УТВЕРЖДЕНО

RU.09445927.425530-03 34 01-ЛУ

СИСТЕМА INVGUARD AS

Программный комплекс invGuard AS-SW

Руководство оператора

RU.09445927.425530-03 34 01

Листов 150

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
0017	29.05.2014			

2014

АННОТАЦИЯ

В данном программном документе приведено руководство оператора по применению и эксплуатации программного комплекса invGuard AS-SW системы invGuard AS (далее Анализатор), предназначенного для сбора статистики по трафику и нагрузке на сетевое оборудование с целью обнаружения и отражения различных атак на сеть передачи данных оператора связи. Анализатор является составной частью системы защиты от сетевых атак (СЗСА) invGuard (далее Система).

В данном программном документе 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 данном программном документе 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, а также ответы программы на эти команды.

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

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Функциональное назначение программы

Функциональным назначением Анализатора является обнаружение DoS/DDoS-атак на телекоммуникационное оборудование в высокоскоростных сетях передачи данных и управление аппаратными средствами Системы для отражения (подавления) данных атак.

1.2 Эксплуатационное назначение программы

Программный комплекс разработан для применения в составе системы invGuard AS, входящей в СЗСА invGuard.

Пользователями Системы должны быть специалисты в области сетевой безопасности, ответственные за эксплуатацию телекоммуникационного оборудования.

2. УСЛОВИЯ ВЫПОЛНЕНИИЯ ПРОГРАММЫ

2.1 Минимальный состав аппаратных средств

Минимальный состав используемых технических (аппаратных) средств:

1) сервер с процессором Intel с частотой не менее 2,9 ГГц;
2) оперативная память объемом не менее 16 Гб;
3) жесткий диск объемом 500 Гб и выше;
4) две сетевые карты LAN не менее 1 Гбит/с.

2.2 Минимальный состав программных средств

Для функционирования программы необходимо следующее программное обеспечение:

1) Локализованная и сертифицированная по требованиям безопасности операционная система (например, РОСА SX «КОБАЛЬТ» 1.0);
2) Apache 2.2 и выше;
3) PHP 5.2 и выше;
4) MySQL 5.1 и выше.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1 Использование веб-интерфейса

3.1.1 Вход и выход из Системы

3.1.1.1 Введение

Прежде чем использовать веб-интерфейс убедитесь, что на ПЭВМ установлен веб-браузер.

3.1.1.2 Принятие сертификата

При первом входе в Систему 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.

3.1.1.3 Вход в веб-интерфейс пользователя

Для того чтобы зайти в веб-интерфейс, 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.
5) Нажмите «Войти». Откроется суммарный отчет по сети (Система → Статус → Суммарный отчет).

3.1.1.4 Выход из веб-интерфейса пользователя

Для выхода из интерфейса пользователя выполните следующие действия:

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

2) Закройте браузер.

3.1.1.5 Действия при первом входе в Систему

При первом входе в Систему необходимо выполнить действия, описанные в таблице 1.

Таблица 1 – Действия при первом входе в Систему

Режим	Действия
Администратор	– Войдите в Систему, используя учетную запись администратора. – Смените пароль. – Создайте учетные записи для пользователей.
Пользователь	– Войдите в Систему, используя учетную запись и пароль, выданные администратором. – Если у вас достаточно прав доступа для смены пароля, сделайте это.

3.1.2 Навигация по веб-интерфейсу

3.1.2.1 Введение

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

3.1.2.2 Навигационное меню

Навигационное меню (см. рисунок 1) позволяет перемещаться между экранами веб-интерфейса.

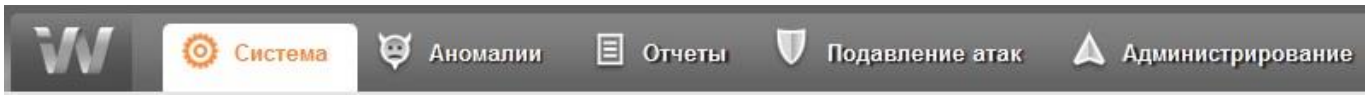


Рисунок 1 – Вид навигационного меню

Все экраны размещены по пунктам в навигационном меню. Описание пунктов смотрите в таблице 2.

Таблица 2 – Пункты навигационного меню

Пункт	**Описание**
Отчеты	Содержит всевозможные отчеты о сети, трафике, наблюдаемых объектах 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.

3.1.2.3 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

подчёркнут. 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.

3.1.2.4 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.

3.1.2.5 Обновление страницы

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

3.1.2.6 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.

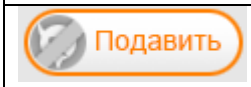
3.1.3 Средства работы с аномалиями

3.1.3.1 Введение

При просмотре экрана «Детальный отчет» по аномалии, можно быстро предпринять какие-либо действия в отношении неё.

Для удобства оператора, на этом экране есть кнопки для работы с аномалией, описание которых приведено в таблице 3.

Таблица 3 - Кнопки для работы с аномалией

Кнопка	Описание
	Позволяет подавить аномалию одним из следующих способов: – Очистителем; – blackhole маршрутизацией; – созданием flow specification; – скриптом; – ACL-фильтром для маршрутизатора.
	Позволяет скрыть текущую аномалию в списке аномалий на указанное время.

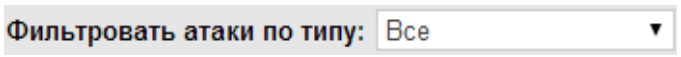
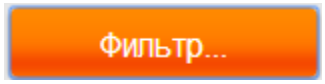
3.1.4 Средства навигации по списку аномалий

3.1.4.1 Введение

Когда возникает большое количество аномалий, которое не может поместиться на странице, используйте инструменты навигации по списку аномалий.

Для таблиц аномалий применяются те же инструменты, что и для многостраничных таблиц. В дополнении к этому имеется несколько специфичных для аномалий инструментов. Описание этих инструментов приведено в таблице 4.

Таблица 4 - Инструменты навигации для аномалий

Инструмент навигации	Описание
Перейти по ID 	Позволяет показать только аномалию с введенным ID.
Фильтровать по типу 	Позволяет показать атаки только определенного типа.
Фильтр 	Расширенный фильтр. Позволяет вывести только аномалии, соответствующие параметрам, см. рисунок 2.

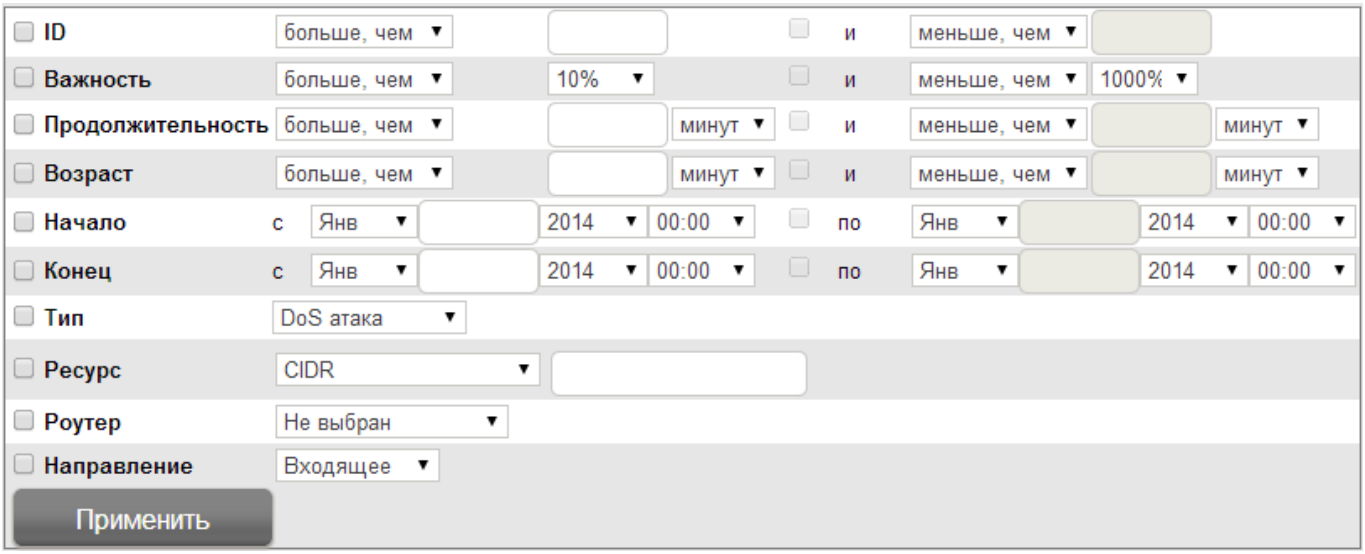


Рисунок 2 – Расширенный фильтр по аномалиям

3.1.5 Средства навигации на страницах отчетов

3.1.5.1 Введение

Вид и параметры выводимого отчета могут быть настроены.

