

УТВЕРЖДЕН

RU.АЦВТ.62.01.29-01 34 01-ЛУ

Программный комплекс invGUARD СЕКАТОР

**Руководство оператора**

RU.АЦВТ.62.01.29-01 34 01

Листов 34

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
0192	 12.01.2024			

## **АННОТАЦИЯ**

В данном программном документе приведено руководство оператора по применению и эксплуатации программного изделия «Программный комплекс invGUARD СЕКАТОР» (далее – Очиститель или ПК invGUARD СЕКАТОР).

В разделе «Назначение программы» указаны сведения о назначении программы и информация, достаточная для понимания функций программы и ее эксплуатации.

В разделе «Условия выполнения программы» указаны условия, необходимые для выполнения программы (минимальный состав аппаратных и программных средств и т.п.).

В разделе «Выполнение программы» указана последовательность действий оператора, обеспечивающих загрузку, запуск, выполнение и завершение программы, приведено описание функций, формата и возможных вариантов команд, с помощью которых оператор осуществляет загрузку и управляет выполнением программы.

В разделе «Сообщения оператору» приведены тексты сообщений, выдаваемых в ходе выполнения программы.

Оформление программного документа «Руководство оператора» произведено по требованиям ЕСПД (ГОСТ 19.101-77, ГОСТ 19.103-77, ГОСТ 19.104-78, ГОСТ 19.105-78, ГОСТ 19.106-78, ГОСТ 19.505-79, ГОСТ 19.604-78).

## СОДЕРЖАНИЕ

АННОТАЦИЯ	1
1. НАЗНАЧЕНИЕ ПРОГРАММЫ	4
1.1 Функциональное назначение программы	4
1.2 Эксплуатационное назначение программы	4
1.3 Состав функций	4
2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ	6
2.1 Необходимый состав аппаратных средств	6
2.2 Минимальный состав программных средств	6
3. ВЫПОЛНЕНИЕ ПРОГРАММЫ	10
3.1 Загрузка и запуск программы	10
3.2 Использование веб-интерфейса программы	10
3.2.1 Введение	10
3.2.2 Принятие сертификата	10
3.2.3 Использование веб-интерфейса Анализатора	10
3.2.4 Использование сервисного веб-интерфейса Очистителя	25
3.3 Завершение программы	30
4. СООБЩЕНИЯ ОПЕРАТОРУ	31
ПРИЛОЖЕНИЕ 1	32
ПРИЛОЖЕНИЕ 2	33
Лист регистрации изменений	34

## **1. НАЗНАЧЕНИЕ ПРОГРАММЫ**

### **1.1 Функциональное назначение программы**

Функциональным назначением Очистителя является защита от угроз безопасности информации, направленных на отказ в обслуживании (DoS и DDoS-атак), информационных систем (ИС) и автоматизированных систем управления (АСУ), функционирующих на базе вычислительных сетей, посредством фильтрации вредоносного трафика, статистических данных по обработанному трафику.

### **1.2 Эксплуатационное назначение программы**

Очиститель разработан для применения как совместно с анализаторами трафика (программными комплексами invGUARD AS-SW или invGUARD AI-SW), так и самостоятельно.

Пользователями Очистителя должны быть специалисты в области сетевой безопасности, ответственные за эксплуатацию телекоммуникационного оборудования или администраторы безопасности.

### **1.3 Состав функций**

Очиститель обеспечивает возможность выполнения перечисленных ниже функций:

1) Интеллектуальная фильтрация сетевого трафика, на основании полученных заданий:

- от программных комплексов invGUARD AS-SW или invGUARD AI-SW (анализаторов трафика);

- от внешних программ посредством собственного программного интерфейса управления (API);

- сформированных с использованием собственного графического интерфейса пользователя.

2) Сбор статистических данных о пропущенном и обработанном трафике, отображение их в пользовательском интерфейсе и передача Анализатору трафика или другой программе с использованием собственного API.

## **2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ**

### **2.1 Необходимый состав аппаратных средств**

Минимальный состав используемых технических (аппаратных) средств:

- 1) сервер на базе процессора Intel Xeon с 8 и более вычислительными ядрами и частотой не менее 2,0 ГГц;
- 2) оперативная память объемом не менее 32 Гб;
- 3) жесткий диск объемом 500 Гб и выше;
- 4) сетевой порт Ethernet для управления;
- 5) сетевая карта, поддерживающая технологию XDP для обеспечения пропуска входящего и исходящего трафика.

### **2.2 Минимальный состав программных средств**

Для обеспечения функционирования Очистителя на сервере должна быть установлена и сконфигурирована серверная операционная система Debian версий 12.

### **2.3 Требования и условия технического и технологического характера**

Очиститель может применяться как с использованием Анализатора трафика, так и без.

Логически Очиститель подключается к двум сетям:

Внешней сети – сеть, из которой приходит трафик, требующий очистки;

Внутренней сети – сеть, в которой расположены защищаемые ресурсы.

Используется асимметричная схема подключения, при которой Очиститель «видит» трафик только в одном направлении – из внешней сети во внутреннюю.

В нормальном режиме работы вычислительной сети («Без атаки») трафик из внешней сети направляется непосредственно во внутреннюю сеть. Очиститель не оказывает влияние на трафик.

В аномальном режиме работы вычислительной сети («Под атакой») маршрут прохождения трафика в защищаемую сеть изменяется посредством отправки BGP-анонса на пограничный маршрутизатор, и трафик из внешней сети направляется во внутреннюю сеть через Очиститель. Маршрут обратного трафика (из защищаемой сети во внешнюю сеть) в данном случае не изменяется.

Возможно использование Очистителя в режиме постоянной фильтрации трафика из внешней во внутреннюю сеть. В таком случае схема его применения аналогична варианту «Под атакой».

Для обеспечения работы Очистителя требуется реализация схемы включения в сегмент вычислительной сети с учетом типовых схем применения.

### 2.3.1 Типовая схема применения Очистителя в ИС и АСУ «Без атаки» с использованием Анализатора трафика – см. Рисунок 1.

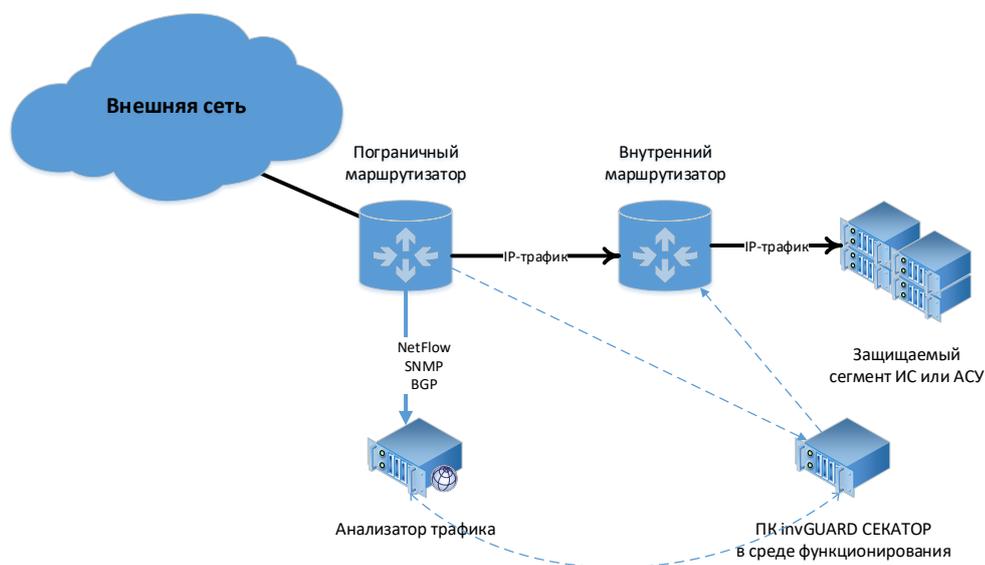


Рисунок 1 – Типовая схема применения Очистителя в ИС и АСУ «Без атаки» с использованием Анализатора трафика

### 2.3.2 Типовая схема применения Очистителя в ИС и АСУ «Под атакой» с использованием Анализатора трафика – см. Рисунок 2.

