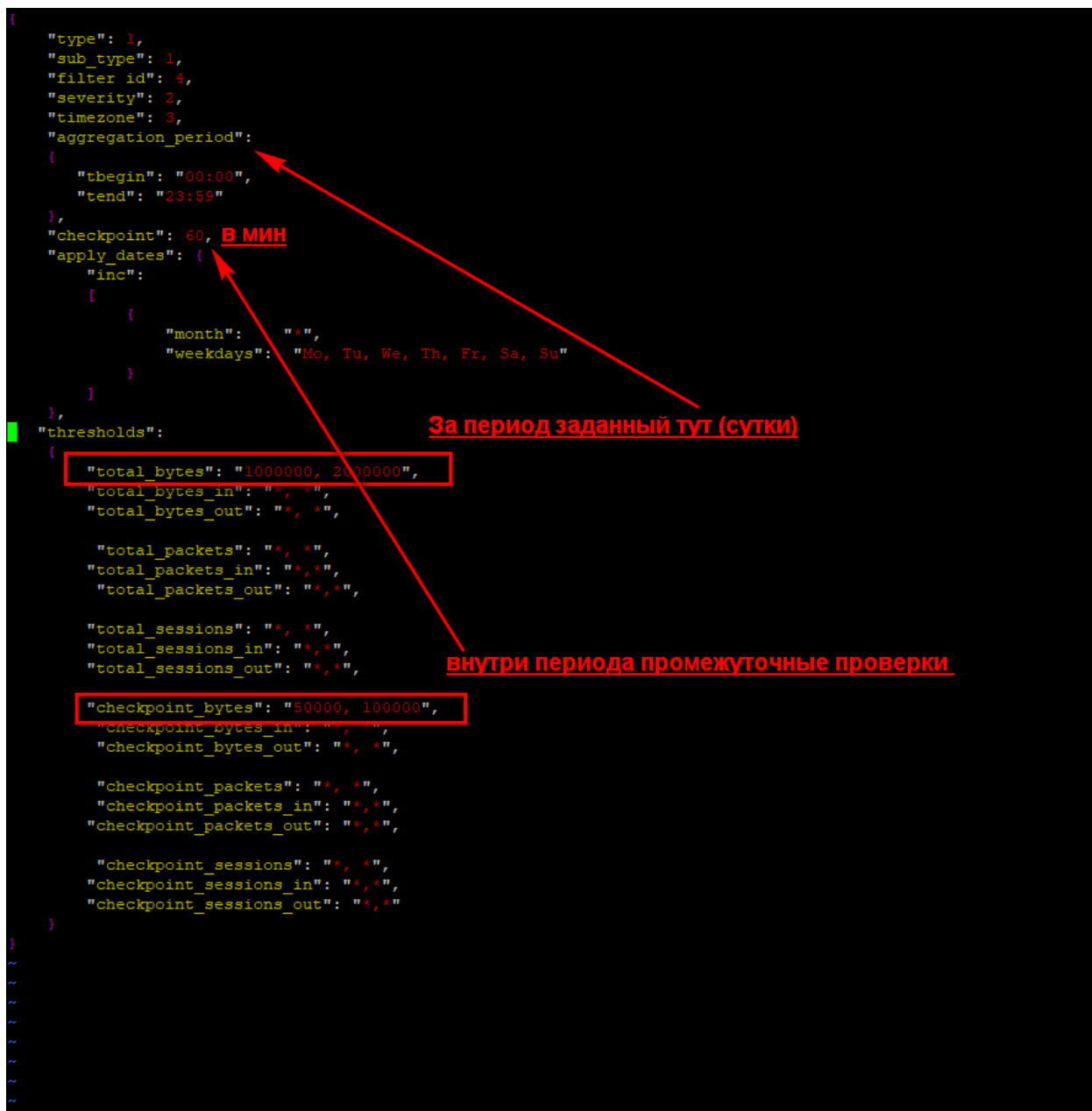
- выявление превышения порогового значения за период времени;
- выявление недостижения порогового значения за период времени;

Каждый фильтр порогового анализатора содержит два периода:

- общий период агрегации (aggregation_period),
- локальный период агрегации (checkpoint).

Общий период агрегации фильтра задается строго по времени начала и времени завершения и делится на несколько частей - локальные интервалы проверки (интервал проверки). Каждый фильтр включает указание его применимости в соответствии дням недели, месяцам и датам.