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

3.1.5.2 Выбор периода отчета

Каждый отчет содержит поле выбора периода, за который представлены данные, см. рисунок 3. Интервалы, содержащиеся в меню выбора периода, описаны в таблице 5.

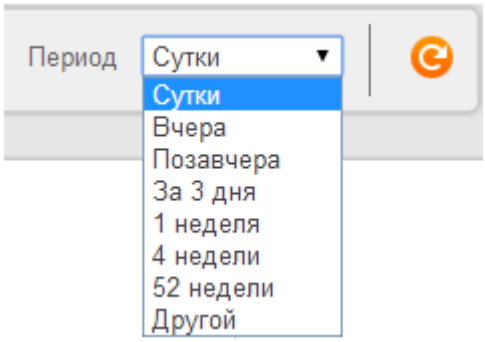


Рисунок 3 – Поле выбора периода

Таблица 5 - 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

3.1.5.3 Выбор единиц измерения

Единицы измерения, в которых показывается сетевой трафик в отчете, выбираются пользователем. В поле выбора «Единицы» (см. рисунок 4) можно выбрать одну из двух единиц измерения:

- bps (биты в секунду);
- pps (пакеты в секунду).

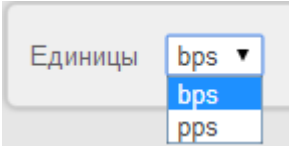


Рисунок 4 – Поле выбора единиц измерения

3.1.5.4 Выбор объекта

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

3.1.5.5 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.

3.1.5.6 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».

3.1.5.7 Значения в таблицах отчетов

Виды значений в таблицах отчетов приведены в таблице 6.

Таблица 6 – Виды значений в таблицах отчетов

Вычисление	Описание
Текущий	Значения за последний 5-минутный интервал времени. **Замечание:** для большинства отчетов доступно только при выбранном периоде «Сутки».

Вычисление	Описание
Средний	Средние значения за выбранный период времени
Максимальный	Максимальное значение за выбранный период времени
PCT95	95-ый процентиль за выбранный период времени

Замечание: чтобы выбрать тот или иной вид вычисления, нажмите на соответствующую ссылку под панелью выбора параметров отчета, см. рисунок 5.

Рисунок 5 – Поле выбора режима вычислений

3.1.5.8 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.

3.1.6 Виды отчетов

Виды отчетов, которые строит веб-интерфейс Анализатора, приведены в таблице 7.

Таблица 7 – Виды отчетов

	Состояние сети	Соседи	Клиент	Профиль	Черви	Роутер	Интерфейс	Очиститель	XML
Суммарный отчет	●								
Сравнение соседей		●							
Соседи		●							
Сравнение клиентов			●						
Клиенты			●						
Сравнение профилей				●					
Профиль				●					
Приборная панель						●			
Сравнение роутеров						●			
Роутер						●			
Сравнение интерфейсов							●		
Интерфейс							●		
SNMP-счетчики							●		
Сравнение Очистителей								●	
Очиститель								●	
Приложения									
Все	●	●	●	●		●	●	●	
ICMP	●	●	●	●		●	●	●	
TCP	●	●	●	●		●	●	●	
UDP	●	●	●	●		●	●	●	
DNS									
Рейтинг FQDN-запросов								●	
Рейтинг RDN-запросов								●	
HTTP									
Рейтинг FQDN-запросов								●	
Рейтинг RDN-запросов								●	
Рейтинг запрашиваемых документов								●	
Рейтинг MIME типов								●	
VOIP									
Рейтинг кто звонит								●	

	Состояние сети	Соседи	Клиент	Профиль	Черви	Роутер	Интерфейс	Очиститель	XML
Рейтинг кому звонят								●	
Рейтинг звонков								●	
BGP-атрибуты									
AS-Расстояния		●					●		
ASN									
Все	●	●	●	●		●	●		
Origin	●	●	●	●		●	●		
Соседи	●		●	●		●	●		
NULL		●	●	●		●	●		
TCP						●			
UPD						●			
ASPaths	●	●				●	●		
ASxAS	●								
Communities	●	●				●	●		
NextHops	●	●	●	●		●	●		
Префиксы	●	●				●	●		
По объектам									
Клиенты	●	●	●	●		●	●		
Профили	●	●	●	●		●	●		
Роутеры	●	●	●						
Интерфейсы	●								
Локальные границы			●	●					
Сетевые границы			●	●					
Multicast	●								
Приложения	●								
Все	●								
Ipv4 UDP	●								
Клиенты	●								
Интерфейсы	●								
Размер пакетов	●								
Профили	●								
Протоколы	●								

	Состояние сети	Соседи	Клиент	Профиль	Черви	Роутер	Интерфейс	Очиститель	XML
QoS	●								
Тип сервиса	●								
Тип сервиса (DTRM)	●								
IP Precedence	●								
DSCP	●								
Роутеры	●								
Рейтинг по потреблению трафика	●								
Источники	●								
Группы	●								
Размер пакетов	●	●	●	●		●	●	●	
Соседи	●	●	●	●		●	●		
Протоколы	●	●	●	●		●	●	●	
QoS									
Тип сервиса	●	●	●	●		●	●	●	
Тип сервиса (DTRM)	●	●	●	●		●	●	●	
IP Precedence	●	●	●	●		●	●	●	
DSCP	●	●	●	●		●	●	●	
Топология роутинга									
BGP суммарный отчет	●								
BGP статистика маршрутов	●								
BGP нестабильность	●	●				●			
BGP сообщения	●								
BGP таблица маршрутизации	●								
BGP количество маршрутов		●				●			
BGP длина префикса						●			
Интерфейсы						●			
DoS-аномалии			●						
Все аномалии			●						
Инфицированные хосты									
Суммарный отчет			●	●					
Инфицированные хосты по червям			●	●					
Рейтинг по потреблению трафика							●		

	Состояние сети	Соседи	Клиент	Профиль	Черви	Роутер	Интерфейс	Очиститель	XML
Внутренние префиксы			●	●					
Внешние префиксы			●	●					
Отчет об активности					●				
Отчет активности									
Инфицированные хосты клиентов					●				
Инфицированные хосты клиентов по червям					●				
Инфицированные хосты профилей					●				
Инфицированные хосты профилей по червям					●				
Сигнатуры червей									
Суммарный отчет					●				
Детали					●				
Рейтинг инфицированных хостов					●				
По объектам									
Клиенты					●				
Профили					●				
Интерфейсы					●				
Темные IP					●				
Суммарный отчет					●				
Подозрительные хосты					●				
По объектам					●				
Клиенты					●				
Профили					●				
Интерфейсы					●				
Утилиты									
Диаграмма AS		●							
Оценка договоренностей соседей		●							
XML-импорт									●
XML-экспорт									●

3.1.7 Классификация интерфейсов

3.1.7.1 Введение

Система производит автоматическое определение типов интерфейсов, базируясь на характеристиках трафика.

Это важный шаг для использования интерфейсов в качестве границ и дальнейшего определения направления трафика относительно сети и наблюдаемых объектов.

3.1.7.2 Типы интерфейсов

Анализатор классифицирует интерфейсы по типам, перечисленным в таблице 8. Графическая иллюстрация на рисунке 6.

Таблица 8 – Типы интерфейсов

Тип	Описание
Внешний	Интерфейс подключен к внешней сети (соседу).
Внутренний	Интерфейс подключен только к локальным хостам внутри сети.
Магистральный	Интерфейс соединяет роутеры внутри сети, передает как внешний, так и внутренний трафик.
Смешанный	Интерфейс, соединенный с роутером с которого Система не получает NetFlow-поток. Трафик этого интерфейса может быть, как внешним трафиком, так и внутренним.
Игнорируемый	Интерфейс, трафик идущий через который игнорируется. Независимо от того, является ли интерфейс входящим или исходящим в NetFlow-дейтаграмме, он будет проигнорирован Анализатором.

