ГАРДА
ТЕХНОЛОГИИ

ООО "Гарда Технологии"

Руководство пользователя

Модуль Очиститель ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 ВВЕДЕНИЕ

1.1 Аннотация

Данный документ представляет собой Руководство пользователя к программному модулю «Очиститель», входящий в состав программного обеспечения ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР».

1.2 Термины, определения и сокращения

Термин	Значение
ПК	ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР»
Система	ПК «ПЕРИМЕТР»
Модуль	Модуль «Очиститель»
СПД	Сеть передачи данных
DoS	Сетевая (компьютерная) атака, направленная на отказ в обслуживании
DDoS	DoS-атака, выполняемая одновременно с большого числа компьютеров

1.3 Использование имен, номеров телефонов, сетевых адресов

Все регистрационные имена пользователей, а также номера телефонов, имена и другие данные абонентов, используемые в Руководстве, являются вымышленными, а IP-адреса не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4 О компании

«Гарда Технологии» – российский разработчик систем защиты от внутренних и внешних угроз информационной безопасности, противодействия мошенничеству и расследования инцидентов. Решения «Гарда Технологии» занимают лидирующие позиции на российских рынках решений информационной безопасности.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Исследовательский центр компании обладает 5 патентами на уникальные технологии. Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, операторах связи и государственных структурах России и СНГ. Подробнее – на gardatech.ru

1.5 Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании «Гарда Технологии»:

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по Московскому времени).
- Email: ddos.support@gardatech.ru

2 НАЗНАЧЕНИЕ СИСТЕМЫ

ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР» (далее ПК «ПЕРИМЕТР») представляет собой систему обнаружения и противодействия сетевым атакам типа «Отказ в обслуживании DoS/DDoS» (далее DDoS) и анализа трафика на сети передачи данных (далее СПД).

Решение данной задачи основано на:

- постоянном контроле состояния трафика СПД и его многостороннем анализе;
- обнаружении отклонений параметров трафика (аномалий);
- интеллектуальной фильтрации трафика с блокированием вредоносной составляющей и пропуском легитимной.

3 НАЧАЛО РАБОТЫ

Настройка и администрирование комплекса осуществляется через графический интерфейс пользователя (далее web-интерфейс) модуля Анализатор либо модуля Лидер (если он установлен).

Чтобы открыть web-интерфейс:

1. Запустите web-браузер.
2. Установите в настройках следующие параметры отображения страниц:
   - Использовать безопасное соединение;
   - Разрешить появление всплывающих окон;
   - Разрешить исполнение скриптов Javascript
   - Разрешить приём файлов cookie.
3. Введите в поле адресной строки web-браузера https://IP-address, где IP-address – это адрес интерфейса управления модуля Лидер (если комплекс не поставлялся с данным модулем, то необходимо указать адрес модуля Анализатор), настроенный в рамках подготовки комплекса к эксплуатации.
4. На странице Аутентификация пользователя введите имя учётной записи пользователя и пароль (при проверке введённых данных система учитывает регистр символов), которые были настроены в рамках подготовки комплекса к эксплуатации.
5. Нажмите кнопку Войти.

4 НАСТРОЙКА ОЧИСТИТЕЛЯ

Описание добавление очистителя и его начальная настройка в зависимости от режима работы находится в документе «Руководство администратора Модуль Очиститель».

4.1 Дополнительные настройки

4.1.1 Сбор DPI статистики

Для детектирования атак по сигнатурам, имеющим в составе ключевое слово «dpi», необходимо, чтобы была сконфигурирована логическая связь между модулями Очиститель, выполняющими сбор dpi-статистики, и модулями Анализатор, обрабатывающими эту статистику.

Со стороны модулей Очиститель настройка выполняется при редактировании модуля на вкладке «DPI Flow». Передаваемые данные не зависят от других настроек модуля Очиститель и влияют только на сбор статистики по dpi-сигнатурам атак.

Для включения передачи dpi-статистики, необходимо:

- установить флаг «Включить»;
- установить период отправки статистики (в секундах);
- указать список адресов модулей Анализатор, обрабатывающих dpi-статистику, с указанием портов, на которые необходимо отправлять данные;
- создать объекты «Сенсор» в меню «Администрирование / Мониторинг / Инфраструктура / Маршрутизаторы», прослушивающий указанные выше порты на модулях Анализатор.