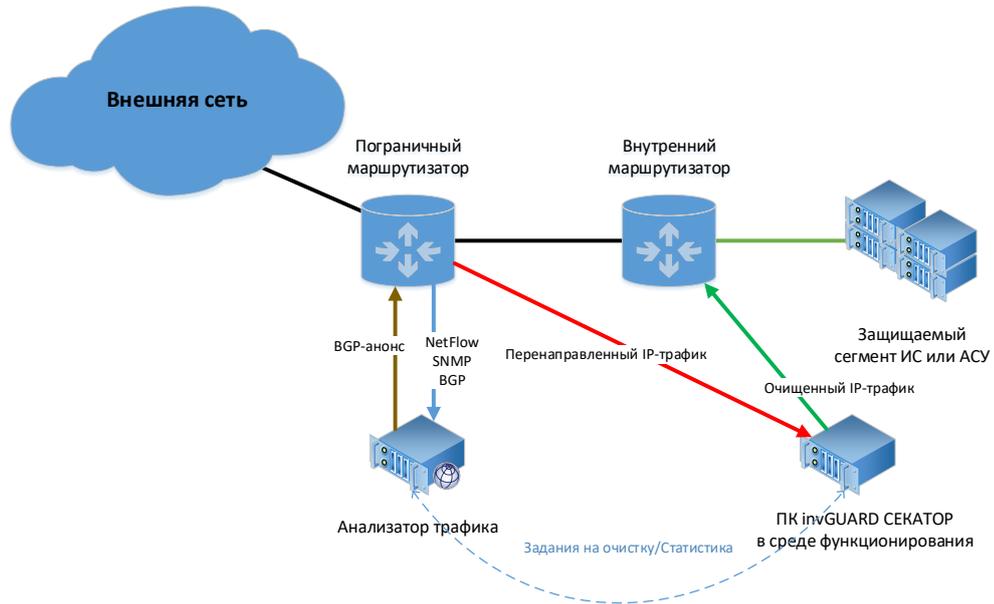


Рисунок 2 – Типовая схема применения Очистителя в ИС и АСУ «Под атакой» с использованием Анализатора трафика

### 2.3.3 Типовая схема применения Очистителя в ИС и АСУ «Без атаки» без использования Анализатора трафика – см. Рисунок 3.

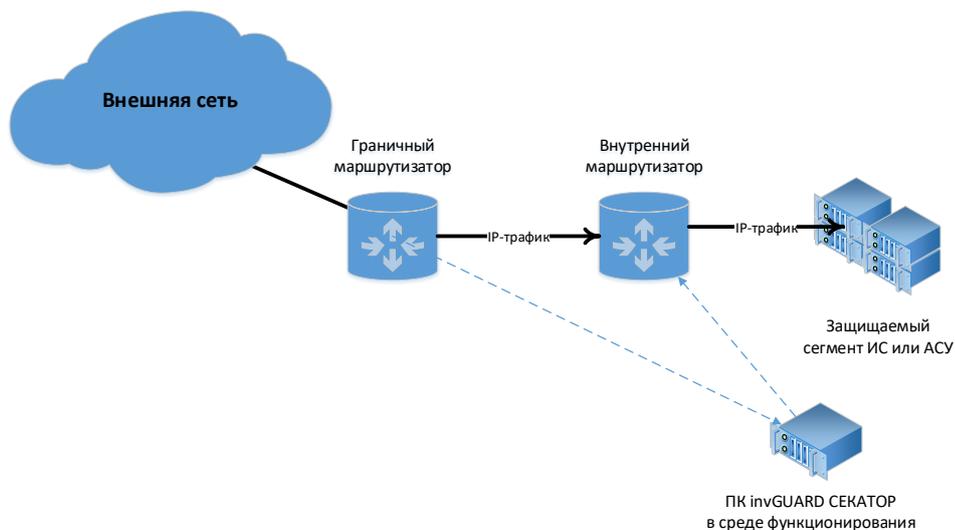


Рисунок 3 – Типовая схема применения Очистителя в ИС и АСУ «Без атаки» без использования Анализатора трафика

### 2.3.4 Типовая схема применения Очистителя в ИС и АСУ «Под атакой» без использования Анализатора трафика – см. Рисунок 4.

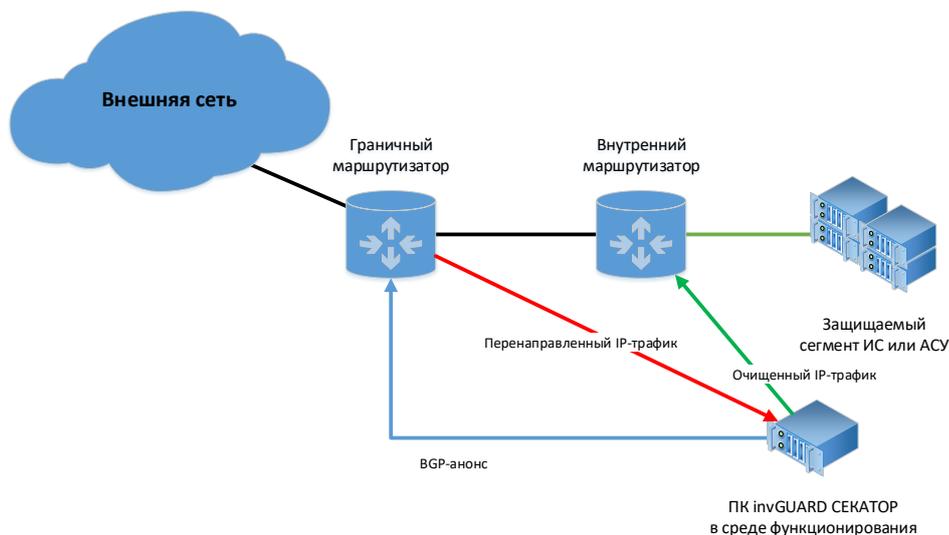


Рисунок 4 – Типовая схема применения Очистителя в ИС и АСУ «Под атакой» без использования Анализатора трафика

## **3. ВЫПОЛНЕНИЕ ПРОГРАММЫ**

### **3.1 Загрузка и запуск программы**

Загрузка и запуск программы осуществляется автоматически после загрузки/перезагрузки сервера.

### **3.2 Использование веб-интерфейса программы**

#### **3.2.1 Введение**

Управление Очистителем возможно с использованием веб-интерфейса программных комплексов invGUARD AS-SW или invGUARD AI-SW (далее по тексту – Анализатор) или с использованием собственного сервисного веб-интерфейса.

#### **3.2.2 Принятие сертификата**

При первом входе в веб-интерфейс возможно появление сообщения о том, что сертификат, используемый на сайте, является недействительным. Для продолжения работы с веб-интерфейсом необходимо принять сертификат безопасности. В дальнейшем это предупреждение появляться не будет.

#### **3.2.3 Использование веб-интерфейса Анализатора**

Для обеспечения процесса управления может использоваться веб-интерфейс Анализатора, в котором часть пунктов меню используются для мониторинга и управления Очистителем.

Полное описание работы с веб-интерфейсом Анализатора содержится в документе RU.09445927.425530-03 34 01 «Программный комплекс invGUARD AS-SW. Руководство оператора».