Пример фильтра анализатора пороговых значений указан на рисунке ниже:



В процессе обработки статистики трафика по заданным фильтрам анализатор пороговых значений выдает две группы сообщений. Первая группа сообщений – это основные сообщения, генерируемые в конце основного периода агрегации. Если задан период агрегации равный суткам, то в случае превышения или недостижения заданных порогов фильтра, сообщение будет сгенерировано в конце заданного периода один раз. Вторая группа – это вспомогательные (промежуточные) сообщения, которые генерируются внутри основного периода агрегации в конце локальных

периодов агрегации, в случае превышения или недостижения заданных порогов до окончания основного периода.

Конфигурационный файл анализатора пороговых значений расположен по пути: «*/etc/stet-3.0/stet_anlz_threshold.cfg*».

Директория с фильтрами расположена по пути: «*/etc/stet-3.0/stet_anlz_threshold*». Каждый файл в этой директории является отдельным фильтром и должен иметь расширение «*.json*». Анализатор пороговых значений поддерживает неограниченное количество фильтров. Фильтры задаются в формате JSON.

Значение параметра типа программы (tag) для SYSLOG-сообщений данного анализатора «*stet_anlz_thrld*».

Перезапуск анализатора выполняется командой «*sudo systemctl restart stet_anlz_threshold*».

Пример файла фильтра представлен в Приложении 1.

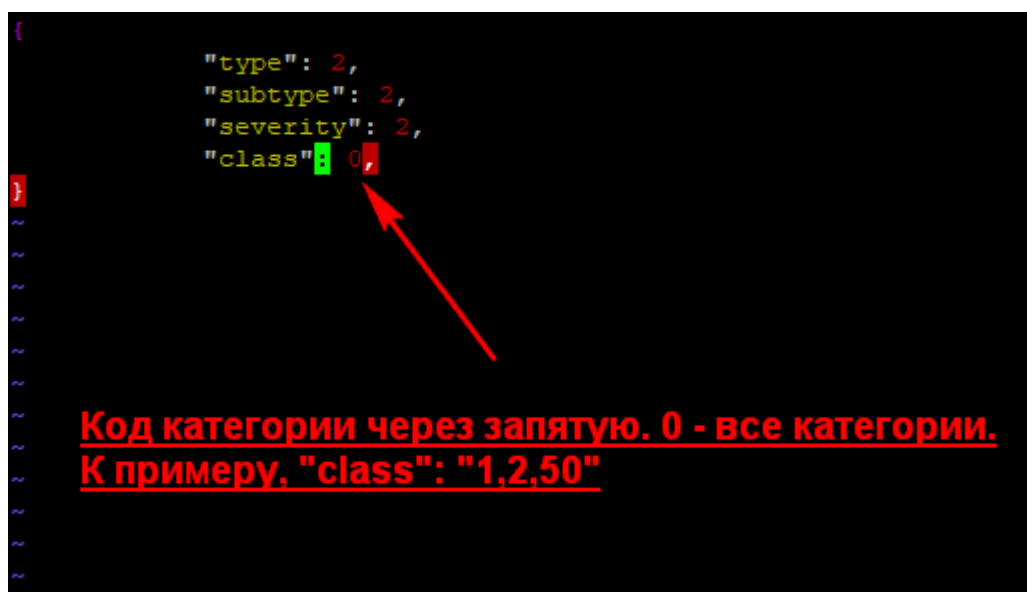
4.2 Анализатор подозрительных IP-адресов

Анализатор подозрительных IP-адресов (Анализатор badip) реализует логику выявления обращений к ресурсам сети Интернет, имеющим определенную характеристику, на основании базы данных списка IP-адресов сети Интернет и их классификации.

Каждый фильтр содержит перечисление номеров категорий IP-адресов, при обнаружении которых необходимо регистрировать сообщение. Анализатор при обнаружении сессии, содержащей IP-адрес из категории, заданной в фильтре, сразу регистрирует сообщение. Для сокращения количество сообщений, регистрируемых при обнаружении одних и тех же IP-адресов, попадающих в категории фильтра, предусмотрен параметр анализатора «*check-interval*». Этот параметр задает период времени в течение которого накапливается статистика обнаружения одного и того же IP-адреса, и по завершении этого периода регистрирует сообщение с информацией о

статистике обращений к каждому подозрительному IP-адресу. Перечень категорий подозрительных IP-адресов с номерами категорий указаны в Приложении 3 настоящего документа.

Пример фильтра анализатора пороговых значений указан на рисунке ниже:



Конфигурационный файл анализатора подозрительных IP-адресов расположен по пути: `«/etc/stet-3.0/stet_anlz_badip.cfg»`.

Директория с фильтрами расположена по пути: `«/etc/stet-3.0/stet_anlz_badip»`. Каждый файл в этой директории является отдельным фильтром и должен иметь расширение `«json»`. Анализатор подозрительных IP-адресов поддерживает неограниченное количество фильтров. Фильтры задаются в формате JSON.