Для выключения передачи dpi-статистики, необходимо снять флаг «Включить».

4.1.2 Управление функцией аппаратного байпаса

Очиститель поддерживает управление функцией аппаратного байпаса через веб-интерфейс. Для управления аппаратным байпасом, необходимо перейти в меню «Администрирование / Подавление атак / Управление очистителями». В столбце «Режим Bypass» указывается текущий режим работы сетевого адаптера с поддержкой функции аппаратного байпаса:

- Не поддерживается – сетевой адаптер не поддерживает функцию аппаратного байпаса;
- Активный – сетевой адаптер подает трафик в Очиститель для фильтрации;
- Холостой – сетевой адаптер находится в режиме аппаратного байпаса.

Для переключения режимов, необходимо перейти по ссылке «Переключить в Холостой» или «Переключить в Активный» в столбце «Режим Bypass» и подтвердить изменение режима нажатием кнопки «ОК».

4.1.3 Параметры групповой очистки

Использование групповой очистки с изменяемым количеством задействованных модулей очистки, а также балансировка нагрузки между модулями очистки в составе группы очистителей, опирается на контроль превышения максимальных разрешенных параметров для каждого модуля Очиститель. Разрешенные параметры модуля задаются при создании или редактировании модуля Очиститель в меню «Администрирование / Подавление атак / Управление очистителями» веб-интерфейса на вкладке «Параметры оборудования». Для использования очистителя в составе группы очистителей, необходимо установить значения для следующих параметров:

- Число запущенных заданий — максимальное число одновременно работающих заданий, разрешенных для модуля очистки;
- Максимальный pps — максимальная разрешенный входящий трафик для модуля очистки в pps;
- Максимальный bps — максимальная разрешенный входящий трафик для модуля очистки в bps;
- Число отслеживаемых сессий — максимальное число сессий, отслеживаемых модулем очистки;
- Число отслеживаемых адресов — максимальное число IP адресов, отслеживаемых модулем очистки.

Алгоритм контроля перегрузки использует указанные параметры для расчета емкости группы очистителей и динамического распределения нагрузки между модулями Очиститель. Пороговые значения, используемые для подключения дополнительных модулей Очиститель или их отключения задаются в разделе «Балансировка: пороговые значения» в меню «Администрирование / Подавление атак / Глобальные настройки».

5 ВЫЯВЛЕНИЕ АНОМАЛИЙ И ПРОТИВОДЕЙСТВИЕ

5.1 Подтипы аномалий «Аномалия очистителя»

Подтип аномалии	Выявляется по ...
Перегрузка модуля вывода	слишком большой загрузке модуля вывода
Ошибка конфигурации системы	ошибке конфигурации очистителя
Ошибка модуля системы	ошибке в одном из программных модулей очистителя
Ошибка обработки задания очистки	ошибке в процессе запуска/остановки/изменения задания очистки
Обнаружение замены устройства	замене одного из очистителей
Не удается разрешить MAC-адрес nexthop-а IPv4	ошибке в работе протокола ARP
Не удается разрешить MAC-адрес nexthop-а IPv6	ошибке в работе протокола NDP
Отказ GRE туннеля	не доступности туннеля для доставки очищенного трафика (при использовании GRE туннеля в качестве способа доставки)
Очиститель уже используется другим анализатором	ошибке конфигурирования: модуль Очиститель должен находиться под управлением только одного модуля Анализатор
Ошибка запуска системы / Ошибка перезапуска модуля системы	невозможности нормального запуска/перезапуска программных компонентов модуля Очиститель
Ошибка сбора пакетов сырого трафика	ошибке в процессе сбора трафика по запросу пользователя
По крайней мере один из интерфейсов отключен (link down)	отсутствию канального соединения (link) на одном из интерфейсов (входных или выходных) модуля Очиститель
Разрыв BGP соединения	ошибке BGP соединения на управляющем модулем Очиститель Анализаторе
Черный список загружен не полностью	неполной загрузке черного списка в модуль Очиститель

Примечание: Подтип аномалии «Перегрузка модуля вывода» указывает на ошибку в процессе обработки пакетов очистителем.