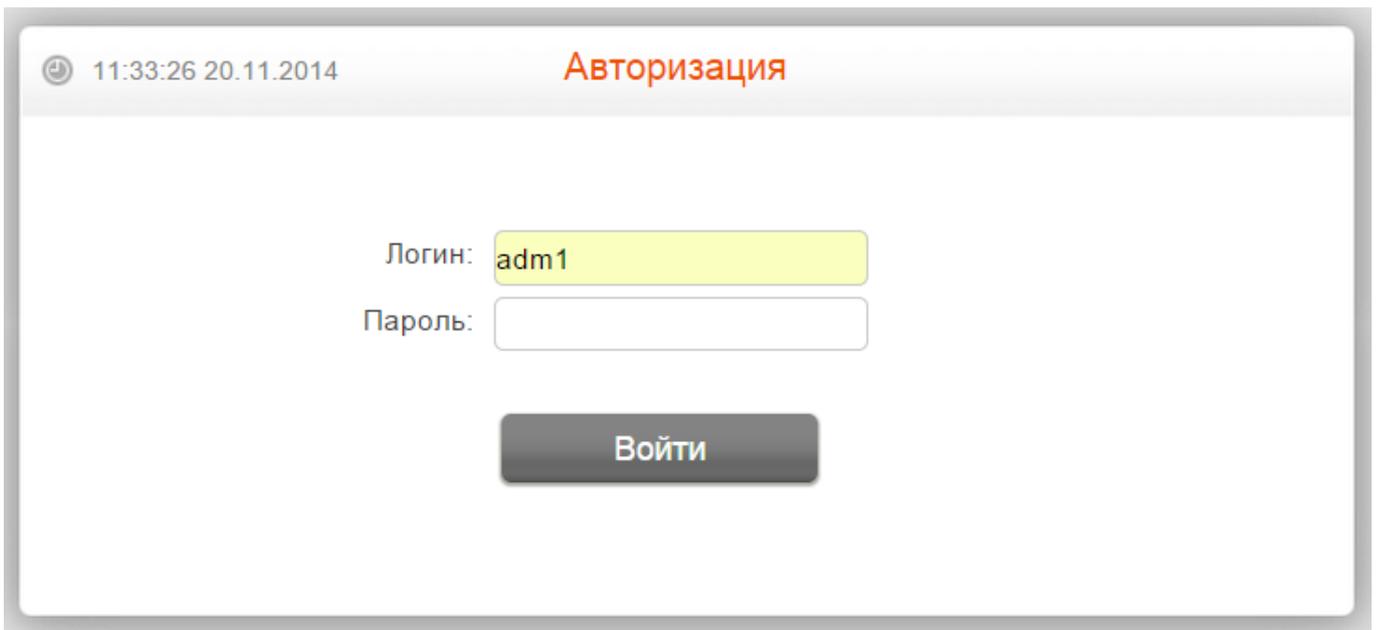
##### **3.2.3.1 Вход в веб-интерфейс пользователя**

Для того чтобы зайти в веб-интерфейс Анализатора, выполните следующие действия.

- 1) Запустите веб-браузер.
- 2) Введите <https://<ip-адрес Анализатора>>.

**Важно:** необходимо использовать безопасное соединение и настроить веб-браузер таким образом, чтобы разрешить появление всплывающих окон и прием идентификационных файлов-маркеров (cookies) от веб-интерфейса Анализатора.

- 3) Если появится сообщение о том, что сертификат безопасности сайта недействителен, следует разрешить использовать сертификат.
- 4) Введите имя пользователя и пароль в окне авторизации – см. Рисунок 5.
- 5) Нажмите «Войти». Откроется суммарный отчет по сети (Система / Статус / Суммарный отчет) – см. Рисунок 14.
- 6) Для проверки состояния Очистителя перейти на вкладку (Система / Статус / Устройства invGUARD / Статус устройств) и выбрать вкладку «Очистители» – см. Рисунок 7.



11:33:26 20.11.2014

**Авторизация**

Логин: adm1

Пароль:

Войти

Рисунок 5 – Окно авторизации веб-интерфейса Анализатора

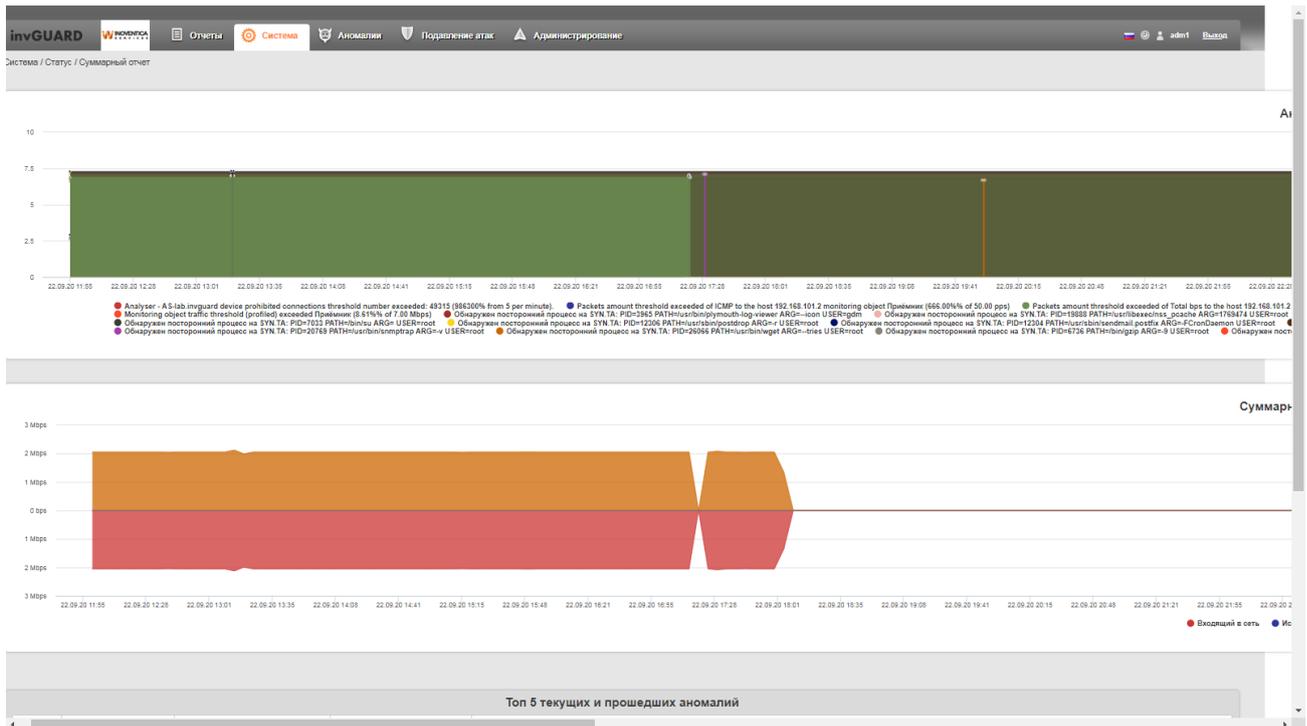


Рисунок 6 – Окно «Суммарный отчет» веб-интерфейса Анализатора

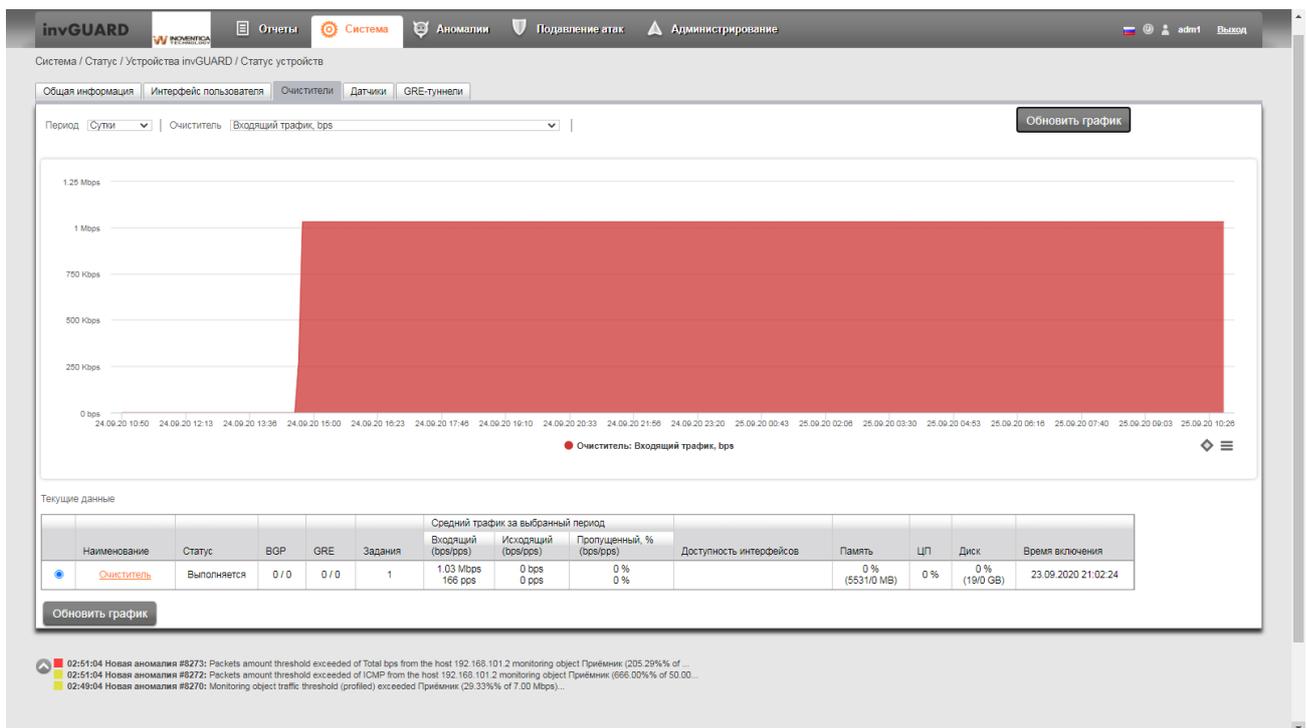


Рисунок 7 – Окно статус Очистителя веб-интерфейса Анализатора

### 3.2.3.2 Выход из веб-интерфейса пользователя

Для выхода из интерфейса пользователя выполните следующие действия.

- 1) Нажмите «Выход» (с правой стороны навигационного меню).

2) Закройте браузер.

### 3.2.3.3 Навигация по веб-интерфейсу Анализатора

Для перемещения по экранам веб-интерфейса Анализатора, используется навигационное меню и разнообразные средства управления на страницах.

#### 3.2.3.3.1 Навигационное меню Анализатора

Навигационное меню (см. Рисунок 8) позволяет перемещаться между экранами веб-интерфейса.



Рисунок 8 – Вид навигационного меню Анализатора

Все экраны размещены по пунктам в навигационном меню. Описание пунктов смотрите в таблице 1.

Таблица 1 – Пункты навигационного меню

Пункт	Описание
Отчеты	Содержит всевозможные отчеты о сети, трафике, наблюдаемых объектах, очистителях и т.п.
Система	Содержит информацию о Системе, о состоянии устройств, активности пользователей и т.п.
Аномалии	Содержит информацию о текущих и имевших место аномалиях, менеджер фингерпринтов и т.п.
Подавление атак	Содержит экраны для просмотра, конфигурирования и управления заданиями подавления атак.
Администрирование	Содержит экраны, с помощью которых происходит управление и конфигурирование Системы.

**Замечание:** некоторые пункты меню могут отсутствовать у некоторых пользователей. Наличие или отсутствие пункта зависит от прав доступа группы пользователей к соответствующим компонентам меню.

### **3.2.3.3.2 Многостраничные таблицы**

Информация на экранах часто выводится в таблицах, которые состоят из нескольких страниц. В этом случае над и под таблицей отображается список номеров страниц. Та страница, которая отображена в настоящий момент, в списке обозначается черным цветом, остальные выделены рамкой и номер страницы подчеркнут. Для перемещения по страницам таблицы выполните одно из следующих действий:

кликните по номеру нужной страницы в списке страниц;

используйте управляющие элементы “<” и “>” для перемещения на одну страницу назад или вперед соответственно;

используйте управляющие элементы “<<” и “>>” для перемещения на первую или последнюю страницу соответственно.

### **3.2.3.3.3 Сортировка элементов таблиц**

Строки таблицы можно сортировать в зависимости от значений выбранного столбца. Чтобы отсортировать таблицу, кликните на название столбца в шапке таблицы. Данные отсортируются, а выбранный столбец выделится темным цветом. Справа от названия столбца появится стрелочка, которая покажет направление сортировки.

**Замечание:** при многостраничном выводе таблицы сортировка применяется ко всем страницам.

### **3.2.3.3.4 Обновление страницы**

Для обновления экрана нажмите «Обновить». Для обновления только графика на экране, нажмите «Обновить график».

### **3.2.3.3.5 Управление загрузкой страницы**

При работе с веб-интерфейсом возможны ситуации, когда требуется прервать загрузку текущего экрана или элементов на нем, например, при загрузке отчета за

длительный период или при переходе на какой-либо отчет по ошибке. В этом случае достаточно нажать клавишу ESC, загрузка данных будет немедленно прекращена.

### **3.2.3.4 Мониторинг устройств очистки**

Экран «Статус устройств» (Система / Статус / Устройства invGUARD / Статус устройств) отражает информацию о статусе каждого устройства (в том числе и очистителей) подключенного к Анализатору индивидуально в реальном времени.

#### **3.2.3.4.1 Вкладки экрана «Статус устройств»**

Экран «Статус устройств» (Система / Статус / Устройства invGUARD / Статус устройств) имеет следующие вкладки:

Информация на экране разбита по следующим вкладкам:

- 1) «Общая информация». Позволяет диагностировать состояние всех устройств по заданному периоду времени.
- 2) «Интерфейс пользователя». Позволяет диагностировать состояние всех устройств пользовательского интерфейса по заданному периоду времени.
- 3) «Очистители». Позволяет диагностировать состояние очистителей по заданному периоду времени.
- 4) «Датчики». Отображает состояние датчиков, сконфигурированных в Системе.

#### **3.2.3.4.2 Настройка отображения информации на вкладках экрана «Статус устройств»**

Все вкладки экрана «Статус устройств» позволяют выбирать тип графика и период времени, за который необходимо отображать информацию на графике. Таблицы отображают текущие данные за последние 5 минут.

#### **3.2.3.4.3 Вкладка «Общая информация» экрана «Статус устройств»**

Вкладка показывает график, который можно настраивать и таблицу, содержащую оперативную информацию по всем сконфигурированным устройствам, как Анализатору, так и Очистителям. Таблица отражает текущие данные за последние

5 минут. Вкладка позволяет диагностировать Систему за указанный период времени по всем устройствам.

График позволяет отображать следующие параметры Очистителя:

- загрузку процессора, %;
- использование памяти, %;
- использование виртуальной памяти, %.

Таблица «Текущие данные» содержит следующую информацию по каждому Очистителю, см. Таблица 2.

Таблица 2 – Поля таблицы «Текущие данные» экрана

Колонка	Описание
Пиктограмма <input checked="" type="radio"/>	Определяет, информацию о каком устройстве отображать на графике
Наименование	Наименование устройства
Тип	Тип устройства
Статус	Статус устройства
Netflow	Не используется для Очистителя
SNMP	Не используется для Очистителя
BGP	Количество роутеров, с которыми в данный момент установлено соединение BGP и общее число роутеров с поддержкой BGP
Память	Процент использования оперативной памяти
ЦП	Процент использования центрального процессора
БД	Не используется для Очистителя
Время включения	Дата и время включения устройства

#### **3.2.3.4.4 Вкладка «Интерфейс пользователя» экрана «Статус устройств»**

Вкладка «Интерфейс пользователя» экрана «Статус устройств» (Система / Статус / Устройства invGUARD / Статус устройств) показывает график и таблицу, содержащие информацию о веб-интерфейсе Анализатора. Таблица показывает текущие данные за последние пять минут.

График на этой вкладке отображает количество активных пользователей в каждый момент времени.

#### **3.2.3.4.5 Вкладка «Очистители» экрана «Статус устройств»**

Вкладка показывает график, который можно настраивать и таблицу, содержащую оперативную информацию по всем сконфигурированным Очистителям. Таблица отражает текущие данные за последние 5 минут. Вкладка позволяет диагностировать состояние Очистителя за указанный период времени.

График позволяет отображать следующие параметры Очистителя:

- загрузку процессора, %;
- использование памяти, %;
- использование диска, %;
- использование виртуальной памяти, %;
- входящий трафик, bps;
- входящий трафик, rps;
- статистика по трафику интерфейсов очистителя, bps;
- статистика по трафику интерфейсов очистителя, rps;
- доступность интерфейсов;
- трафик не попавший ни в одно задание, bps;
- трафик не попавший ни в одно задание, rps.