Значение параметра типа программы (tag) для SYSLOG-сообщений данного анализатора `«stet_anlz_badip»`.

Перезапуск анализатора выполняется командой `«sudo systemctl restart stet_anlz_badip»`.

Пример файла фильтра представлен в Приложении 1.

5 ПРИЛОЖЕНИЕ 1. ПРИМЕРЫ ФИЛЬТРОВ АНАЛИЗАТОРОВ

5.1 Пример фильтра анализатора пороговых значений

Пример фильтра анализатора пороговых значений в формате JSON:

```
{
  "type": 1, // фильтр пороговых значений трафика
  "sub_type": 1, //подтип (без группировки)
  "filter id": 123, // уникальный id фильтра в рамках данного анализатора
  "severity": 1, //критичность событий (от 0 до 3)
  "timezone": 3, // часовой пояс для заданного в фильтре вр. интервала
  "aggregation period": //тег для периода агрегации
  {
    "tbegin": "09:00", //начало (24ч, без секунд)
    "tend": "19:00" //конец (24ч, без секунд)
  },
  "checkpoint": 15, // интервал проверки в минутах
  "apply dates":
  {
    "inc": // применить ко всем датам в массиве структур ниже
    [
      {
        # Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec или "*"
        "month": "Jan - May, Jul",
        "dates": "*" // или "1,2, 20-31",
        "weekdays": "Mo - Fr, Su" // Mo, Tu, We, Th, Fr Sa, Su или *
      },
      {
        "month": "Sep - Dec",
        "dates": "1,2, 20-31",
        "weekdays": "*" // "*" - является default-ым значением
      }
    ],
    "exc": // исключить даты ниже
    [
      {
        "month": "Jan",
        "dates": "1-10",
        "weekdays": "*"
      },
      {
        "month": "May",
        "dates": "1-4",
        "weekdays": "*"
      },
      {
        "month": "Jun",
        "dates": "12",
        "weekdays": "*"
      }
    ]
  },
  "thresholds":
  {
    // При отсутствии любого из пороговых параметров, его значение задается по умолчанию как "*", "*"
    "total_bytes": "50000, *" // max,min в байтах за весь период
  }
}
```

```

"total_bytes_in": "5000, 1000" // max,min вх. байт за весь период
"total_bytes_out": "*, 1000" // max,min исх. байт за весь период

"total_packets": "500, 200" // max,min пакетов за весь период
"total_packets_in": "*,*" // max,min вх. пакетов за весь период
"total_packets_out": "400,*" // max,min исх. пакетов за весь период

"total_sessions": "2000, 500" // max,min сессий за весь период
"total_sessions_in": "300,*" // max,min вх. сессий за весь период
"total_sessions_out": "*,200" // max,min исх. сессий за весь период

"checkpoint_bytes": "500, *" // max,min в байтах за checkpoint
"checkpoint_bytes_in": "500, 100" // max,min вх. байт за checkpoint
"checkpoint_bytes_out": "*, 100" // max,min исх. байт за checkpoint

"checkpoint_packets": "500, 20" // max,min пакетов за checkpoint
"checkpoint_packets_in": "*,*" // max,min вх. пакетов за checkpoint
"checkpoint_packets_out": "300,*" // max,min исх. пакетов за checkpoint

"checkpoint_sessions": "200, 50" // max,min сессий за checkpoint
"checkpoint_sessions_in": "30,*" // max,min вх. сессий за checkpoint
"checkpoint_sessions_out": "*,20" // max,min исх. сессий за checkpoint
},

"protocols":
{
  "net_IPv4": //тег для фильтруемых IPv4-адресов
  {
    "transport_tcp":
    {
      "addr": //тег для фильтруемых IPv4-адресов
      {
        "loc":
        {
          "inc": "*,",
          "exc": "192.168.0.1-192.168.250.255,192.168.15.20"
        },
        "rem":
        {
          "inc": "212.34.54.122, 27.122.20.6" // удл. адреса
        }
      },
      "ports": //тег для фильтруемых портов для TCP
      {
        "loc": // Локальные порты
        {
          "inc": "1025-9000, 10000",
          "exc": "2000, 2001"
        },
        "rem": // Удаленные порты
        {
          "inc": "80, 443, 9000-10000",
          "exc": "9090"
        },
      },
    }
  }
  "proto": //тег для фильтруемых протоколов (приклад + сервис)
  {
    "inc":
    {
      "proto_set": [ "HTTP", "HTTPS", "SSH", "SMTP" ]
    }
  }
}