5.2 Подготовка к подавлению атак

Перед началом работы по противодействию DoS/DDoS атакам, необходимо произвести настройку модуля Очиститель:

- создать и настроить шаблоны настроек подключения для используемых инструментов подавления: Очистителей, BGP FlowSpec и Blackhole-маршрутизации в меню «Администрирование / Подавление атак / Шаблоны»;
- создать и настроить шаблоны настроек методов очистки в меню «Администрирование / Подавление атак / Шаблоны»;
- при необходимости создать и настроить шаблоны регулярных выражений для использования в заданиях очистки в меню «Администрирование / Подавление атак / Шаблоны PCRE regexp»;
- установить флаг «Автоматически создавать задания фильтрации в ответ на атаки» в меню «Администрирование / Подавление атак / Глобальные настройки»;
- настроить наблюдаемые объекты для автоматического подавления.

В документе «Руководство пользователя Модуль Анализатор» описана настройка следующих компонентов:

- Группы очистки
- Шаблоны подавления атак
- Настройка шаблонов подключения
- Шаблоны регулярных выражений
- SSL-сертификаты защищаемых узлов
- Пользовательские списки
- DNS списки

6 ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

6.1 Противодействие атакам

При появлении DoS-атак, возникает необходимость противодействия им. Подавление атаки возможно:

- на границе сети (вариант применим, если атака содержит значительный объем аномального трафика, и нет смысла пропускать его в контролируемую СПД);
- на системах очистки ПК «ПЕРИМЕТР» (модулях Очиститель), имеющих разнообразные методы очистки трафика и позволяющих противодействовать всем видам атак.

Подавление атак в ПК «ПЕРИМЕТР» основано на заданиях подавления, которые используют сконфигурированные инструменты подавления и предварительно подготовленные наборы контрмер для эффективного противодействия атакам.

6.1.1 Подавление на очистителе

Подавление атак на очистителе является основным и самым эффективным инструментом, предоставляемым ПК «ПЕРИМЕТР». Очистка трафика происходит в рамках заданий очистки, которые создаются на модулях Очиститель. Схема прохождения трафика через модуль Очиститель представлена на рисунке 1.

Направленный на очиститель трафик поступает на входной интерфейс и проходит этап фильтрации некорректно сформированных IP-пакетов. Корректно сформированный трафик поступает на глобальный фильтр, где может быть блокирован согласно определённому запрещающему правилу или направлен сразу на выходной интерфейс согласно разрешающему правилу. Проверка на корректность IP-пакетов и глобальный фильтр работают в рамках всего очистителя. Трафик, не подошедший ни под одно из заданных в глобальном фильтре правил, анализируется на предмет соответствия одному из заданий очистки на очистителе.

Каждое задание представляет собой набор инструментов инспектирования и подавления атак в трафике, идущем на определенный IP-префикс.

IP-пакет считается соответствующим одному из заданий очистителя, если IP-адрес получателя этого пакета входит в диапазон IP-префиксов, анонсированных при захвате трафика на очистку. Поскольку IP-области различных заданий очистителя не могут пересекаться, один и тот же IP-пакет подлежит обработке согласно набору правил только одного задания очистителя. Если IP-пакет не попадает ни под одно из заданий очистителя, он направляется на выходной интерфейс. IP-пакет, соответствующий заданию очистителя, проходит фильтрацию набором методов. В результате фильтрации он может быть признан вредоносным и отброшен, либо направлен на выходной интерфейс.

Трафик с выходного интерфейса доставляется в защищаемую сеть согласно стандартным правилам маршрутизации, либо через заранее настроенный GRE-туннель.

Так же, как и в случае с перехватом трафика, варианты возврата очищенного трафика будут различаться в зависимости от варианта включения. Самой главной задачей возврата трафика в сеть – является организация безопасного пути возврата, который не будет создавать петель маршрутизации и трафик будет доставлен до назначения без потерь.