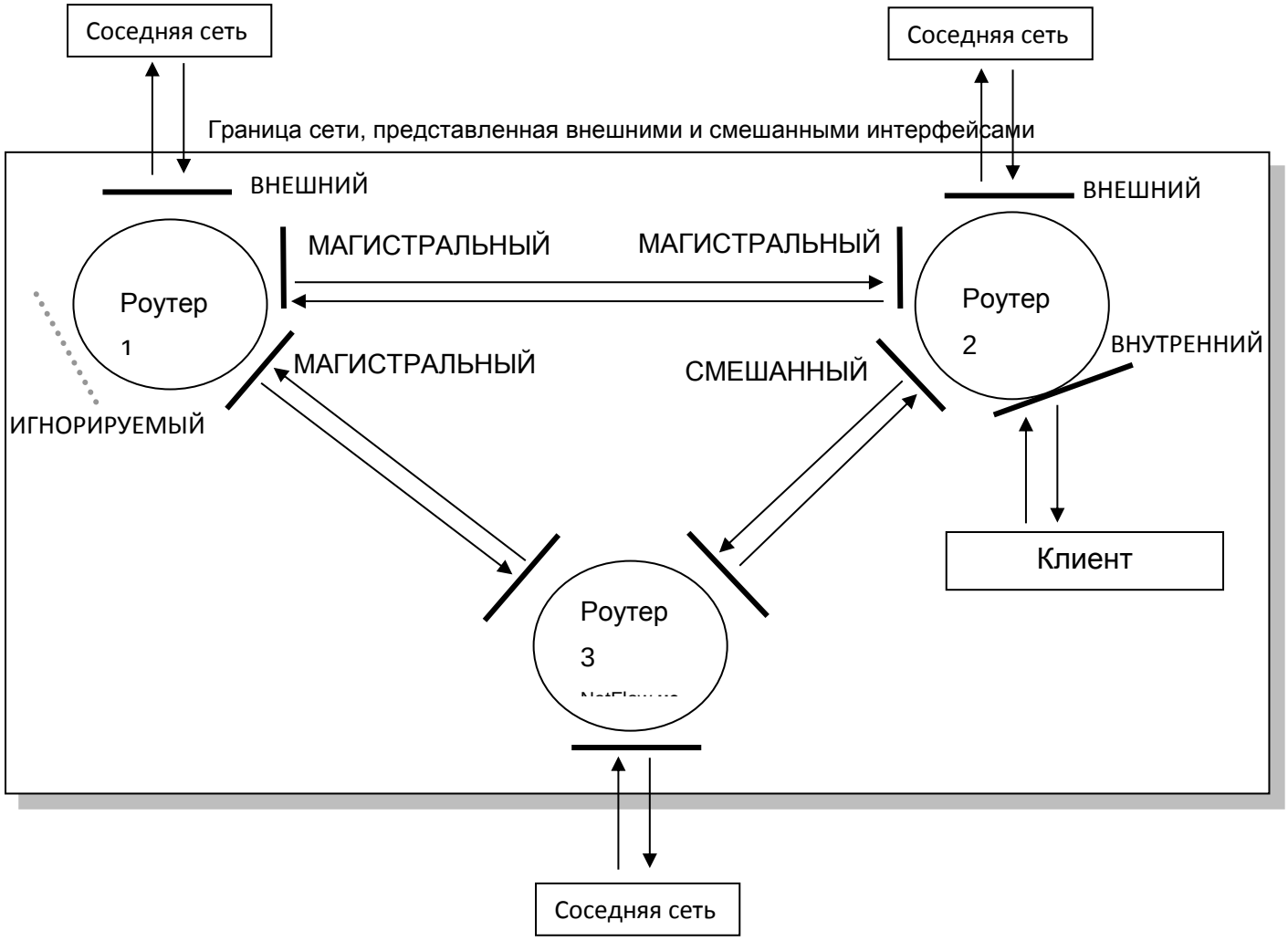


Рисунок 6 – Типы интерфейсов

3.1.8 Работа с наблюдаемыми объектами

3.1.8.1 Введение

Наблюдаемые объекты – совокупность объектов сети, потоков трафика и сетевых сервисов, рассматриваемая Анализатором как единое целое в контексте задач мониторинга и обнаружения сетевых угроз.

3.1.8.2 Типы наблюдаемых объектов

Анализатор делит наблюдаемые объекты на типы, представленные в таблице 9.

Таблица 9 – Типы наблюдаемых объектов

Тип наблюдаемого объекта	Описание
Клиент	Сетевая единица, которую можно определить для отслеживания трафика и обнаружения аномалий клиентов, как находящихся внутри контролируемой сети, так и вне её.
Профиль	Подсеть контролируемой сети или любой другой сети. Профили можно использовать для наблюдения за любыми сетевыми сервисами, например, DNS-серверами, центрами коммутации данных, медиа-порталами.
Сосед	Внешняя сеть, непосредственно подключенная к контролируемой сети. Используйте для отслеживания трафика соседних сетей.
Червь	Сетевые потоки, представляющие потенциально опасность для контролируемой сети.

3.1.8.3 Просмотр всех наблюдаемых объектов

Для просмотра списка всех созданных в Системе наблюдаемых объектов используйте экран «Все наблюдаемые объекты» (Администрирование → Мониторинг → Наблюдаемые объекты → Все). Экран перечисляет наблюдаемые объекты всех типов с указанием названия объекта и способа его определения. С этого экрана можно перейти к редактированию или удалению объекта.

3.1.9 Работа с наблюдаемыми объектами «Клиент» и «Профиль»

3.1.9.1 Введение

Наблюдаемые объекты «Клиент» и «Профиль» очень похожи по характеристикам и способам настройки. В этой главе дается описание этих типов объектов и инструкции по работе с ними.

3.1.9.2 О наблюдаемом объекте «Клиент»

Используйте наблюдаемый объект «Клиент» для отслеживания трафика и обнаружения аномалий ваших клиентов, находящихся как в вашей сети, так и вне её.

3.1.9.3 О наблюдаемом объекте «Профиль»

Используйте наблюдаемый объект «Профиль» для отслеживания трафика и выявления аномалий в подсети контролируемой сети или любой другой сети. Объект «Профиль» может использоваться для мониторинга любых сетевых сервисов, например, HTTP-серверов или медиа-порталов.

3.1.9.4 Экраны для работы с наблюдаемыми объектами «Клиент» и «Профиль»

Экран «Клиент» (Администрирование → Мониторинг → Наблюдаемые объекты → Клиент) перечисляет все раннее созданные наблюдаемые объекты типа «Клиент».

Экран «Профиль» (Администрирование → Мониторинг → Наблюдаемые объекты → Профиль) перечисляет все раннее созданные наблюдаемые объекты типа «Профиль».

На этих экранах в списке объектов указываются названия и способ задания объектов.

3.1.9.5 О фильтрах, используемых в конфигурации наблюдаемых объектов «Клиент» и «Профиль»

Анализатор определяет наблюдаемый объект «Клиент» и «Профиль» по следующим основным характеристикам: название и фильтр.

Трафик, который «видит» Анализатор, сравнивается с фильтром наблюдаемого объекта и, если он соответствует фильтру, трафик ассоциируется с объектом.

Типы фильтров для задания наблюдаемых объектов, поддерживаемые Анализатором, см. в таблице 10.

Таблица 10 – Фильтры для задания наблюдаемых объектов «клиент» и «профиль»

Фильтр	**Описание**
Advanced Boolean matching	Выражение для фильтрации трафика, комбинирующее атрибуты потока и атрибуты маршрутизации. Атрибуты маршрутизации включают в себя: регулярное выражение для AS-маршрута, BGP communities, CIDR-блоки.
ASPath regexp	Регулярное выражение для AS-маршрута соответствующее формату Cisco.
CIDR-блоки	Один или несколько CIDR-блоков в формате A.B.C.D/N. Используйте пробелы для разделения нескольких значений. Анализатор для обнаружения аномалий учитывает суммарный трафик по всем CIDR-блокам и создает аномалию для всего объекта.
CIDR-группы	Один или несколько CIDR-блоков в формате A.B.C.D/N, объединенных одним названием и представляющих собой CIDR-группу. Возможен ввод нескольких CIDR-групп через разделитель точка с запятой (;). Внутри одной группы для разделения CIDR-блоков используйте запятую. При выявлении аномалий, Анализатор учитывает трафик для каждой группы независимо и в случае аномалии по профилю поведения объекта создает аномалию для каждой из групп объекта независимо.
BGP communities	Одна или несколько BGP community в формате X:Y, где X обозначает ASN и Y обозначает локальный номер для AS X. Используйте запятые для разделения нескольких BGP community. Фильтр срабатывает, если как минимум одна из перечисленных BGP community соответствует потоку.
Соседние ASN	Один или несколько ASN соседних сетей.
Local ASN / SubAS	ASN используемый в контролируемой сети.
Фингерпринт	Выражение на языке “Фингерпринт”.

3.1.9.6 Создание или редактирование наблюдаемого объекта «Клиент» или «Профиль»

Для создания или редактирование наблюдаемого объекта «Клиент» или «Профиль» выполните следующие действия:

1) В зависимости от типа объекта перейдите на один из следующих экранов:

- «Клиент» (Администрирование → Мониторинг → Наблюдаемые объекты → Клиент);
- «Профиль» (Администрирование → Мониторинг → Наблюдаемые объекты → Профиль).

2) Выполните одно из следующих действий:

- кликните на название объекта в списке;
- нажмите «Добавить наблюдаемый объект».

3) Введите название объекта в поле «Название».

4) Введите описание объекта в поле «Описание».

5) Нажмите «Сохранить».