```

```

    },
    "exc":
    {
        "proto_set": [ "hotmail.com", "mail.ru" ]
    }
},

"transport_udp":
{
    "addr": "*", //тег для фильтруемых IPv4-адресов
    "ports": "*", //тег для фильтруемых портов UDP
    "proto": //тег для фильтруемых протоколов (2 уровня)
    {
        "inc":
        {
            "SKYPE": ["*"],
            "DNS": ["*"]
        }
    }
},

"transport_other":
{
    "addr": //тег для фильтруемых IPv4-адресов
    {
        "loc": "*", // лок. адреса
        "rem":
        {
            "inc": "237.10.208.9" // удл. адреса
        }
    }
},

"net_Ipv6": //тег для фильтруемых IPv6-адресов
{
    "transport_tcp":
    {
        "addr": //тег для фильтруемых IPv6-адресов
        {
            "loc":
            {
                "inc": "2:3:5:::1-8:9:4:::2, 23::1" // локальные адреса
            }
            "rem": "*" // удаленные адреса
        },
        "ports": "*", //тег для фильтруемых портов для IPv6
        "proto": "*" //тег для фильтруемых протоколов (приклад + сервис)
    },

    "transport_udp": "*",
    "transport_other":
    {
        "addr": //тег для фильтруемых IPv6-адресов
        {
            "loc": "*", // лок. адреса
            "rem": // удл. адреса
            {
                "inc": "23::1"
            }
        }
    }
}

```

```

    }
  }
},
"net_other": //тег для не IP-протоколов
{
  "addr": // MAC адреса
  {
    "inc": "*",
    "exc": "12:67:AF:E2:11:89, 11:22:33:AA:A6:B7"
  }
}
}

```

5.2 Пример фильтра анализатора подозрительных IP-адресов

Пример фильтра анализатора подозрительных IP-адресов в формате JSON:

```

{
  "type": 2,
  "sub_type": 1, //подтип (без группировки)
  "severity": 1, //критичность событий
  "ip": //тег для фильтруемых IP-адресов
  {
    "in": "192.168.0.1--192.168.250.255", //фильтруемые локальные адреса
  },
  "class": "1, 3, 4, 51", //фильтрация только по указанным классам (в примере использованы классы,
  связанные со спамом)
}

```

6 ПРИЛОЖЕНИЕ 2. СООБЩЕНИЯ АНАЛИЗАТОРОВ

6.1 Структура и поля сообщений порогового анализатора

Пример основного сообщения (общий период агрегации), регистрируемого в стандартном системном журнале ОС Linux, управляемом сервисом «rsyslogd»:

```

May 15 18:01:16 stet_1-30 stet_anlz_thrld[16186]: d4e78fc5-f986-3e4f-
b576-de6bb9c6e7da/a857384a-39fe-ac11-0afa-665a850632a5/1/2022-05-05
20:59:00/2022-05-05 20:59:00/Thresholds
analyzer|src1|2|11|1|<b>Агрегационный интервал: </b>23 ч. 59 мин. [00:00 --
23:59] </br><b>Интервал проверки: </b>60 мин </br><b>Часовой пояс:
</b> UTC +3 ч </br></br><b>Даты:</b> </br> +месяц: * | день недели:
Mo, Tu, We, Th, Fr, Sa, Su</br></br><b>Пороги (интервал проверки):
</b></br>-- Трафик: 48.83 Кб, 97.66 Кб</br></br><b>Пороги
(агрегационный интервал): </b> </br>-- Трафик: 976.56 Кб, 1.91
Мб</br>|4|nBytesSum|0|0|0|0|0|0|0|0|0|<Статистика трафика в формате
HTML>/

```

Регулярное выражение для разбора (синтаксис языка Python):

[illegible]

Цветовое разделение полей представлено на рисунке ниже:

```
May 15 18:01:16 stet_1-30 stet_anlz_thrld[16186]: d4e78fc5-f986-3e4f-b576-
de6bb9c6e7da|a857384a-39fe-ac11-0afa-665a850632a5|1|2022-05-05 20:59:00|2022-05-05
20:59:00|Thresholds analyzer|src1|2|11|1|<b>Арперационный интервал: </b>23 ч. 59
мин. [00:00 -- 23:59] </br><b>Интервал проверки: </b>60 мин </br><b>Часовой пояс:
</b> UTC +3 ч </br></br><b>Даты:</b> </br> +месяц: * | день недели: Мо, Ту, We,
Th, Fr, Sa, Su</br></br><b>Пороги (интервал проверки): </b></br>-- Трафик: 48.83
Кб, 97.66 Кб</br></br><b>Пороги (арперационный интервал): </b> </br>-- Трафик:
976.56 Кб, 1.91 Мб</br>|4|nBytesSum|0|0|0|0|0|0|0|0|0|0|<Статистика трафика в
формате HTML>|
```