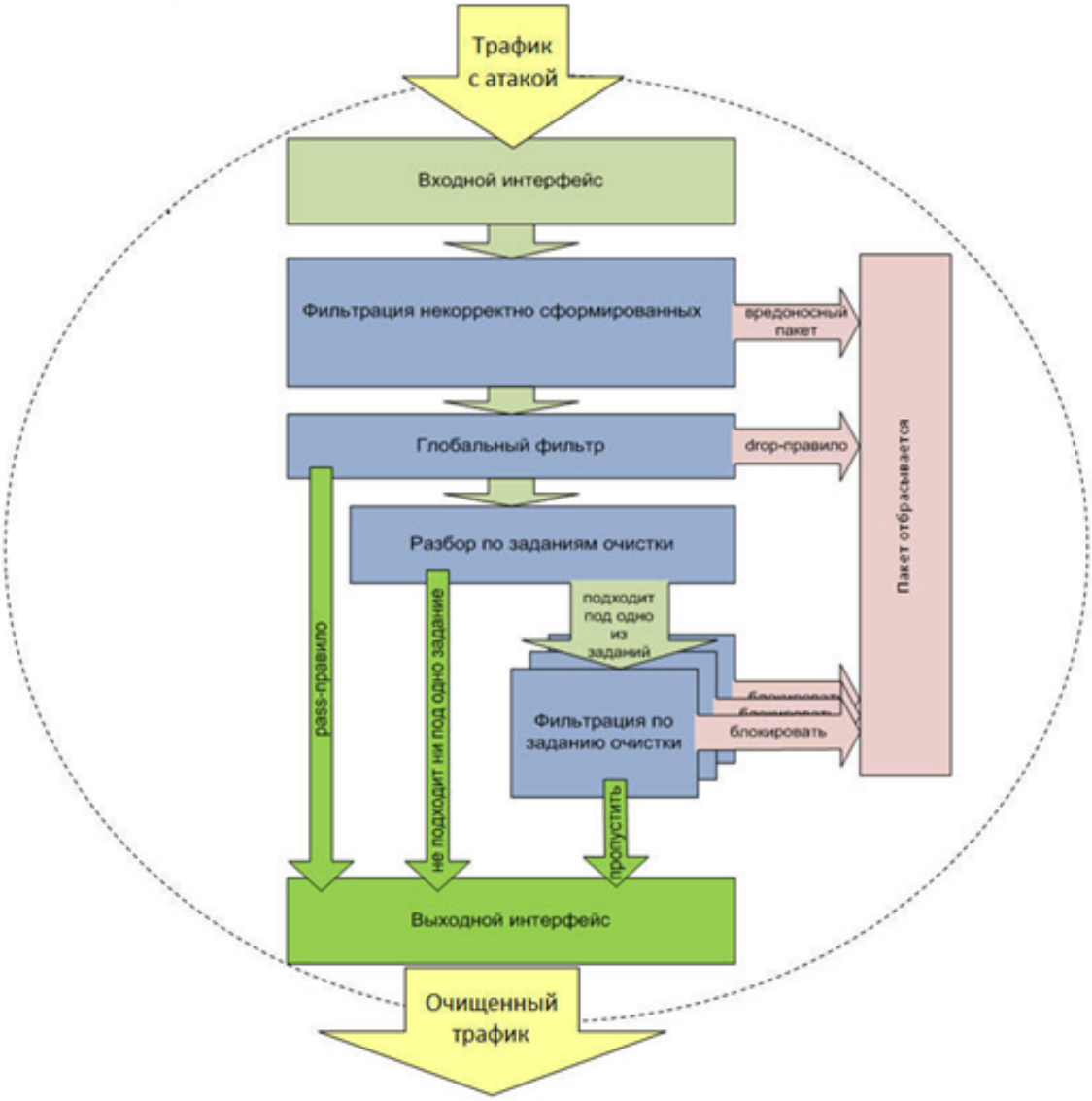

Рис. 1 Логическая схема работы очистителя.

Для решения данной задачи комплекс имеет такие инструменты как указание в перенаправляющем на очистку BGP-анонсе NextHop точки, куда будет передан очищенный трафик, указание BGP-сообществ, а также возможность организации GRE-туннеля между очистителем и L3 устройством, являющимся точкой для передачи очищенного трафика. GRE-туннель может быть организован как для всего очищенного трафика, выходящего с очистителя, так и для очищенного трафика, идущего на определенный объект, отдельно.

6.1.2 Задания подавления атак

Работа с заданиями очистки ведется на странице интерфейса «Подавление атак / Задания».