Таблица «Текущие данные» содержит следующую информацию по каждому Очистителю, см. Таблица 3.

Таблица 3 – Поля таблицы «Текущие данные» экрана

<b>Колонка</b>	<b>Описание</b>
Пиктограмма 	Определяет, информацию о каком очистителе отображать на графике

<b>Колонка</b>	<b>Описание</b>
Наименование	Наименование очистителя
Статус	Статус Очистителя
BGP	Количество роутеров, с которыми в данный момент установлено соединение BGP и общее число роутеров с поддержкой BGP
Задания	Количество запущенных заданий подавления атак
Входящий (bps/pps)	Средний входящий трафик за выбранный период.
Исходящий (bps/pps)	Средний исходящий трафик за выбранный период.
Пропущено, % (bps/pps)	Процент пропущенного трафика за выбранный период.
Доступность интерфейсов	Состояние интерфейсов
Память	Процент использования оперативной памяти
ЦП	Процент использования центрального процессора
Диск	Процент и объем использования дискового пространства
Время включения	Дата и время включения устройства

#### **3.2.3.4.6 Вкладка «Датчики» экрана «Статус устройств»**

Вкладка «Датчики» экрана «Статус устройств» (Система / Статус / Устройства invGUARD / Статус устройств) показывает графики зависимости показаний датчиков Анализатора от времени.

#### **3.2.3.5 Отчеты по очистителям**

Группа отчетов «Очистители (invGUARD CS)» (Отчеты / Очистители (invGUARD CS) включает в себя отчеты, которые отображают данные о трафике подключенных Очистителей.

##### **3.2.3.5.1 Средства навигации на страницах отчетов**

Вид и параметры выводимого отчета могут быть настроены.

Отчет, выведенный на экран, можно сохранить в различных форматах.

### 3.2.3.5.1.1 Выбор периода отчета

Каждый отчет содержит поле выбора периода, за который представлены данные, см. рисунок 6. Интервалы, содержащиеся в меню выбора периода, описаны в таблице 4.

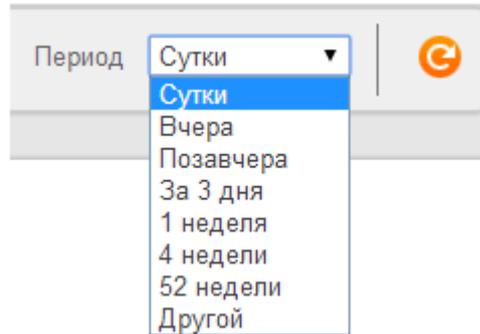


Рисунок 9 – Поле выбора периода

Таблица 4 - Периоды построения отчета

Период	Описание
Сутки	Позволяет вывести отчет за последние 24 часа
Вчера	Позволяет вывести отчет за предыдущий день (с 00:00 до 23:59)
Позавчера	Позволяет вывести отчет за пред-предыдущий день (с 00:00 до 23:59)
За 3 дня	Выводит отчет за последние 72 часа
1 неделя	Выводит отчет за неделю
4 недели	Выводит отчет за 4 недели
52 недели	Выводит отчет за 52 недели
Другой	Позволяет выбрать произвольный промежуток времени

### 3.2.3.5.1.2 Выбор единиц измерения

Единицы измерения, в которых показывается сетевой трафик в отчете, выбираются пользователем. В поле выбора «Единицы» (см. рисунок 7) можно выбрать одну из двух единиц измерения:

- bps (биты в секунду);

- pps (пакеты в секунду).

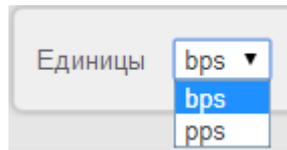


Рисунок 10 – Поле выбора единиц измерения

#### 3.2.3.5.1.3 Выбор объекта

В зависимости от типа отчета, можно выбрать тот или иной объект (инфраструктурный или наблюдаемый), для которого нужно вывести отчет.

#### 3.2.3.5.1.4 Таблицы отчетов

Большинство экранов с отчетами выводит данные в таблицы. Можно изменить следующие параметры таблиц:

- выбрать строки, которые будут отображены на графике;

**Замечание:** по умолчанию на графике отображены первые 4 строки таблицы. Эта настройка доступна для администратора Системы через конфигурационный файл.

- выбрать количество строк, которое будет выведено на одной странице таблицы;
- пересортировать таблицу, кликнув на соответствующий столбец. Столбец, по которому будет отсортирована таблица, будет выделен.

#### 3.2.3.5.1.5 Отображение данных на графике

Чтобы отобразить зависимость трафика от времени для объекта в таблице отчета выполните следующие действия:

- поставьте флажок в поле «Показать» нужной строки;
- нажмите «Обновить график».

#### 3.2.3.5.1.6 Значения в таблицах отчетов

Виды значений в таблицах отчетов приведены в таблице 5.

Таблица 5 – Виды значений в таблицах отчетов

Вычисление	Описание
Текущий	Значения за последний 5-минутный интервал времени. <b>Замечание:</b> для большинства отчетов доступно только при выбранном периоде «Сутки».
Средний	Средние значения за выбранный период времени
Максимальный	Максимальное значение за выбранный период времени
PCT95	95-ый перцентиль за выбранный период времени

**Замечание:** чтобы выбрать тот или иной вид вычисления, нажмите на соответствующую ссылку под панелью выбора параметров отчета, см. рисунок 8.

[Текущий](#) / [Средний](#) / [Максимальный](#) / [PCT95](#)

Рисунок 11 – Поле выбора режима вычислений

#### 3.2.3.5.1.7 Сохранение отчетов

Отчет можно сохранить в одном из следующих форматов:

- PDF;
- CSV;
- Excel;
- XML.

Для сохранения отчета выполните следующие действия:

- 1) Перейдите на экран с отчетом.
- 2) Выберите параметры отчета.
- 3) Наведите указатель мыши на изображение дискеты в правой верхней части экрана и нажмите «Экспорт». Откроется меню с вариантами экспорта отчета.

4) Кликните на ссылку соответствующего формата экспорта и сохраните файл.

#### **3.2.3.5.2 Типы отчетов группы «Очистители (invGUARD CS)»**

Группа отчетов «Очистители (invGUARD CS)» включает в себя следующие подгруппы отчетов и отчеты:

- суммарный отчет;
- приложения;
- размер пакетов;
- протоколы;
- QoS;
- GRE туннели.

#### **3.2.3.5.3 Подгруппа отчетов «Суммарный отчет»**

Подгруппа содержит два отчета:

- Сравнение Очистителей;
- Очиститель.

Отчет «Сравнение Очистителей» (Отчеты / Очистители (invGUARD CS) / Суммарный отчет / Сравнение Очистителей) отображает данные по входящему, исходящему, отброшенному и отброшенному глобальным фильтром трафику для выбранной группы очистителей. График показывает зависимость трафика от времени.

Отчет «Очиститель» (Отчеты / Очистители (invGUARD CS) / Суммарный отчет / Очиститель) отображает общую информацию о трафике, проходящем через выбранный Очиститель, распределенную по типам (входящий, исходящий, отброшенный, отброшенный глобальным фильтром) по заданному временному интервалу.

### **3.2.3.6 Управление очистителями**

Для управления очистителями перейти на страницу «Управление очистителями» (Администрирование / Подавление атак / Управление очистителями).

На web-странице отображаются подключенные к Анализатору очистители.

Для добавления очистителя выбрать пиктограмму <Добавить очиститель>, добавить новый Очиститель на странице «Создание нового очистителя».

Для удаления очистителя выбрать удаляемый очиститель, а затем выбрать пиктограмму <Удалить отмеченные>, добавить новый Очиститель на странице «Создание нового очистителя».

### **3.2.3.7 Подавление атак с использованием Очистителя**

В случае обнаружения DoS и DDoS-атак, может применяться метод подавления атак – направление трафика на Очиститель, который позволяет эффективно бороться с DoS и DDoS-атаками.