Семантика полей и возможные значения полей сообщения о событии (в порядке следования в SYSLOG-сообщении) представлена в таблице ниже:

№	Описание поля	Пример значения	Ограничения
1	Глобальный идентификатор события	<i>d4e78fc5-f986-3e4f-b576-de6bb9cbe7da</i>	-
2	Глобальный идентификатор сообщения	a857384a-39fe-ac11-0afa-665a850632a5	-
3	Уровень вложенности сообщения	1	1 - сейчас применяется одно значение
4	Дата и время возникновения события на датчике (С точностью до секунды). Реальная дата и время события когда оно произошло.	2022-05-05 20:59:00	-
5	Дата и время регистрация события в БД.	2022-05-05 20:59:00	-
6	Название программного анализатора	Thresholds analyzer	-
7	Название источника	src1	-
8	Код критичности события.	2	0 – инфо, 1 – низкий, 2 – средний, 3 – высокий.
9	Идентификатор типа сообщения	11	Целое положительное 32-битное число
10	Идентификатор типа события	1	Целое положительное 32-битное число
11	Описание сработавшего фильтра	Агрегационный интервал: 23 ч. 59 мин. [00:00 -- 23:59] Интервал проверки: 60 мин Часовой пояс: UTC +3 ч	-

		</br></br>Даты: </br> +месяц: * день недели: Mo, Tu, We, Th, Fr, Sa, Su</br></br>Пороги (интервал проверки): </br>-- Трафик: 48.83 Кб, 97.66 Кб</br></br>Пороги (агрегационный интервал): </br>-- Трафик: 976.56 Кб, 1.91 Мб</br>	
12	Идентификатор сработавшего фильтра	4	Задается в конфигурации фильтра пользователем в поле "filter id"
13	Поля агрегации статистики, которые превысили пороги	nBytesSum	-
14	Кол-во входящих пакетов за весь период	0	-
16	Кол-во исходящих пакетов за весь период	0	-
17	Общее кол-во пакетов за весь период	0	-
18	Кол-во входящих байт за весь период	0	-
19	Кол-во исходящих байт за весь период	0	-
20	Общее кол-во байт за весь период	0	-
21	Кол-во исходящих сессий за весь период	0	-
22	Кол-во входящих сессий за весь период	0	-
23	Общее кол-во сессий за весь	0	-

	период		
33	Детальная информация о событии	<Статистика трафика в формате HTML>	-

Пример вспомогательного сообщения (локальный период агрегации/интервал проверки), регистрируемого в стандартном системном журнале ОС Linux, управляемом сервисом «rsyslogd»:

```
May 15 20:19:49 stet_1-30 stet_anlz_thrld [24116]: 0b1007bc-24b6-0547-9cd1-4cd19cd5d16c/4d04f54b-5570-8213-c59d-9e0506239fbc/1/2022-05-13
12:00:00/2022-05-13 12:00:00/Thresholds
analyzer|src1|2|1|1|<b>Агрегационный интервал: </b>23 ч. 59 мин. [00:00 --
23:59] </br><b>Интервал проверки: </b>60 мин </br><b>Часовой пояс:
</b> UTC +3 ч </br></br><b>Даты:</b> </br> +месяц: * | день недели:
Mo, Tu, We, Th, Fr, Sa, Su</br></br><b>Пороги (интервал проверки):
</b></br>-- Трафик: 48.83 Кб, 97.66 Кб</br></br><b>Пороги
(агрегационный интервал): </b> </br>-- Трафик: 976.56 Кб, 1.91
Мб</br>|4|1|nBytesSumLoc,nBytesSum|2492|49022|51514|266118|3215836|3481
954|0|0|0|150896|836710|987606|156873156|57549264|214422420|0|0|0|<Стат
истика трафика в формате HTML>|
```

Регулярное выражение для разбора (синтаксис языка Python):

```
(.*[/[d]+/]): ([da-f-+])\([da-f-+])\([d]+)\([d\d\d\d-d\d-d\d\d\d:
\d\d:\d\d:\d\d)\([d\d\d\d-d\d-d\d\d\d
\d\d:\d\d:\d\d)\([.]*\([.]*\([d]\([d]\([d]\([.]*\([d]\([d]\([.]*\([d+]\([d+]\([d+]\([d
+)\([d+)\([d+)\([d]\([d]\([d]\([d+)\([d+)\([d+)\([d+)\([d+)\([d+)\([d]\([d]\([
d]\([.]*)/
```