На данной странице присутствуют:

- Фильтр выбора заданий очистки по различным критериям (критерии объединяются условием логического И):
  - Административный статус - фильтр по состоянию задания подавления, будут отображены только задания с указанным статусом, например, для отображения только работающих заданий подавления, необходимо указать в фильтре вариант «запущено»;
  - Операционный статус - может принимать значения OK, если все компоненты задания подавления имеют одинаковый административный статус, либо NOT OK, если существует различия в статусах компонентов задания подавления, например, если задание очистки на одном из модулей Очиститель аварийно завершилось, а на других продолжается нормальная работа, операционный статус примет значение NOT OK;
  - Название - фильтр по части названия задания подавления (поиск по вхождению текста);
  - Длительность - фильтр по длительности фильтрации, использует фиксированные диапазоны: до 30 минут, до 1 часа, до 5 часов или более 5 часов;
  - Наблюдаемый объект - фильтр по одному из зарегистрированных наблюдаемых объектов;
  - IP-префикс - фильтр по значению защищаемого префикса или части префикса (поиск по вхождению текста), учитываются, как префиксы, заданные вручную пользователем, так и префиксы, подключаемые к заданиям подавления для отражения выявленных атак;
  - DoS-атака - фильтр по связанному с заданием подавления идентификатору (номеру) выявленной DoS атаки;
  - Авто-задания - фильтр, позволяющий не отображать задания, созданные автоматически для подавления выявленных атак, или наоборот отображать только их;
  - Настройки методов - фильтр, позволяющий отображать задания подавления, использующие выбранный шаблон методов фильтрации;
  - Настройки подключения очистителей - фильтр, позволяющий отображать задания подавления, использующие выбранный шаблон подключения очистителей;

  - Настройки подключения Blackhole-маршрутизации - фильтр, позволяющий отображать задания подавления, использующие выбранный шаблон blackhole-маршрутизации;
  - Настройки подключения BGP FlowSpec - фильтр, позволяющий отображать задания подавления, использующие выбранный шаблон BGP FlowSpec;
  - Теги наблюдаемых объектов - ограничивает отображение заданиями, связанными с наблюдаемыми объектами, имеющими хотя бы один из выбранных тегов;
  - Создание - отображаются задания подавления, созданные в указанном интервале времени;
  - Запуск - отображаются задания подавления, запускаемые в указанном интервале времени;
  - Остановка - отображаются задания подавления, останавливаемые в указанном интервале времени;
- кнопки управления заданиями, приведенные на рисунке 2, информацию о назначении каждой кнопки можно получить из контекстной информации, доступной при наведении курсора мыши на кнопку, если действие не может быть выполнено, то кнопка неактивна;

Рис. 2 Кнопки управления заданиями.

- Информацию о созданных в системе заданиях очистки, представленную в табличном виде со следующими полями:
  - флаг, элемент управления, позволяющий отметить задания на запуск, остановку, удаление или сравнение;
  - поле действия, позволяющее выполнить действие с заданием без необходимости его отметки флагом, данное поле дублирует набор кнопок управления;
  - мини-график зависимости отброшенного/пропущенного трафика от времени, в заголовке поля можно выбрать какой трафик (прямой или обратный) и за какое время будет отображаться;
  - название задания, нажатием на гиперссылку осуществляется переход к редактированию задания;
  - состояние задания, в поле дополнительно расположена пиктограмма «История задания», нажатие на данную пиктограмму вызывает окно, содержащее информацию с комментариями по заданию и изменениями, выполненными в нем;
  - дата и время создания задания очистителя;
  - дата и время последнего запуска задания очистителя;
  - дата и время последней остановки задания;
  - время, в течение которого задание находится в статусе запущено;
  - текущий трафик (Входящий) - текущий объем входящего трафика задания на системе очистки;
  - текущий трафик (Отброшенный) - объем отброшенного очистителем трафика задания на системе очистки;

– текущий трафик (Пропущенный) - объем пропущенного очистителем трафика задания на системе очистки;

– создатель, имя учётной записи пользователя, который последним запускал или вносил изменения в параметры задания очистителя;

– наблюдаемый объект - наименование наблюдаемого объекта, по которому создано задание. Данный параметр присутствует если задание очистителя было создано в рамках противодействия аномалии;

– активные атаки - гиперссылки, указывающие на идущие в настоящий момент DoS-атаки, связанные с заданием подавления.