3.1.9.7 Настройка фильтра для наблюдаемого объекта «Клиент» или «Профиль»

Для настройки фильтра по трафику выполните следующие действия:

1) Перейдите на вкладку «Конфигурация».

2) Выберите тип фильтра в поле «Фильтр 1».

3) В соответствии с типом фильтра заполните поле «Значение фильтра».

4) При необходимости выберите и сконфигурируйте дополнительный фильтр в поле «Фильтр 2». Трафиком объекта будет являться трафик, соответствующий одновременно обоим фильтрам.

5) Нажмите «Сохранить».

Если ни один фильтр не задан, то весь трафик, прошедший через граничные интерфейсы учитывается как трафик объекта. Таким образом, задание объекта возможно только при помощи интерфейсов.

3.1.9.8 Настройка расположения для наблюдаемого объекта «Клиент» или «Профиль»

Расположение объекта относительно контролируемой сети может быть задано на вкладке «Границы».

Необходимо точно указывать расположение объекта, т.к. в случае некорректного задания часть трафика, либо весь трафик объекта не будут приниматься во внимание.

По умолчанию Система считает объект «клиент» внутренним объектом контролируемой сети, а объект «профиль» внешним.

3.1.9.9 Использование глобальной границы сети для наблюдаемого объекта «Клиент» или «Профиль»

Для использования глобальной границы сети в качестве границы для наблюдаемого объекта выполните следующие действия:

1) Перейдите на вкладку «Границы».
2) Выберите «Нет (глобальный клиент, игнорировать правила)» в поле «Тип».
3) Нажмите «Сохранить».

3.1.9.10 Использование правил автоконфигурации для определения границы наблюдаемого объекта «Клиент» или «Профиль»

1) Перейдите на вкладку «Границы».
2) Выберите «На основе правил» в поле «Тип».
3) В списке «Правила автоконфигурации» будут перечислены уже существующие правила, соответствующие этому наблюдаемому объекту. Для управления ими используется специализированный экран «Правила автоконфигурации». Чтобы создать новое правило, которое

будет соответствовать этому наблюдаемому объекту, нажмите «Добавить».

4) Нажмите «Сохранить».

3.1.9.11 Использование интерфейсов и правил автоконфигурации для определения границы наблюдаемого объекта «Клиент» или «Профиль»

1) Перейдите на вкладку «Границы».

2) Выберите «Интерфейсы и правила» в поле «Тип».

3) Выберите режим конфигурации граничных интерфейсов объекта в поле «Тип граничного интерфейса». Возможны следующие варианты.

- Простой режим. Граничные интерфейсы пропускают трафик как к объекту, так и от объекта. В этом режиме просто укажите список граничных интерфейсов в поле «Граничные интерфейсы» нажав на «Выбрать интерфейсы».
- Расширенный режим. Граничные интерфейсы делятся на два типа:
    - обращенные к клиенту – трафик через этот интерфейс будет считаться выходным трафиком объекта, когда интерфейс будет являться выходным интерфейсом для потока трафика;
    - обращенные от клиента (к backbone) – трафик через этот интерфейс будет считаться исходящим трафиком объекта, когда интерфейс будет являться выходным для потока трафика.

В этом режиме в полях «Интерфейсы, обращенные к клиенту» и «Интерфейсы, обращенные к backbone» укажите оба списка граничных интерфейсов.

4) В списке «Правила автоконфигурации» будут перечислены уже существующие правила, соответствующие этому наблюдаемому объекту. Для управления ими используется специализированный экран «Правила автоконфигурации». Чтобы создать новое правило, которое будет соответствовать наблюдаемому объекту, нажмите «Добавить».

5) Нажмите «Сохранить».

3.1.9.12 Выявление аномалий по шаблонным пакетам для наблюдаемого объекта «Клиент» или «Профиль»

1) Перейдите на вкладку «Детекция».

2) В поле «По шаблонным пакетам» выберите один из вариантов работы детектора:

- «Всегда выключено». Детектор отключен;
- «По умолчанию (использовать глобальные настройки)». Используются настройки по умолчанию;
- «Всегда включено». Детектор включен. Нажмите «Редактировать» и проведите настройку параметров детектора. Настройки аналогичны глобальным настройкам детектора;

3) Нажмите «Сохранить».

3.1.9.13 Обнаружение аномалий по профилю поведения для наблюдаемого объекта «Клиент» или «Профиль»

1) Перейдите на вкладку «Детекция».

2) В поле «По профилю поведения» выберите один из вариантов работы детектора:

- «Всегда выключено». Детектор отключен;
- «По умолчанию (использовать глобальные настройки)». Используются настройки по умолчанию;
- «Всегда включено». Детектор включен. Нажмите «Редактировать» и проведите настройку параметров детектора. Настройки аналогичны глобальным настройкам детектора;

3) Нажмите «Сохранить».

3.1.9.14 О детекции аномалий по порогам трафика наблюдаемого объекта «Клиент» или «Профиль»

Анализатор позволяет установить для наблюдаемого объекта граничные значения по трафику.

При превышении объема трафика верхней границы или при падении трафика ниже нижней границы, Система создаст аномалию с высокой важностью, без направления.

3.1.9.15 Удаление наблюдаемого объекта «Клиент» или «Профиль»

Для удаления наблюдаемого объекта «Клиент» или «Профиль» выполните следующие действия:

1) Перейдите на один из следующих экранов в зависимости от типа объекта:

- «Клиент» (Администрирование → Мониторинг → Наблюдаемые объекты → Клиент);
- «Профиль» (Администрирование → Мониторинг → Наблюдаемые объекты → Профиль).

2) Установите флажки напротив объектов, которые необходимо удалить.

3) Нажмите «Удалить выбранные».

3.1.9.16 Объединение наблюдаемых объектов «Клиент» и «Профиль» в группы

3.1.9.16.1 Введение

Группирование наблюдаемых объектов упрощает работу со сравнительными отчетами по объектам (например, отчет «Сравнение соседей», «Сравнение клиентов»).

В системе со множеством объектов удобно сравнивать не все объекты между собой, а объекты внутри одной логической группы.

3.1.9.16.2 Добавление и редактирование группы наблюдаемых объектов

Экран «Группы объектов» (Администрирование → Мониторинг → Наблюдаемые объекты → Группы объектов) перечисляет все группы, которые настроены, а также позволяет добавить новую группу или удалить уже существующую.

Находясь на экране выполните одно из следующих действий:

- кликните по названию группы в списке;
- нажмите «Добавить группу».

После этого выполните следующие действия:

1) Введите название группы наблюдаемых объектов в поле «Название».
2) Введите описание в поле «Описание».
3) Нажмите «Добавить/удалить наблюдаемые объекты» для редактирования списка объектов, которые будут входить в группу.

Замечание: объект может принадлежать только одной группе. Для перемещения объекта между группами удалите его из первой группы и только после этого добавляйте во вторую.

4) Нажмите «Сохранить».

3.1.9.16.3 Удаление группы наблюдаемых объектов

Для удаления группы наблюдаемых объектов выполните следующие действия:

1) Перейдите на экран «Группы объектов» (Администрирование → Мониторинг → Наблюдаемые объекты → Группы объектов).
2) Установите галочки для тех групп, которые необходимо удалить.
3) Нажмите «Удалить выбранные».

3.1.10 Общие элементы конфигурации наблюдаемых объектов

3.1.10.1 Введение

В этой главе дается описание общих элементов конфигурации, используемых для наблюдаемых объектов разных типов.

3.1.10.2 Пороги трафика наблюдаемых объектов

Анализатор позволяет установить граничные значения по трафику для наблюдаемого объекта.

При превышении объема трафика верхней границы или если трафик упадет ниже нижней границы, Система создаст аномалию с высокой важностью без направления.

Граничное значение может быть установлено как в pps, так и в bps. Анализатор рассчитывает среднее значение скорости потоков трафика, идущих с объекта и на объект за минуту.

При создании нового наблюдаемого объекта настройки детектирования установлены на использование граничных значений, заданных в Системе по умолчанию. Значение границы по умолчанию задается в абсолютных значениях трафика (не в процентах от скорости, как для интерфейсов), поэтому рекомендуется устанавливать границу для каждого объекта индивидуально (вкладка «Детекция» в диалоге редактирования объекта).

Граница по умолчанию должна быть задана с учетом трафика как самого «большого» объекта, так и трафика «наименьшего» объекта, в противном случае возможны частые срабатывания детектора для этих объектов.

3.1.10.3 Мастер фингерпринтов

Язык «Фингерпринт» позволяет описывать потоки трафика, используя комбинации адресов, портов, протоколов, TCP-флагов.

Фильтры трафика, выполненные на языке «Фингерпринт», называются фингерпринт-выражениями. Они используются в конфигурации всех типов

наблюдаемых объектов для описания потоков трафика, которые должны рассматриваться как трафик объекта.