Цветовое разделение полей представлено на рисунке ниже:

```
May 15 20:19:49 stet_1-30 [24116]: 0b1007bc-24b6-0547-9cd1-4cd19cd5d16c|4d04f54b-
5570-8213-c59d-9e0506239fbc|1|2022-05-13 12:00:00|2022-05-13 12:00:00|Thresholds
analyzer|src1|2|1|1|<b>Агрегационный интервал: </b>23 ч. 59 мин. [00:00 -- 23:59]
</br><b>Интервал проверки: </b>60 мин </br><b>Часовой пояс: </b> UTC +3 ч </br>
</br><b>Даты:</b> </br> +месяц: * | день недели: Mo, Tu, We, Th, Fr, Sa, Su</br>
</br><b>Пороги (интервал проверки): </b></br>-- Трафик: 48.83 Кб, 97.66 Кб</br>
</br><b>Пороги (агрегационный интервал): </b> </br>-- Трафик: 976.56 Кб, 1.91
Мб</br>|4|1|nBytesSumLoc,nBytesSum|2492|49022|51514|266118|3215836|3481954|0|0|0|1
50896|836710|987606|156873156|57549264|214422420|0|0|0|<Статистика трафика в
формате HTML>|
```

Семантика полей и возможные значения полей сообщения о событии (в порядке следования в SYSLOG-сообщении) представлена в таблице ниже:

№	Описание поля	Пример значения	Ограничения
1	Глобальный идентификатор события	<i>0b1007bc-24b6-0547-9cd1-4cd19cd5d16c</i>	-
2	Глобальный идентификатор сообщения	<i>4d04f54b-5570-8213-c59d-9e0506239fbc</i>	-
3	Уровень вложенности сообщения	1	1 - сейчас применяется одно значение
4	Дата и время возникновения события на датчике (С точностью до секунды). Реальная дата и время события когда оно произошло.	<i>2022-05-13 12:00:00</i>	-
5	Дата и время регистрация события в БД.	<i>2022-05-13 12:00:00</i>	-
6	Название программного анализатора	<i>Thresholds analyzer</i>	-
7	Название источника	<i>src1</i>	-
8	Код критичности события.	2	0 – инфо, 1 – низкий, 2 – средний, 3 – высокий.
9	Идентификатор типа сообщения	<i>1</i>	Целое положительное 32-битное число
10	Идентификатор типа события	<i>1</i>	Целое положительное 32-битное число
11	Описание сработавшего	<i>Агрегационный интервал: 23 ч. 59 мин. [00:00 -- 23:59]</i>	-

	фильтра	</br>Интервал проверки: 60 мин </br>Часовой пояс: UTC +3 ч </br></br>Даты: </br> +месяц: * день недели: Мо, Tu, We, Th, Fr, Sa, Su</br></br>Пороги (интервал проверки): </br>- - Трафик: 48.83 Кб, 97.66 Кб</br></br>Пороги (агрегационный интервал): </br>-- Трафик: 976.56 Кб, 1.91 Мб</br>	
12	Идентификатор сработавшего фильтра	1	Задается в конфигурации фильтра пользователем в поле "filter id"
13	Количество полей агрегации статистики, превысивших пороги фильтра (hints)	1	Целое положительное 32-битное число
14	Поля агрегации статистики, которые превысили пороги	nBytesSumLoc,nBytesSum	-
15	Кол-во входящих пакетов за промежуточный период	2492	-
16	Кол-во исходящих пакетов за промежуточный период	49022	-
17	Общее кол-во пакетов за промежуточный период	51514	-
18	Кол-во входящих байт за промежуточный	266118	-

	период		
19	Кол-во исходящих байт за промежуточный период	3215836	-
20	Общее количество байт за промежуточный период	3481954	-
21	Кол-во исходящих сессий за промежуточный период	0	-
22	Кол-во входящих сессий за промежуточный период	0	-
23	Общее кол-во сессий за промежуточный период	0	-
24	Кол-во входящих пакетов за весь период	150896	-
25	Кол-во исходящих пакетов за весь период	836710	-
26	Общее кол-во пакетов за весь период	987606	-
27	Кол-во входящих байт за весь период	156873156	-
28	Кол-во исходящих байт за весь период	57549264	-
29	Общее кол-во байт за весь период	214422420	-
30	Кол-во исходящих сессий за весь период	0	-
31	Кол-во входящих	0	-

Семантика полей и возможные значения полей сообщения о событии (в порядке следования в SYSLOG-сообщении) представлена в таблице ниже:

№	Описание поля	Пример значения	Ограничения
1	Глобальный идентификатор события	<i>3dec1fee-7409-8f42-a255-16184b826bfc</i>	-
2	Глобальный идентификатор сообщения	<i>f0ff8f4e-58cd-2633-c3b1-d97bd825db87</i>	-
3	Уровень вложенности сообщения	1	1 - сейчас применяется одно значение
4	Дата и время возникновения события на датчике (С точностью до секунды). Реальная дата и время события когда оно произошло.	<i>2022-05-12 09:35:00</i>	-
5	Дата и время регистрация события в БД.	<i>2022-05-24 09:19:22</i>	-
6	Название программного анализатора	<i>Bad IP analyzer</i>	-
7	Название источника	<i>src1</i>	-
8	Код критичности события.	2	0 – инфо, 1 – низкий, 2 – средний, 3 – высокий.
9	Описание сработавшего фильтра	<i>тип - с группировкой по локальным IP, интервал проверки: [2022-05-12 11:38--2022-05-12 12:38], класс адресов - фильтрация всех существующих классов</i>	-
9	Идентификатор сработавшего фильтра	<i>808821328</i>	
10	Идентификатор типа сообщения	3	Целое положительное 32-битное число
11	Идентификатор типа события	2	Целое положительное

			32-битное число
12	Тип IP-адреса	0	Признак типа IP: 0 – IPv4; 1 – IPv6; 2 – нет IP
13	IP-адрес источника	192.168.69.204	-
14	IP-адрес получателя	1.0.136.29	-
15	Порт (TCP/UDP) источника	54204	-
16	Порт (TCP/UDP) получателя	445	-
17	Идентификатор города	13175	-
18	Идентификатор страны	1520	-
19	Идентификатор класса характеристики IP-адреса	2	-
20	Количество входящих байт	0	-
21	Количество исходящих байт	296	-
22	Суммарное количество байт	296	-
23	Количество входящих сессий	0	-
24	Количество исходящих сессий	2	-
25	Суммарное количество сессий	2	-
26	Описание класса характеристики IP-адреса	Fake Google Bot	-
27	Протокол (транспортный/прикладной)	TCP/SMBv23	-
28	Глобальный идентификатор сетевой сессии	{943d81e0-d6d1-ec11-92a7-5254003cc1d5}	-

Пример сообщения с информацией о статистике обращений к каждому подозрительному IP-адресу, регистрируемом в стандартном системном журнале ОС Linux, управляемом сервисом «rsyslogd»:

May 14 09:19:22 stet_1-30 stet_anlz_badip[6074]: 3dec1fee-7409-8f42-a255-16184b826bfc/28f2ae4b-9945-fc13-8db2-3d69ab0e66a5/0/2022-05-12 09:38:00/2022-05-24 09:19:22|Bad IP analyzer|src1|2|mun - с группировкой по локальным IP, интервал проверки: [2022-05-12 11:38--2022-05-12 12:38], класс адресов - фильтрация всех существующих классов|808821328/5/2/0/0.0.0/1.0.136.29/54204/445/13175/1520/2/444/120/56 4/0/2/2/Fake Google Bot/ |192.168.69.204 -> 25:1.0.136.29, Сессий: 1, Пакетов : 4, Трафик (б): 296 #012 192.168.69.204 -> 445:1.0.136.29, Сессий: 1, Пакетов : 4, Трафик (б): 268 #012 |

Регулярное выражение для разбора (синтаксис языка Python):

[illegible]

Цветовое разделение полей представлено на рисунке ниже:

```
May 14 09:19:22 stet_1-30 stet_anlz_badip[6074]: 3dec1fee-7409-8f42-a255-
16184b826bfc|28f2ae4b-9945-fc13-8db2-3d69ab0e66a5|0|2022-05-12 09:38:00|2022-05-24
09:19:22|Bad IP analyzer|src1|2|тип - с группировкой по локальным IP, интервал
проверки: [2022-05-12 11:38--2022-05-12 12:38], класс адресов - фильтрация всех
существующих
классов|808821328|5|2|0|0.0.0.0|1.0.136.29|54204|445|13175|1520|2|444|120|564|0|2|
2|Fake Google Bot||192.168.69.204 -> 25:1.0.136.29, Сессий: 1, Пакетов : 4,
Трафик (б): 296 #012 192.168.69.204 -> 445:1.0.136.29, Сессий: 1, Пакетов : 4,
Трафик (б): 268 #012 |
```

Семантика полей и возможные значения полей сообщения о событии (в порядке следования в SYSLOG-сообщении) представлена в таблице ниже:

№	Описание поля	Пример значения	Ограничения
1	Глобальный идентификатор события	<i>3dec1fee-7409-8f42-a255-16184b826bfc</i>	-
2	Глобальный идентификатор сообщения	<i>28f2ae4b-9945-fc13-8db2-3d69ab0e66a5</i>	-
3	Уровень вложенности сообщения	<i>0</i>	1 - сейчас применяется одно значение
4	Дата и время	<i>2022-05-12 09:38:00</i>	-