Примечание: Набор полей таблицы можно настраивать нажатием по ссылке «Отображаемые данные». Также можно выбрать один из доступных режимов отображения данных: все задания, проблемные, текущие, прошедшие.

6.1.3 Экран статуса задания

Контроль процесса подавления и индивидуальная настройка методов очистки задания подавления производится на экране статуса задания подавления атаки (Рисунок 3).

На экран статуса задания можно попасть из меню «Подавление атак / Задания», щелкнув левой кнопкой мыши по миниатюре в поле «Трафик» того задания, состояние которого необходимо увидеть, а также из меню редактирования начальных параметров, нажав кнопку «Статус».

Экран статуса представляет собой рабочую область, разделенную на две вкладки: суммарная информация и методы очистки.

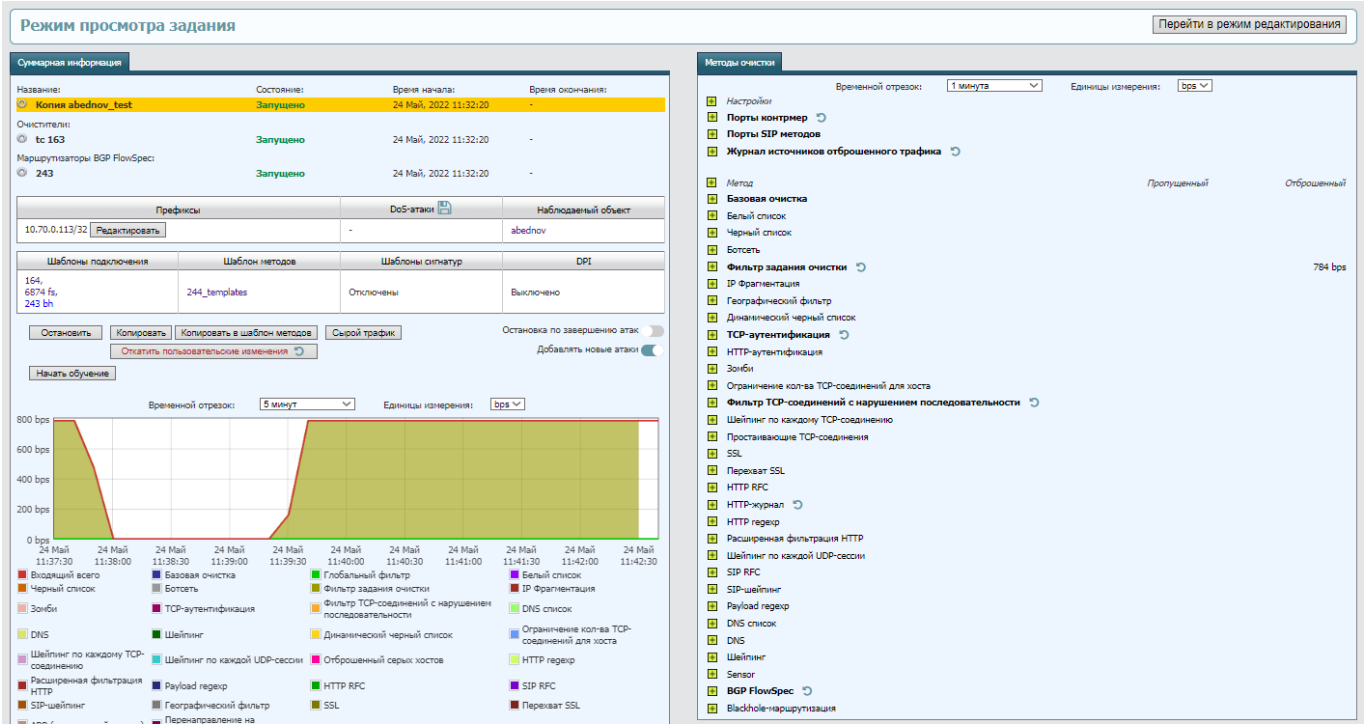

Рис. 3 Экран статуса задания подавления атаки.