Мастер фингерпринт-выражений позволяет создавать выражения без знания синтаксиса языка, просто заполняя поля на форме.

Для добавления фингерпринт-выражения в конфигурацию наблюдаемого объекта выполните следующие действия:

1) Перейдите на экран редактирования (или создания) наблюдаемого объекта.
2) Перейдите на вкладку «Конфигурация».
3) В поле «Фильтр 1» или «Фильтр 2» выберите «Фингерпринт» или «Сигнатура червя» если вы редактируете объект типа червь.
4) Нажмите «Открыть мастер фингерпринтов».
5) Заполните необходимые поля в появившейся форме.
6) Нажмите «Добавить».
7) Установите флажок «Использовать фингерпринт для определения направления» в случае, если направление трафика на объект или от объекта должно определяться с помощью фингерпринт-выражения.

Замечание: при использовании указанного флажка убедитесь, что введенный фингерпринт не противоречит другим правилам. Пример противоречивой ситуации: задано фингерпринт выражение src host «адрес внешний по отношению к сети»; граница объекта совпадает с границей сети; расположение объекта внутреннее. В этом случае трафик, идущий с указанного src host, не будет учтен как трафик объекта, так как направление по фингерпринту определяется как «трафик от объекта», а по границам как «трафик, идущий на объект» (объект же внутренний для сети), в чем и состоит противоречие ситуации.

3.1.10.4 Расположение объекта

Расположение для объекта задается относительно контролируемой сети. Объект может находиться внутри или вне сети. По умолчанию клиент является внутренним объектом, а профиль и сосед внешними. Расположение объекта можно задать на вкладке «Границы» в диалоге редактирования. Для червя расположение не задается, т.к. его специфика в том, что он может быть где угодно относительно сети и говорить о направлении трафика для него нельзя.

Анализатор использует информацию о расположении объекта для определения направления трафика относительно объекта (входящий или исходящий), а также для других целей.

Для определения направления трафика используются фильтры, задающие объект, граничные интерфейсы и расположение объекта. Если направление трафика, определенное разными методами получается противоречивым, трафик для объекта не учитывается.

3.1.10.5 Дочерние объекты

Дочерние объекты – это наблюдаемые объекты являющиеся логическим подмножеством объекта. Они используются для расширения множества объектов, с которыми может работать ограниченный пользователь.

Пример использования: клиенту для его личного участия в работе с Системой создана учетная запись ограниченного пользователя. В свойствах учетной записи через группу указан наблюдаемый объект за которым он может наблюдать. Эта схема работает до тех пор, пока сеть клиента не вырастает до той стадии, когда он хочет поделить ее на несколько независимых объектов, к примеру: объект для IT-отдела, для программистов, для гостевого доступа. В этом случае, к первоначальному наблюдаемому объекту в дочерние добавляются объекты, описывающие бухгалтерию, программистов и IT. После этого клиент через ограниченную учетную запись может работать с ними всеми.

3.2 Управление пропускной способностью сети

3.2.1 Введение

Планирование пропускной способности сети – это важнейшая часть работы по управлению сетью.

Планирование пропускной способности экономит ресурсы компании и гарантирует эффективное использование внутренних и внешних каналов передачи данных.

Анализатор предоставляет различные инструменты для решения этих задач, в том числе для поиска перегруженных элементов сети.

3.2.2 Поиск загруженных интерфейсов в сети

3.2.2.1 Введение

Большие объемы трафика могут легко перегрузить интерфейсы. Во избежание перегрузки Анализатор следит за трафиком интерфейсов, и администратор имеет возможность своевременно перенаправить трафик на другие интерфейсы.

3.2.2.2 О пороговых значениях трафика на интерфейсах

Система позволяет настроить пороговые значения нагрузки для интерфейсов, как глобальные для всей Системы, так и индивидуальные, по отдельным интерфейсам.

Если объем трафика на интерфейсах выйдет за заданные рамки Система создаст аномалию по трафику.

По умолчанию верхний порог равен 95%, что означает 95% от пропускной способности интерфейса. Когда трафик в течении минутного интервала превышает объем в 95% от пропускной способности интерфейса, Система создает аномалию для уведомления оператора о потенциальной перегрузке на элементе сети. В этом случае оператор может перенаправить трафик через другие интерфейсы внеся изменения в политику маршрутизации.

3.2.2.3 Экран «Пороги по трафику»

Экран «Пороги по трафику» (Администрирование → Детекция → Пороги по трафику) позволяет настроить следующие пороги:

- верхние и нижние граничные значения трафика интерфейсов, используемые по умолчанию, в процентах от пропускной способности интерфейса;
- верхние и нижние граничные значения трафика наблюдаемых объектов, используемые по умолчанию (в bps и pps).

Примеры использования:

- отслеживание ситуации, когда DNS-серверы достигли значительной нагрузки;
- отслеживание ситуации, когда трафик к определенному серверу стал ниже минимально возможного.

3.2.2.4 Настройка пороговых значений трафика отдельных интерфейсов

Можно настроить граничные значения трафика для каждого интерфейса в отдельности учитывая его специфику.

3.2.2.5 Об использовании экрана аномалий при планировании пропускной способности сети

Экран «Все события» (Аномалии → Все события) отображает все аномалии, в том числе и аномалии по трафику. Для удобства установите в фильтре значение «загрузка канала». В полученном списке будут все аномалии, указывающие на выход трафика за разрешенные граничные значения, как для интерфейсов, так и для наблюдаемых объектов.

Используйте этот экран для поиска загруженных интерфейсов и принятия решений относительно перенаправления трафика через другие интерфейсы.

3.2.2.6 Отчет «Интерфейс»

Отчет «Интерфейс» (Отчеты → Интерфейс → Суммарный отчет → Интерфейс) позволяет оценить объем трафика через интерфейс в течении периода времени. Эта информация может быть использована для определения перегрузки на интерфейсе, анализа картины по трафику за период времени.

3.2.2.7 Сравнительный отчет по интерфейсам

Сравнительный отчет по интерфейсам «Сравнение интерфейсов» (Отчеты → Интерфейс → Суммарный отчет → Сравнение интерфейсов) позволяет сравнить объемы трафика через различные интерфейсы в течении периода времени. Это позволяет определить наиболее и наименее загруженные интерфейсы, сравнить динамику загрузки по времени суток, дням недели и определить интерфейсы с нестандартной моделью использования.

Для использования отчета выполните следующие действия:

1) Перейдите на экран «Сравнение интерфейсов» (Отчеты → Интерфейс → Суммарный отчет → Сравнение интерфейсов).
2) Сравните объем трафика входящего и исходящего по интерфейсам с целью поиска перегруженных интерфейсов.
3) При необходимости кликните по названию интерфейса для просмотра детального отчета.
4) Выбирая различные периоды времени (неделя, месяц, год) проанализируйте, как увеличивался трафик с течением времени. Это поможет заранее предупреждать перегрузку интерфейсов.
5) Для интерфейсов, которые близки к максимальной загрузке проанализируйте трафик других интерфейсов, на которые есть возможность перенаправить трафик.

3.2.3 Использование отчетов по интерфейсам для управления пропускной способностью контролируемой сети

3.2.3.1 Введение

Используйте отчеты по интерфейсам для наблюдения за трафиком в контролируемой сети. Это особенно полезно для управления пропускной способностью сети.

3.2.3.2 Отчеты по интерфейсам

В отличие от других типов отчетов, большинство отчетов по интерфейсам недоступны для всех интерфейсов. К примеру, по умолчанию подробные отчеты по трафику доступны только для интерфейсов, классифицированных как внешние. Сбор детальной статистики может быть включен или выключен для других интерфейсов на экране «Редактирование интерфейса».

Важно: включение детальной статистики влияет на производительность Системы. Включайте детальную статистику, только если в этом есть необходимость.

3.2.3.3 Отчет «SNMP-счетчики»

Анализатор собирает статистику о трафике интерфейсов, опрашивая роутеры по протоколу SNMP дополнительно к NetFlow.

Статистика доступна в отчете «SNMP-счетчики» (Отчеты → Интерфейс → Суммарный отчет → SNMP-счетчики).

В отчете доступна информация по следующим счетчикам, см. таблицу 11.

Таблица 11 – SNMP-счетчики

SNMP-счетчик	Описание
Количество пакетов	Трафик bps интерфейса по информации из SNMP.
Количество unicast-пакетов	unicast пакеты в pps.
Количество multicast-пакетов	multicast пакеты в pps.
Количество broadcast-пакетов	broadcast пакеты в pps.

3.2.3.4 Отчеты по приложениям

Отчеты по трафику приложений, идущему через интерфейсы (Отчеты → Интерфейс → Приложения) включают шесть различных отчетов. В таблице 12 даётся описание каждого отчета.