	возникновения события на датчике (С точностью до секунды). Реальная дата и время события когда оно произошло.		
5	Дата и время регистрация события в БД.	2022-05-24 09:19:22	-
6	Название программного анализатора	<i>Bad IP analyzer</i>	-
7	Название источника	<i>src1</i>	-
8	Код критичности события.	2	0 – инфо, 1 – низкий, 2 – средний, 3 – высокий.
9	Описание сработавшего фильтра	<i>тип - с группировкой по локальным IP, интервал проверки: [2022-05-12 11:38--2022-05-12 12:38], класс адресов - фильтрация всех существующих классов</i>	-
9	Идентификатор сработавшего фильтра	808821328	-
10	Идентификатор типа сообщения	5	Целое положительное 32-битное число
11	Идентификатор типа события	2	Целое положительное 32-битное число
12	Тип IP-адреса	0	Признак типа IP: 0 – IPv4; 1 – IPv6; 2 – нет IP
13	IP-адрес источника	192.168.69.204	-
14	IP-адрес получателя	1.0.136.29	-
15	Порт (TCP/UDP) источника	54204	-
16	Порт (TCP/UDP) получателя	445	-
17	Идентификатор города	13175	-
18	Идентификатор страны	1520	-
19	Идентификатор класса	2	-

	характеристики IP-адреса		
20	Количество входящих байт	444	
21	Количество исходящих байт	120	
22	Суммарное количество байт	564	
23	Количество входящих сессий	0	
24	Количество исходящих сессий	2	
25	Суммарное количество сессий	2	
26	Описание класса IP-адреса	<i>Fake Google Bot</i>	
27	Протокол		
28	Детальная информация о событии	<p>192.168.69.204 -> 25:1.0.136.29, Сессий: 1, Пакетов : 4, Трафик (б): 296 #012</p> <p>192.168.69.204 -> 445:1.0.136.29, Сессий: 1, Пакетов : 4, Трафик (б): 268 #012</p>	

7 ПРИЛОЖЕНИЕ 3. ПЕРЕЧЕНЬ КАТЕГОРИЙ ПОДОЗРИТЕЛЬНЫХ IP-АДРЕСОВ

Перечень категорий подозрительных IP-адресов и их номеров представлен на рисунке ниже:

No	Blacklist Bot/Crawler Type	Blacklist ID
1	Unknown Spam Bot masking himself as a normal user	1
2	Fake Google Bot	2
3	Spam DTS Agent - Beijing Express Email Address Extractor	3
4	Spam Bot - Advanced Email Extractor	4
5	HTTrack Offline Browser - Website Extractor	5
6	80 legs Web Crawler - Website Extractor	6
7	SEOpProfiler Bot - Website Extractor	7
8	Majestic12 Web Crawler - Website Extractor	8
9	Ezzooms Web Crawler - Website Extractor	9
10	Warebay Web Crawler - Website Extractor	10
11	Nuisance little known/unknown Crawler - Website Extractor	11
12	Ahrefs Web Crawler - Website Extractor	12
13	ProximiC Web Crawler - Website Extractor	13
14	Sistrix Web Crawler - Website Extractor	14
15	SemrushBot Crawler - Website Extractor	15
16	Commoncrawl Crawler - Website Extractor	16
17	Fake Bing Bot	17
18	Fake Baidu Bot	18
19	Fake Yahoo Bot	19
20	User Submission - Hacker from this IP	50
21	User Submission - Spam from this IP	51
22	User Submission - Obtrusive Bot	52
23	User Submission - Other	53

8 ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АИС	– Автоматизированная информационная система
ОС	– Операционная система
ФС	– Файловая система
FTP	– File Transfer Protocol – протокол передачи данных
IDS	– Служба обнаружения компьютерных атак
NTP	– Network Time Protocol – протокол синхронизации времени в сети
RPM	– RPM (Red Hat Package Manager) – средство поиска, загрузки и установки пакетов программ, а также получения информации об установленных пакетах и их удалении в Linux от Red Hat
SPAN-порт	– Switched Port Analyzer коммутатора сети
IP	– Internet Protocol – «межсетевой протокол» маршрутизируемый протокол сетевого уровня стека TCP/IP
ICMP	– Internet Control Message Protocol — протокол межсетевых управляющих сообщений
SMTP	– Simple Mail Transfer Protocol – простой протокол передачи почты
HTTP	– HyperText Transfer Protocol – протокол передачи гипертекста
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
BSD	– Berkeley Software Distribution- система распространения программного обеспечения в исходных текстах
COM	– Communication port – последовательный порт
CEF	– ArcSight Common Event Format – формат передачи СИ
CPU	– Central Processing Unit – центральное процессорное устройство
SSL	– Secure Sockets Layer – уровень защищённых сокетов

[illegible]