Вкладка «Суммарная информация» содержит:

- информационный блок - состояние задания подавления и заданий, запущенных на инструментах подавления: очистителях, маршрутизаторах Blackhole и FlowSpec. Пиктограмма позволяет перейти к настройкам элемента, название которого указано справа от неё;
- список защищаемых префиксов, с возможностью текстового поиска по части префикса в режиме редактирования префиксов, список DoS-атак, связанных с заданием подавления, защищаемый наблюдаемый объект, а также признак использования dpi-сигнатур атак;
- начальные параметры: шаблоны подключения, шаблон настройки методов и шаблоны сигнатур (при автоматическом подавлении), используемые при запуске задания;
- блок управления заданием подавления:
  - Запустить/Остановить - управление заданием подавления;

  Примечание. Кнопки не отображаются при выборе на вкладке Суммарная информация одного из задний очистителей (строка в разделе Очистители). Если одно или несколько заданий очистителя находятся в состоянии Ошибка или Остановлено, и есть необходимость запустить их, нужно выбрать на вкладке Суммарная информация строку с названием задания, после чего нажать на кнопку «Запустить». Все задания на очистителях, которые находятся в ошибочном или остановленном состоянии будут перезапущены. Перезапуск также будет производиться при любом изменении в конфигурации задания подавления.

  - Сырой трафик - переход к функции сбора «сырых пакетов»;
  - HTTP-журнал и HTTP-анализ - кнопки, доступные после активации метода «HTTP-журнал», позволяют проводить статистический анализ собранного журнала HTTP запросов;
  - Копировать - позволяет клонировать задание подавления;
  - Копировать в шаблон методов - позволяет перенести все настройки методов из задания подавления в шаблон методов для повторного использования;
  - Откатить пользовательские изменения - позволяет отменить все изменения, внесенные пользователем в задание подавления. Параметры подавления будут соответствовать подключенному шаблону настроек методов и, при включенном режиме объединения с шаблонами сигнатур, настройкам подавления для активных в данный момент времени векторов атак;
  - Начать обучение - позволяет переключить задание подавления в режим определения оптимальных параметров методов защиты на реальном трафике;
  - Применить результаты - позволяет просмотреть и применить рекомендованные параметры методов защиты, полученные в результате обучения;
  - Удалить результаты - позволяет очистить результаты обучения;
  - Остановка по завершению атак - переключатель, позволяющий управлять остановкой задания после завершения всех связанных атак (отображается только для заданий, связанных с наблюдаемым объектом);
  - Добавлять новые атаки - переключатель, управляющий возможностью добавлять новые атаки в существующее задание подавления при активированном параметре «Объединять атаки в одно задание фильтрации» в настройках наблюдаемого объекта (отображается только для заданий, связанных с наблюдаемым объектом, автоматически синхронизируется с параметром «Добавлять новые атаки» при его изменении);

- блок управления режимом обучения, включающий кнопки начала/окончания обучения, а также применения и удаления результатов обучения;
- блок статистической информации, включающий в себя график трафика в разрезе методов очистки, а также суммарную статистику пропущенного и отброшенного трафика;
- блок комментариев с возможностью просмотра по категориям и добавления нового комментария.

Вкладка «Методы очистки» содержит детальную информацию о параметрах методов очистки. Состоит из двух разделов:

- Настройки - содержит общие параметры для нескольких методов, например, анализируемые порты транспортных протоколов tcp и udp;
- Метод - содержит методы противодействия атакам и их параметры.

Используемые настройки и методы выделены жирным шрифтом. При раскрытии пиктограммы отображаются параметры блока и индивидуальная детальная статистика. Для активных методов в строке с названием метода отображается суммарная статистика по отброшенному и пропущенному трафику.

В верхней части окна расположен информационный блок, отображающий текущие режим работы экрана статуса задания подавления атаки. Допустимы следующие режимы:

- режим просмотра - в этом режиме не допускается внесение изменений пользователем. При автоматическом подавлении с объединением сигнатур, в зависимости от текущих векторов атаки, могут активизироваться различные методы очистки.
- режим редактирования - в этом режиме пользователь может внести правки в задание подавления, при этом в автоматическом режиме подавления с объединением сигнатур система не вмешивается в настройки методов при изменении характера атаки до момента перехода в режим просмотра.

7 ЗАВЕРШЕНИЕ РАБОТЫ

Для завершения работы с Комплексом необходимо:

- нажать кнопку «Выход» в правом верхнем углу страницы веб-интерфейса;
- закрыть веб-браузер.