Для подавления атаки Анализатор в автоматическом режиме или по команде оператора запускает соответствующее «Задание очистителя» (далее по тексту – Задание). После запуска Задания его параметры через API передаются на Очиститель, а на маршрутизатор направляется BGP-анонс для направления трафика на вход Очистителя.

#### **3.2.3.7.1 Управление заданиями Очистителей**

Для управления заданиями Очистителей необходимо перейти на страницу «Задания очистителя» (Подавление атак / Задания очистителя) (см. Рисунок 12).

		Наименование	mo_id	Длит.	Время начала	Пользователь	Трафик за последнюю минуту			Состояние
							Входящий	Отброшенный	Пропущенный	
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID470 (защитное действие)	Привычки (2234)	0 min	28 Sept, 2020 11:20:25	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID319 (защитное действие)	Привычки (2234)	1 o 4 h 10 min	15 Sept, 2020 10:50:47	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID320 (защитное действие)	Привычки (2234)	0 min	15 Sept, 2020 10:45:05	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID299 (защитное действие)	Привычки (2234)	7 h 5 min	10 Sept, 2020 11:07:40	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID270 (защитное действие)	Привычки (2234)	15 h 47 min	09 Sept, 2020 17:23:09	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID271 (защитное действие)	Привычки (2234)	0 min	09 Sept, 2020 17:25:25	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID272 (защитное действие)	Привычки (2234)	0 min	09 Sept, 2020 16:55:37	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID273 (защитное действие)	Привычки (2234)	0 min	09 Sept, 2020 16:16:23	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID274 (защитное действие)	Привычки (2234)	23 min	09 Sept, 2020 16:25:09	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID275 (защитное действие)	Привычки (2234)	19 h 7 min	09 Sept, 2020 16:29:01	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID276 (защитное действие)	Привычки (2234)	0 min	09 Sept, 2020 16:21:20	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID277 (защитное действие)	Привычки (2234)	0 min	09 Sept, 2020 16:20:00	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID278 (защитное действие)	Привычки (2234)	9 min	09 Sept, 2020 14:01:29	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID190 (защитное действие)	Привычки (2234)	13 min	07 Sept, 2020 11:45:59	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID191 (защитное действие)	Привычки (2234)	21 min	07 Sept, 2020 11:12:07	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID170 (защитное действие)	Привычки (2234)	22 h 16 min	04 Sept, 2020 17:29:59	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID192 (защитное действие)	Привычки (2234)	21 min	04 Sept, 2020 16:32:22	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID193 (защитное действие)	Привычки (2234)	0 min	03 Sept, 2020 12:29:37	auto	Нет данных	Нет данных	Нет данных	Остановлено
<input type="checkbox"/>	Детали Редактировать	Automatic suppression of attack TC ID7 (защитное действие)	Привычки (2234)	32 min	02 Sept, 2020 12:44:16	auto	Нет данных	Нет данных	Нет данных	Остановлено

Рисунок 12 – Управление заданиями Очистителя

На странице «Задания очистителя» отображаются в табличном виде информация по каждому заданию, см. Таблица 6.

Таблица 6 – Поля таблицы «Задания очистителя»

Колонка	Описание
Пиктограмма:	Используется для выбора задания
Пиктограммы: «Детали» «Редактировать»	Для отображения детальной информации по выбранному заданию Для редактирования выбранного задания
Наименование	Наименование задания
mo_id	Идентификатор наблюдаемого объекта, на который направляется трафик
Длит.	Длительность выполнения задания
Время начала	Дата и время запуска задания
Пользователь	Идентификатор пользователя запустившего задание
Входящий Трафик за последнюю минуту	Объем входящего трафика за последнюю минуту

Колонка	Описание
Отброшенный Трафик за последнюю минуту	Объем отброшенного трафика за последнюю минуту
Пропущенный Трафик за последнюю минуту	Объем пропущенного трафика за последнюю минуту
Состояние	Состояние Задания

Для отображения перечня Заданий по определенным параметрам необходимо выбрать пиктограмму «Фильтр», установить параметры и выбрать пиктограмму «Применить».

Для добавления, удаления, запуска, остановки и редактирования активного задания Очистителя необходимо выбрать соответствующую пиктограмму в нижней части страницы.

### 3.2.4 Использование сервисного веб-интерфейса Очистителя

Для обеспечения процесса управления может использоваться собственный сервисный веб-интерфейс Очистителя (далее – веб-интерфейс Очистителя).

Веб-интерфейс Очистителя используется при варианте применения Очистителя без использования Анализатора трафика, а также в случае потери связи между Очистителем и Анализатором трафика.

#### 3.2.4.1 Вход в веб-интерфейс пользователя

Для того чтобы зайти в веб-интерфейс Очистителя, выполните следующие действия.

- 1) Запустите веб-браузер.
- 2) Введите `http://<ip-адрес Очистителя>:<порт сервисного интерфейса очистителя>`.

**Важно:** необходимо использовать настроить веб-браузер таким образом, чтобы разрешить прием идентификационных файлов-маркеров (cookies) от веб-интерфейса Очистителя.

Форма авторизации в Web-интерфейсе Очистителя представлена на рисунке (см. **Ошибка! Источник ссылки не найден.**).

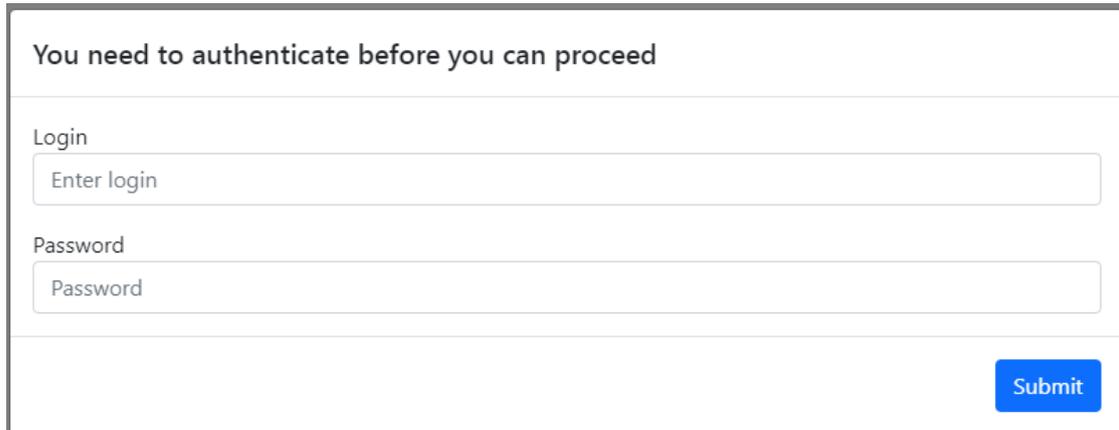


Рисунок 13 – Окно «Авторизация пользователя» веб-интерфейса Очистителя

3) Введите имя пользователя и пароль в окне авторизации.

4) Нажмите «Submit». Откроется окно «Dashboard» («Панель приборов»).

#### **3.2.4.1.1 Окно «Панель приборов»**

В окне «Панель приборов» (см. Рисунок 14) отображаются:

- «Статистика по каждому интерфейсу» («per-interface statistics») – временной график по входящему и исходящему трафику Очистителя (в PPS – пакетов/с) с разбивкой по интерфейсам и таблица «ТОР-10 входящих потоков», содержащая следующие данные:

<№ протокола по IANA> <IP-адрес источника трафика> <IP-адрес приемника трафика>, <скорость трафика в PPS (пакетов/с)> <скорость трафика в BPS (бит/с)>;

В примере, представленном на рисунке отображается 8 интерфейсов:

Enp2s0f0 in и Enp2s0f1 in – интерфейсы входящего (грязного) трафика;

Enp2s0f0 out и Enp2s0f1 out – интерфейсы исходящего (чистого) трафика;

Enp2s0f0 hard drop и Enp2s0f1 hard drop – интерфейсы, указывающие количество “отброшенного” входящего (грязного) трафика по причине нехватки вычислительных мощностей сервера для подавления мощной

атаки (большое количество PPS). Трафик, отображаемый графиками по данным интерфейсам детектируется, но не чистится т.к. он уже отброшен на этапе входа;

Enp2s0f0 drop и Enp2s0f1 drop – интерфейсы, указывающие на количество трафика не пропущенного программным комплексом на объект очистки.