Таблица 12 – Описание отчётов

Отчет	Описание
Все приложения	Показывает входящий и исходящий трафик интерфейса разбитый по приложениям. Система идентифицирует приложения по TCP или UDP-портам.
ICMP	Показывает входящий и исходящий трафик интерфейса разбитый по парам ICMP-тип и код.
TCP	Показывает входящий и исходящий трафик интерфейса разбитый по TCP-портам.
UDP	Показывает входящий и исходящий трафик интерфейса разбитый по UDP-портам.
IPv6 TCP	Показывает IPv6 входящий и исходящий трафик интерфейса разбитый по TCP-портам.
IPv6 UDP	Показывает IPv6 входящий и исходящий трафик интерфейса разбитый по UDP-портам.

3.2.3.5 Отчеты по объектам

Для интерфейсов доступны два вида отчетов по объектам:

- по клиентам;
- по профилям.

Отчеты показывают входящий и исходящий трафик интерфейса для клиентов или профилей.

3.2.4 Отчеты по состоянию сети

3.2.4.1 Введение

Группа отчетов «Состояние сети» (Отчеты → Состояние сети) включает в себя различные отчеты о состоянии, трафике и параметрах наблюдаемой сети.

3.2.4.2 Типы отчетов группы «Состояние сети»

В эту группу входят следующие типы отчетов:

- суммарный отчет;
- приложения;
- BGP-атрибуты;
- Multicast;
- размер пакетов;
- соседи;
- протоколы;
- QoS;
- топология роутинга.

3.2.4.3 Суммарный отчет

Экран «Суммарный отчет» (Отчеты → Состояние сети → Суммарный отчет) позволяет посмотреть сетевой трафик, который Система распределяет по следующим типам:

- входящий;
- исходящий;
- multicast;
- отброшенный;
- всего;

3.2.4.4 О типах трафика

В таблице 13 описаны типы трафика.

Таблица 13 – Типы трафика

Тип трафика	Описание
Входящий	Весь трафик, проходящий через границу наблюдаемой сети внутрь, т.е. проходящий через внешний интерфейс во внутренний.
Исходящий	Весь трафик, проходящий через границу наблюдаемой сети наружу, т.е. проходящий через внутренний интерфейс во внешний.
Multicast	Весь multicast-трафик, входящий в наблюдаемую сеть. Multicast позволяет посылать трафик от одного хоста к нескольким одновременно.

3.2.5 Отчеты по роутерам

3.2.5.1 Введение

Группа отчетов «Роутер» (Отчеты → Роутер) включает в себя отчеты, которые позволяют посмотреть трафик и маршруты настроенных в Системе роутеров.

Замечание: для удобства управления и наблюдения за роутерами, устройства можно объединять в группы.

3.2.5.2 Типы отчетов группы «Роутер»

Группа отчетов «Роутер» включает в себя следующие отчеты:

- суммарный отчет;
- приложения;
- BGP-атрибуты;
- по объектам;
- по размеру пакетов;
- QoS;
- топология роутинга;

3.2.5.3 Отчет «Приборная панель»

Отчет «Приборная панель» (Отчеты → Роутер → Суммарный отчет → Приборная панель) позволяет посмотреть полную информацию о роутере. Информация, которую позволяет просмотреть данный отчет, описана в таблице 14.

Таблица 14 – Описание графиков отчета «Приборная панель»

Название графика	Описание
Трафик (NetFlow)	График показывает объем трафика, идущего через роутер.
Аномалии BGP и аномалии загрузки канала	График отображает количество аномалий BGP и аномалий загрузки канала зарегистрированных на роутере.
Flow	График отображает количество flow-пакетов, полученных Анализатором с роутера.
Загрузка CPU	График показывает загрузку процессора роутера.
Использование памяти	График показывает объем используемой памяти роутера.
Количество BGP-маршрутов	График показывает количество маршрутов в таблице маршрутизации роутера.
Количество BGP-обновлений	График показывает количество BGP-обновлений маршрутов.

3.2.5.4 Отчет «Сравнение роутеров»

Отчет «Сравнение роутеров» (Отчеты → Роутер → Суммарный отчет → Сравнение роутеров) показывает входящий, отброшенный и multicast-трафик для выбранной группы роутеров. График показывает зависимость трафика от времени.

3.2.5.5 Отчет «Роутер»

Отчет «Роутер» (Отчеты → Роутер → Суммарный отчет → Роутер) показывает общую информацию о трафике, проходящем через роутер, распределенную по типам (входящий, отброшенный, multicast, всего).

3.2.5.6 Отчет «Интерфейсы»

Отчет «Интерфейсы» (Отчеты → Роутер → Интерфейсы) позволяет узнать объем трафика, проходящего через интерфейсы роутера. С помощью переключателя

«Источник данных» можно изменять источник статистических данных: NetFlow или SNMP.

В режиме NetFlow-данных в отчете показываются только наблюдаемые интерфейсы роутера, на которых был зарегистрирован трафик. В режиме SNMP показываются все интерфейсы, на которых был зарегистрирован трафик.

3.2.6 Отчеты по объектам «Клиент» и «Профиль»

3.2.6.1 Введение

Наблюдаемые объекты «Клиент» и «Профиль» похожи по способу конфигурирования и по выполняемым функциям, отчеты для них тоже очень похожи. Отчеты доступны через меню по следующему пути:

- «Отчеты → Клиент» для наблюдаемого объекта «Клиент»;
- «Отчеты → Профиль» для наблюдаемого объекта «Профиль».

Замечание: группа отчетов «Клиент» дополнительно содержит отчеты по аномалиям клиента, отчеты аналогичны общесетевым отчетам «Все события» и «DoS-аномалии», но выводят список аномалий только для выбранного клиента.

3.2.6.2 Типы отчетов групп «Клиент» и «Профиль»

Группы отчетов «Клиент» и «Профиль» содержат следующие типы отчетов:

- суммарный отчет;
- приложения;
- BGP-атрибуты;
- инфицированные хосты;
- по объектам;
- по размеру пакетов;
- QoS;
- рейтинг по потреблению трафика.

3.2.6.3 Отчет «Сравнение клиентов/профилей»

Отчет «Сравнение клиентов/профилей» (Отчеты → Клиент/Профиль → Сравнение клиентов/профилей) показывает входящий, исходящий, общий трафик для клиентов или профилей. График показывает зависимость трафика от времени.

3.2.6.4 Отчеты «Клиент» и «Профиль»

Отчеты «Клиент» и «Профиль» (Отчеты → Клиент/Профиль → Клиент/Профилей) показывают суммарную информацию для клиента или профиля. В отчетах можно увидеть информацию о входящем, исходящем, отброшенном и общем трафике для выбранного клиента или профиля. График показывает зависимость трафика от времени.

3.2.6.5 Отчеты по инфицированным хостам

Этот вид содержит следующие отчеты:

- отчет «Суммарный отчет» (Отчеты → Клиент/Профиль → Инфицированные хосты → Суммарный отчет) показывает пиковый трафик, который был классифицирован как трафик червя, идущий с хостов клиента или профиля. Если хост инфицирован несколькими червями, в таблице показывается только пиковый трафик одного червя. При нажатии на «Детали» для хоста отображается график зависимости инфицированного трафика хоста от времени для всех червей. То есть, в случае нескольких червей, весь инфицированный трафик хоста будет отображен на графике.
- отчет «Инфицированные хосты по червям» (Отчеты → Клиент/Профиль → Инфицированные хосты → Инфицированные хосты по червям) похож на предыдущий отчет, но показывает, каким именно червем инфицирован хост. Если хост инфицирован несколькими червями, показываются все черви (в разных строках отчета). При нажатии на «Детали» показывается график только для

выбранного хоста и выбранного червя. По этой причине детальные графики в этих отчетах разные.

3.2.6.6 Отчеты «Рейтинг по потреблению трафика»

Этот вид содержит следующие отчеты:

- отчет «Внутренние префиксы» (Отчеты → Клиент/Профиль → Рейтинг по потреблению трафика → Внутренние префиксы) позволяет просмотреть 100 IP-адресов внутренних для клиента или профиля по пиковому трафику. Для вывода дополнительной информации нажмите на кнопку «Детали»;
- отчет «Внешние префиксы» (Отчеты → Клиент/Профиль → Рейтинг по потреблению трафика → Внешние префиксы) позволяет просмотреть 100 IP-адресов внешних для клиента или профиля по пиковому трафику. Для вывода дополнительной информации нажмите на кнопку «Детали».

3.2.7 Работа с наблюдаемыми объектами типа «Червь»

3.2.7.1 Введение

Наблюдаемый объект «Червь» позволяет следить за потенциальным трафиком червей (вирусов) в сети. Черви могут быть заданы фингерпринт-выражениями, а также диапазонами IP-адресов.

3.2.7.2 Просмотр созданных объектов

Экран «Червь» (Администрирование → Мониторинг → Наблюдаемые объекты → Червь) показывает список всех наблюдаемых объектов типа «Червь», созданных в Системе. На экране показывается наименование и конфигурация червя.

3.2.7.3 Создание или редактирование наблюдаемого объекта «Червь»

Для создания или редактирование наблюдаемого объекта «Червь» выполните следующие действия:

1) Перейдите на экран «Червь» (Администрирование → Мониторинг → Наблюдаемые объекты → Червь).

2) Выполните одно из следующих действий:

- кликните по названию существующего червя в списке;
- нажмите «Добавить наблюдаемый объект».

3) Введите название червя в поле «Название».

4) Введите описание червя в поле «Описание».

5) Перейдите на вкладку конфигурация.

6) Выберите один из двух типов фильтра в поле «Фильтр 1»:

- сигнатура червя;
- CIDR-блоки.

7) Если в качестве фильтра выбрана сигнатура червя, то выполните одно из следующих действий:

- напишите фингерпринты в поле «Фингерпринт»;
- нажмите на кнопку «Открыть мастер фингерпринтов» для добавления фингерпринтов с помощью мастера.

Замечание: при необходимости поставьте флажок «Рассматривать только трафик темных IP», тогда фингерпринт будет применяться только к трафику “темных” IP-адресов, а остальной трафик рассматриваться не будет.

1) Если в качестве фильтра выбрано задание CIDR-блоков, то в поле значение фильтра введите диапазоны IP-адресов, которые соответствуют червю.

2) При необходимости выберите и сконфигурируйте дополнительные фильтры в поле «Фильтр 2».

3) Перейдите на вкладку «Детекция».

4) Введите верхнюю границу трафика по bps и pps в поля «Верхняя граница».

5) Нажмите «Сохранить».

3.2.7.4 Удаление наблюдаемого объекта «Червь»

Для удаления червя выполните следующие действия:

1) Перейдите на экран «Червь» (Администрирование → Мониторинг → Наблюдаемые объекты → Червь).
2) Установите флажки для тех червей, которых необходимо удалить.
3) Нажмите «Удалить выбранные».

3.2.8 Отчеты по червям

3.2.8.1 Введение

Отчеты по червям показывает информацию о возможной активности червей в вашей сети в реальном времени.

3.2.8.2 Отчет об активности червя

«Отчет об активности» (Отчеты → Черви → Отчет об активности) содержит элементы, перечисленные в таблице 15.

Таблица 15 - Элементы отчета об активности червя

Элемент	Описание
График количества инфицированных хостов по червям	График показывает количество хостов, которые соответствуют червю
График влияния червей на сеть	График показывает входящий и исходящий трафик, принадлежащий червю
Таблица количества инфицированных хостов по червям	Таблица показывает для каждого червя текущее, среднее и максимальное количество инфицированных хостов
Таблица влияния червей на сеть	Таблица показывает текущий, средний и максимальный трафик для каждого червя

3.2.8.3 Отчеты по инфицированным хостам клиентов/профилей

Отчеты по инфицированным хостам клиентов/профилей показывают трафик червя для определенного хоста клиента или профиля. Описание отчетов приведено в таблице 16.

Таблица 16 - Отчеты по инфицированным хостам

Отчет	Описание
«Инфицированные хосты клиентов/профилей» (Отчеты → Черви → Отчет активности → Инфицированные хосты клиентов/профилей).	Показывает график зависимости от времени трафика червей посланного с хостов клиента или профиля и таблицу инфицированных хостов с указанием пикового трафика, сгенерированного червем.
«Инфицированные хосты клиентов/профилей по червям» (Отчеты → Черви → Отчет активности → Инфицированные хосты клиентов/профилей по червям).	Показывает график зависимости от времени трафика определенного червя посланного с хоста клиента или профиля. Таблица содержит комбинацию хоста клиента и червя определенного для этого хоста.

Замечание: некоторые хосты могут соответствовать сразу нескольким червям.

Замечание: для вывода графика по определенному червю или хосту нажмите на кнопку «Детали».

3.2.8.4 Суммарный отчет по червям

Экран «Суммарный отчет» (Черви → Сигнатура червей → Суммарный отчет) показывает график зависимости от времени входящего и исходящего инфицированного трафика в сети и за ее пределами для выбранного червя. Таблица содержит список червей и информацию о входящем, исходящем и общем трафике для каждого из них.

3.2.8.5 Отчет «Детали»

Отчет «Детали» (Черви → Сигнатура червей → Детали) показывает входящий и исходящий инфицированный трафик сети (подходящий под сигнатуру червя), а также влияние червя на сеть. График зависимости трафика от времени показывает

трафик червя по типам (входящий, исходящий, влияние на сеть). Таблица содержит информацию о текущем, среднем и максимальном значении по типам трафика.

Влияние на сеть – это сумма трафика подходящего под сигнатуру червя по всем интерфейсам сети. Влияние показывает "ущерб" сети от трафика червя.

3.2.8.6 Отчет «Рейтинг инфицированных хостов»

Отчет «Рейтинг инфицированных хостов» (Черви → Сигнатура червей → Рейтинг инфицированных хостов) показывает информацию по хостам, инфицированным определенным червем. График показывает зависимость трафика инфицированных хостов от времени.

3.2.9 Отчеты по «тёмным» IP-адресам

3.2.9.1 Введение

Отчеты «Тёмные IP» (Отчеты → Черви → Темные IP) позволяют отследить, когда компьютеры сети посылают поддельный трафик (трафик с и для несуществующего получателя, или для получателя, до которого нет маршрута). Задав диапазоны IP-адресов, про которые известно, что они не используются, Анализатор может отслеживать трафик к этим диапазонам и информировать об этом.

Можно настроить определение «тёмных» IP-адресов для контролируемой сети с помощью исходящих и целевых диапазонов IP-адресов. Анализатор будет отслеживать любой трафик для любого из адресов из этих диапазонов и помечать его как трафик «тёмных» IP.

3.2.9.2 Пример «темных» IP

Хост с IP-адресом 2.3.4.5 был инфицирован вирусом. Вирус пытается соединиться со случайным IP-адресом внешней сети. Допустим, он пытается соединиться с адресом 92.32.45.65. Хост с IP-адресом не существует и соединение не удается, однако Анализатор отслеживает эту деятельность, т.к. роутер посылает NetFlow-данные о неудачных попытках.

Анализатор отмечает эти попытки, отмечая адрес роутера, исходящий адрес и протокол. Во многих случаях Система также отмечает целевой адрес и порт.

3.2.9.3 «Суммарный отчет» о «тёмных» IP

Суммарный отчет (Отчеты → Черви → Тёмные IP → Суммарный отчет) показывает график трафика к или от «тёмных» IP в зависимости от времени для некоторых хостов или CIDR-блоков, которые отправляют трафик к пространству «тёмных» IP. В таблице показана информация о текущем, среднем и максимальном трафике.

3.2.9.4 Отчет «Подозрительные хосты»

Отчет «Подозрительные хосты» (Отчеты → Черви → Темные IP → Подозрительные хосты) выводит график, который отображает трафик, посланный для хоста или CIDR-блока, который был послан в пространство «тёмных» IP. Таблица содержит список подозрительных адресов с указанием пикового трафика для них.

3.2.10 Использование multicast-отчетов

3.2.10.1 Введение

Multicast-отчеты (Отчеты → Состояние сети → Multicast) позволяют вам следить за multicast-трафиком в сети.

3.2.10.2 Multicast-отчеты

Таблица 17 содержит описания multicast-отчетов.

Таблица 17 - Описание multicast-отчетов

Отчет	Описание
Все приложения (Отчеты → Состояние сети → Multicast → Приложения → Все)	Показывает весь трафик, направленный на диапазон адресов multicast с разбивкой по приложениям.
IPv4 UDP (Отчеты → Состояние сети → Multicast → Приложения → IPv4 UDP)	Показывает весь трафик, направленный на диапазон адресов multicast с разбивкой по UDP-приложениям.
Клиенты (Отчеты → Состояние сети → Multicast → Клиенты)	Показывает весь трафик, направленный на диапазон адресов multicast с разбивкой по клиентам.