- «Активные задания на подавление» – информация об активных Заданиях, где указываются:

<номер Задания>, <имя задания>, <действие>, <дата и время запуска Задания>, <IP-адрес или группа IP-адресов трафик на которые фильтруется>, а также графа «Stop» в которой содержится «кнопка» остановки Задания.



Рисунок 14 – Окно «Панель приборов» веб-интерфейса Очистителя

### 3.2.4.2 Выход из веб-интерфейса пользователя

Для выхода из интерфейса Очистителя выполните следующие действия.

- 1) Нажмите «Sign out» (в правой верхней части навигационного меню).
- 2) Закройте браузер.

### 3.2.4.3 Управление Заданиями Очистителя

Для управления заданиями Очистителя необходимо перейти на страницу «Mitigations» («Задания») – см. Рисунок 15.

The screenshot shows the 'Mitigations' page in the CEKATOP system. It features a sidebar with navigation options like 'Панель приборов', 'Подваление', 'Глобальный фильтр', 'Geo IP и списки', 'Захват трафика', and 'Настройки'. The main content area is divided into two sections: 'Активные задания на подавление' (Active tasks) and 'Прошедшие задания на подавление' (Past tasks). The active tasks table includes columns for ID, Name, Action, Started, Prefix, and Stop. The past tasks table includes columns for ID, Name, Action, Started, Ended, and Prefix.

Активные задания на подавление						
#	Name	Action	Started	Prefix	Stop	
11	Test Loc 11	pass	вт. 16.01.2024 г. 10:57:13	192.168.1.1	Stop	
13	1	pass	вт. 16.01.2024 г. 22:02:42	192.168.1.2	Stop	
15	Analyzer mitigation [3039] - shaping	shaping	вт. 20.02.2024 г. 13:38:40	192.168.101.5/32	Stop	
16	Analyzer mitigation [3040] - shaping	shaping	вт. 20.02.2024 г. 13:38:40	192.168.101.5/32	Stop	

Прошедшие задания на подавление						
#	Name	Action	Started	Ended	Prefix	
10	Test Loc	drop	вт. 16.01.2024 г. 10:57:13	вт. 16.01.2024 г. 21:27:28	1.2.3.4	
12	2	pass	вт. 16.01.2024 г. 22:02:00	вт. 16.01.2024 г. 22:02:10	192.168.1.10	
14	2	pass	вт. 16.01.2024 г. 22:28:28	пт. 19.02.2024 г. 15:49:39	192.168.1.2	

Рисунок 15 – Окно «Задания» веб-интерфейса Очистителя

#### 3.2.4.3.1 Просмотр состояния, редактирование и завершение Задания Очистителя

Для просмотра информации о Задании необходимо выбрать строку соответствующего Задания, после чего будет выведено окно отображающее детальную информацию о задании – см. Рисунок 16.

The screenshot shows a 'Mitigation' detail window with a close button (X) in the top right corner. It contains four input fields: 'Mitigation ID' with the value '1000013', 'Source' with the value 'Manual', 'Started', and 'Finished'. At the bottom, there are three buttons: 'Close', 'Stop mitigation', and 'Save changes and restart'.

Рисунок 16 – Окно «Панель инструментов» веб-интерфейса Очистителя

Для просмотра информации в окне – использовать полосу прокрутки.

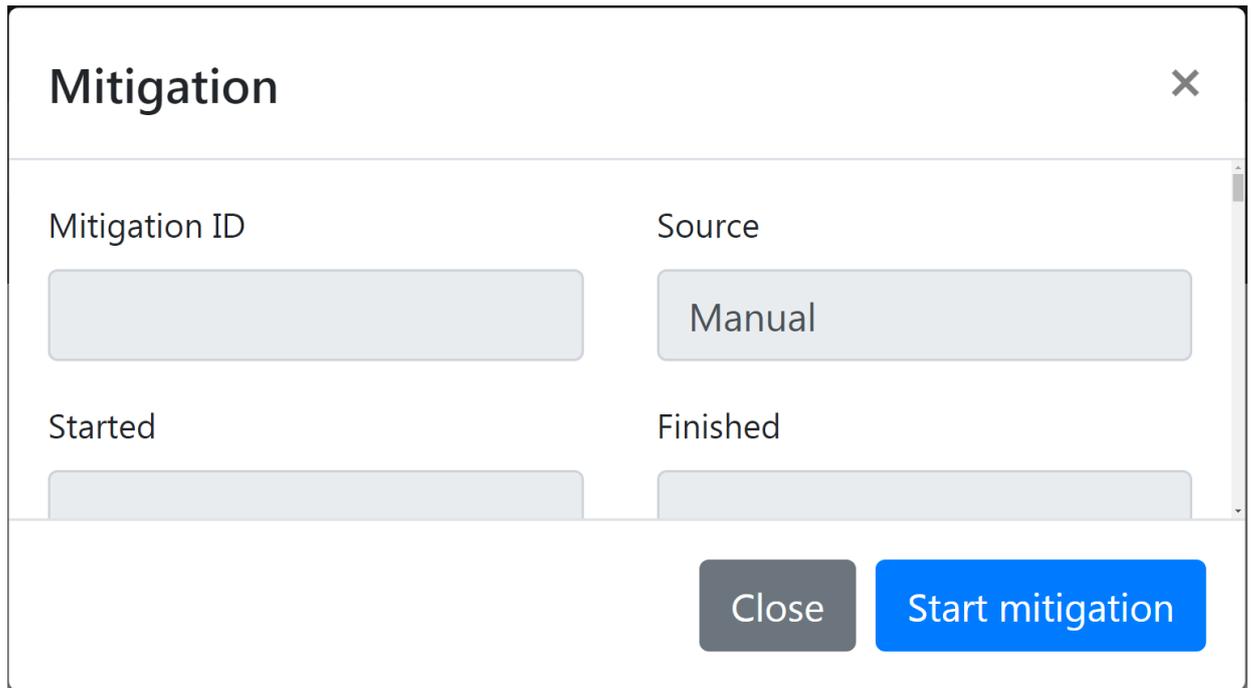
Для закрытия окна – выбрать пиктограмму «Close».

Для остановки Задания – выбрать пиктограмму «Stop mitigation».

Для редактирования Задания и его перезапуска – «Save changes and restart».

### 3.2.4.3.2 Создание и запуск Задания Очистителя

Для создания Задания необходимо выбрать пиктограмму «Create new mitigation», после чего будет выведено соответствующее окно – см. Рисунок 17.



The image shows a web interface window titled "Mitigation". It contains four input fields arranged in a 2x2 grid: "Mitigation ID", "Source" (with "Manual" selected), "Started", and "Finished". At the bottom right, there are two buttons: "Close" and "Start mitigation".

Рисунок 17 – Окно создания Задания веб-интерфейса Очистителя

Для просмотра информации в окне и заполнения всех полей – использовать полосу прокрутки.

Для закрытия окна – выбрать пиктограмму «Close».

Для запуска созданного Задания – выбрать пиктограмму «Start mitigation».

### 3.2.4.4 Просмотр сетевых настроек Очистителя

Для просмотра сетевых настроек Очистителя необходимо перейти на страницу «Settings» («Настройки») в котором отображены данные о парных портах вход/выход («Cleaner pairs») и настройках BGP («Local BGP settings») – см. Рисунок 18.

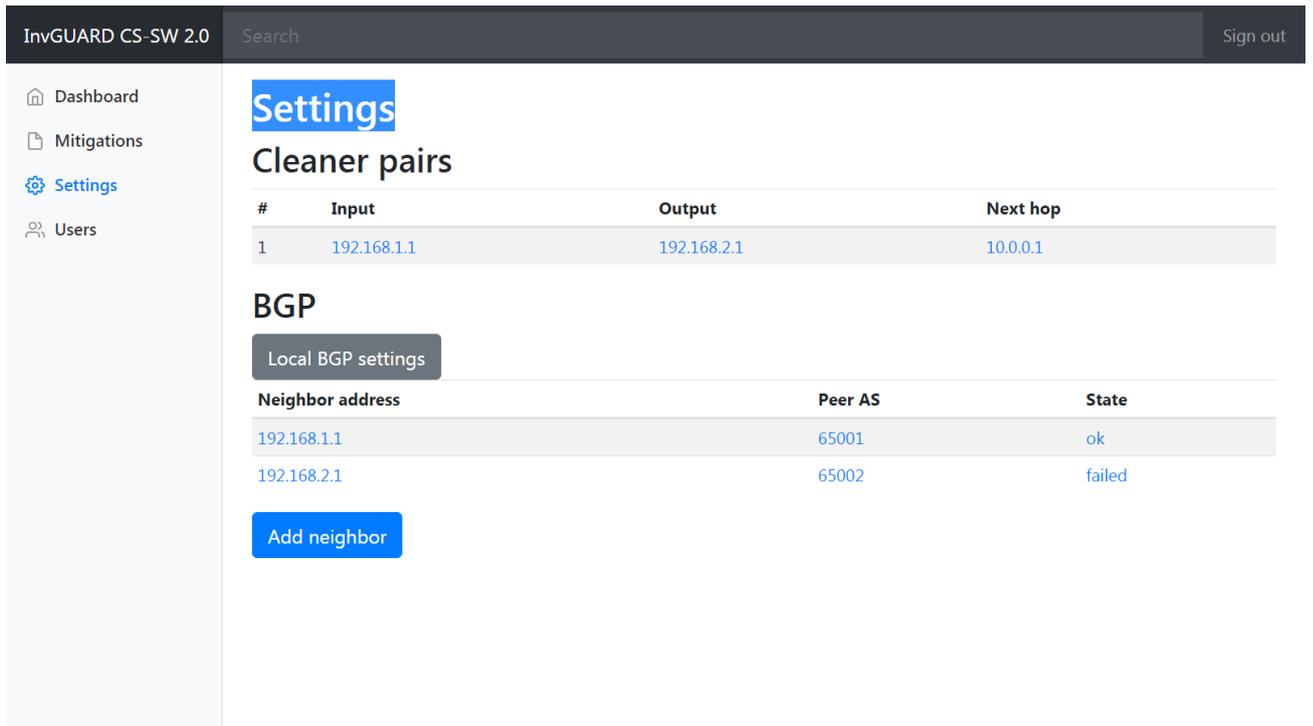


Рисунок 18 – Окно сетевых настроек Очистителя

### 3.2.4.5 Просмотр информации о пользователях Очистителя

Для просмотра информации о пользователях Очистителя необходимо перейти на страницу «Users» («Пользователи») в котором отображены данные о зарегистрированных пользователях – см. Рисунок 18.

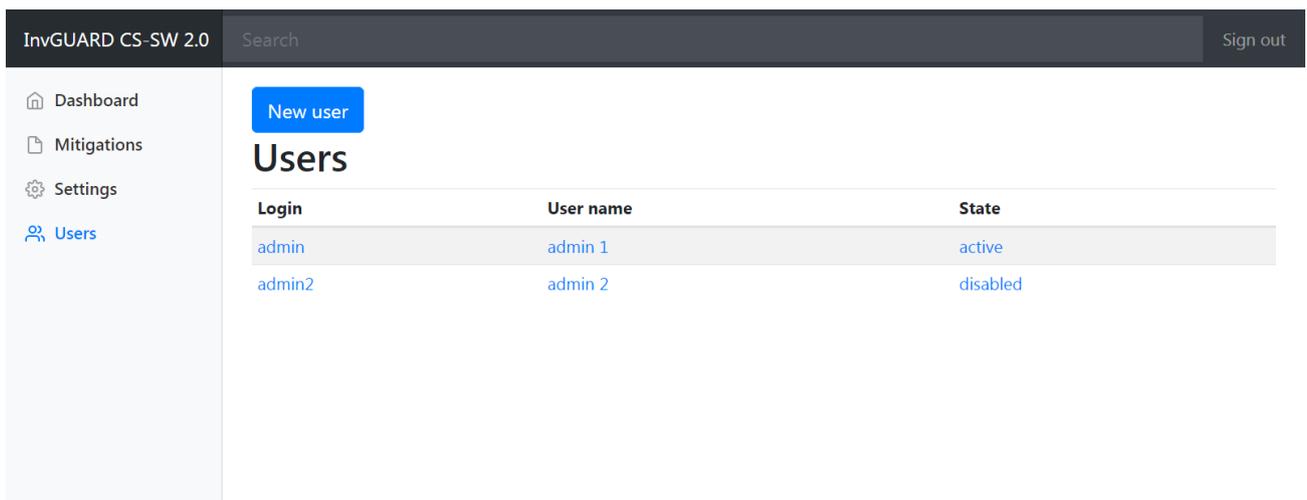


Рисунок 19 – Окно «Пользователи» веб-интерфейса Очистителя

## 3.3 Завершение программы

Завершение работы программы необходимо выполнить следующие действия:

- 1) Выполнить команду: `sudo systemctl stop syn.gui`
- 2) Выполнить команду: `sudo systemctl stop syn`
- 3) Выполнить команду: `sudo systemctl stop kernnethelper`

#### 4. СООБЩЕНИЯ ОПЕРАТОРУ

Для выдачи оператору диагностических сообщений о возникающих ошибках системы используется каталог `/syn/syn/alerts/`, содержащий файлы с информацией о событиях системы.

Файл с информацией о событиях системы представляет собой xml-файл с именем `TS.xml`, где `TS` отражает время создания оповещения. Корневой элемент файла называется `alert`.

Описание сообщений оператору содержатся в таблице – см. Таблица 7.

Таблица 7 – Сообщения оператору

Формат сообщения	Описание
<p><b>«interface %s is down»</b>  где %s - наименование сетевого интерфейса</p>	<p>Пропадание сигнала на сетевом интерфейсе</p>
<p><b>«interfaces pair IF1:IF2 is in inactive state»</b>  где IF1 – название входящей группы интерфейсов, IF2 – исходящей группы интерфейсов</p>	<p>«Разрушение бондинга» - прекращение работы входящей или исходящей группы интерфейсов в режиме Ethernet bonding</p>
<p><b>«Temperature of NAME (INPUT°C) is over threshold (THRESHOLD°C)»</b>  где NAME - наименование датчика,  INPUT - температура датчика,  THRESHOLD - максимальная допустимая температура для датчика</p>	<p>Превышение заданной температуры на определенном датчике (список датчиков задается в конфигурационном файле)</p>

## ПЕРЕЧЕНЬ ТЕРМИНОВ

В настоящем документе применяют следующие термины с соответствующими определениями.

Очистка трафика	Совокупность механизмов и алгоритмов фильтрации трафика с целью отбрасывания пакетов, классифицированных как аномальные.
Сигнатура трафика / угрозы	Описание существенных характеристик трафика (произвольного или аномального) в виде выражения на специальном языке.
NetFlow	Семейство протоколов, поддерживаемых маршрутизаторами, для предоставления "слепков" трафика.
GRE	Протокол туннелирования сетевых пакетов. Его основное назначение — инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP-пакеты.
Ethernet bonding	Объединение двух или более физических сетевых интерфейсов Ethernet в один виртуальный для обеспечения отказоустойчивости и повышения пропускной способности.

## **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ**

IANA	Internet Assigned Numbers Authority – «Администрация адресного пространства Интернет») – функция управления пространствами IP-адресов, доменов верхнего уровня, а также регистрации типов данных MIME и параметров прочих протоколов Интернета.
XML	eXtensible Markup Language, универсальный текстовый формат для хранения и передачи структурированных данных.
SSH	Secure Shell, сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений.
QoS	Quality of service («качество обслуживания») способность сети обеспечить необходимый сервис заданному трафику в определенных технологических рамках.