Отчет	Описание
Профили (Отчеты → Состояние сети → Multicast → Профили)	Показывает весь трафик, направленный на диапазон адресов multicast с разбивкой по профилям.
Роутеры (Отчеты → Состояние сети → Multicast → Роутеры)	Показывает весь трафик, направленный на диапазон адресов multicast с разбивкой по роутерам.
Интерфейсы (Отчеты → Состояние сети → Multicast → Интерфейсы)	Показывает весь трафик, направленный на диапазон адресов multicast с разбивкой по интерфейсам.
Размер пакетов (Отчеты → Состояние сети → Multicast → Размер пакетов)	Показывает весь трафик, направленный на диапазон адресов multicast с разбивкой по размерам пакетов.
Протоколы (Отчеты → Состояние сети → Multicast → Протоколы)	Показывает весь трафик, направленный на диапазон адресов multicast с разбивкой по протоколам.
Тип сервиса (Отчеты → Состояние сети → Multicast → QoS → Тип сервиса)	Показывает количество посланного трафика, направленного на диапазон адресов multicast с разбивкой по TOS (типам сервиса).
Тип сервиса (DTRM) (Отчеты → Состояние сети → Multicast → QoS → Тип сервиса(DTRM))	Показывает количество посланного трафика, направленного на диапазон адресов multicast с разбивкой по DTRM.
IP Precedence (Отчеты → Состояние сети → Multicast → QoS → IP Precedence)	Показывает количество посланного трафика, направленного на диапазон адресов multicast с разбивкой по IP Precedence.
DSCP (Отчеты → Состояние сети → Multicast → QoS → DSCP)	Показывает количество посланного трафика, направленного на диапазон адресов multicast с разбивкой по DSCP.
Источники (Отчеты → Состояние сети → Multicast → Рейтинг по потреблению трафика → Источники)	Отчет показывает рейтинг по потреблению трафика IP-адресов источников multicast-трафика.

Отчет	Описание
Группы (Отчеты → Состояние сети → Multicast → Рейтинг по потреблению трафика → Группы)	Отчет показывает рейтинг по потреблению трафика multicast-групп.

3.3 Описание типов отчетов

3.3.1 Введение

Анализатор запоминает и показывает данные о трафике в различных разрезах:

- сеть;
- роутер;
- интерфейс;
- наблюдаемый объект (сосед, клиент, профиль, червь).

В отчетах одного типа отображается статистика по трафику в соответствующем разрезе для разных объектов. Например, отчет по TCP для всей сети показывает данные о входящем и исходящем трафике, проходящем через границы сети с разбивкой по TCP-приложениям. Отчет по TCP для соседа показывает информацию о трафике для выбранного соседа. И т.д.

3.3.2 Отчеты по приложениям

3.3.2.1 Введение

Используйте отчеты по приложениям для понимания того, какие типы приложений используются в вашей сети. Отчеты по приложениям будут полезны для операторов сети во время планирования и разработки политики маршрутизации.

3.3.2.2 Типы отчетов по приложениям

Система может генерировать следующие типы отчетов по приложениям:

- все приложения;
- ICMP;

- TCP;
- UDP;
- IPv6 TCP;
- IPv6 UDP.

3.3.2.3 Отчеты «Состояние сети → Приложения → Все»

Отчеты «Состояние сети → Приложения → Все» показывают в совокупности следующую информацию об используемых приложениях:

- группа приложений;
- TCP-порт;
- UDP-порт;
- Тип и код ICMP-сообщения;
- другие IP-протоколы.

Замечание: можно установить названия для TCP/UDP-портов для удобства просмотра отчетов.

Для удобства слежения за приложениями, порты можно объединять в группы и просматривать отчет только для этой группы. Допустим, необходимо проследить, как ведут себя http-серверы в сети. Для этого необходимо выполнить следующие действия:

1) Создать группу http, в которую добавить TCP-порты 80, 81, 8080 и UDP-порты 80, 81, 8080.
2) Открыть отчет «Приложения → Все».
3) В таблице «Список групп приложений» выбрать созданную группу http.
4) Нажать «Обновить список приложений».

Замечание: для автоматического обновления приложений в таблице «Список приложений в выбранной группе» поставьте флажок в поле «обновлять сразу».

5) В таблице «Список приложений в выбранной группе» останутся только приложения выбранной группы.

3.3.3 Группы приложений

3.3.3.1 Введение

Для удобства вывода и анализа информации о приложениях, их можно объединять в группы. Каждая группа может содержать список TCP и UDP-портов.

3.3.3.2 Экран «Группы»

Экран «Группы» (Администрирование → Мониторинг → Приложения → Группы) позволяет просмотреть список созданных групп приложений. Экран содержит. На экране можно увидеть следующую информацию:

- наименование группы;
- TCP-порты, входящие в группу;
- UDP-порты, входящие в группу.

3.3.3.3 Создание и редактирование группы

Для создания или редактирования группы приложений, выполните следующие шаги:

1) Перейдите на экран «Группы» (Администрирование → Мониторинг → Приложения).
2) Выполните одно из следующих действий:
   - кликните по названию группы в списке;
   - нажмите «Создать новую группу».
3) Введите название группы в поле «Название».
4) Введите TCP-порты, которые принадлежат приложениям данной группы.
5) Введите UDP-порты, которые принадлежат приложениям данной группы.

6) Нажмите «Сохранить».

3.3.3.4 Удаление группы

Для удаления группы приложений выполните следующие шаги:

1) Перейдите на экран «Группы» (Администрирование → Мониторинг → Приложения).

2) Отметьте группы для удаления.

3) Нажмите «Удалить выбранные».

3.3.3.5 Отчеты «Состояние сети → Приложения → ICMP»

Отчеты «Состояние сети → Приложения → ICMP» показывает входящий и исходящий трафик с разбивкой по парам ICMP-типам и ICMP-кодам. Отчет показывает график и таблицу с данными о трафике с полями:

- ICMP-сообщение (пара ICMP-тип / ICMP-код);
- входящий трафик;
- исходящий трафик;
- всего.

3.3.3.6 Отчеты «Состояние сети → Приложения → TCP/UDP»

Таблица 18 содержит описание отчетов TCP/UDP по приложениям.

Таблица 18 – Описание TCP/UDP отчетов

Отчет	Описание
Приложения → TCP	Показывает входящий и исходящий IPv4-трафик с типом протокола TCP, с разделением по номеру порта.
Приложения → UDP	Показывает входящий и исходящий IPv4-трафик с типом протокола UDP, с разделением по номеру порта.
Приложения → IPv6 →TCP	Показывает входящий и исходящий IPv6-трафик с типом протокола TCP, с разделением по номеру порта.

Отчет	Описание
Приложения → IPv6 → UDP	Показывает входящий и исходящий IPv6-трафик с типом протокола UDP, с разделением по номеру порта.

Замечание: можно установить названия для TCP/UDP-портов для удобства просмотра отчетов.

TCP/UDP-отчеты содержат таблицу со следующими данными:

- TCP/UDP-приложение (если известно);
- порт;
- входящий трафик;
- исходящий трафик;
- всего (сумма входящего и исходящего трафика).

3.3.4 Отчеты по BGP-атрибутам

3.3.4.1 Введение

Отчеты по BGP-атрибутам позволяют узнать о том, откуда пришел трафик и куда он идет, в разрезе BGP-атрибутов.

Информация, представленная в отчетах по BGP-атрибутам, основана на AS-маршруте до следующего IP-адреса:

- отправителя, если трафик является входящим для объекта (сети / наблюдаемого объекта / интерфейса);
- получателя, если трафик является исходящим для объекта (сети / наблюдаемого объекта / интерфейса).

3.3.4.2 Отчеты «Состояние сети → BGP-атрибуты»

Таблица 19 содержит описания отчетов по BGP-атрибутам.

Таблица 19 – Описание отчетов по BGP-атрибутам

Отчет	**Описание**
BGP-атрибуты → ASN → Все	Отчет показывает входящий и исходящий трафик по отношению к сети или выбранному объекту, с разбивкой по ASN на которые или через которые проходит трафик. ASN, перечисленные в отчете – это множество всех ASN всех AS-маршрутов. Отчет позволяет найти ASN с которыми происходит самый интенсивный обмен трафиком или с помощью поиска уточнить объем трафика по произвольному ASN-у.
BGP-атрибуты → ASN → Origin	Отчет показывает входящий и исходящий трафик по отношению к сети или выбранному объекту, с разбивкой по ASN являющимися: – AS сети отправившей трафик входящий в контролируемую сеть; – AS сети получающей трафик исходящий из контролируемой сети.
BGP-атрибуты → ASN → Соседи	Отчет показывает входящий и исходящий трафик по отношению к сети с разбивкой по ASN непосредственных соседей. Отчет позволяет найти соседние сети с которыми происходит самый интенсивный обмен трафиком или с помощью поиска уточнить объем трафика по для произвольной соседней сети.

Отчет	Описание
BGP-атрибуты → ASPaths	Отчет показывает входящий и исходящий трафик по отношению к сети или выбранному объекту с разбивкой по AS-маршрутам, которыми трафик следует в сеть или идет из сети. Отчет позволяет найти самые загруженные AS-маршруты или с помощью поиска уточнить объем трафика по произвольному AS-маршруту. Следует помнить, что для Системы не существует возможности достоверно определить каким AS-маршрутом трафик пришел в контролируемую сеть. Система использует предположение, что входящий AS-маршрут равен исходящему. Это допущение приводит к погрешностям значений входящего в сеть трафика в отчете по AS-маршрутам.
BGP-атрибуты → ASxAS	Отчет показывает объем транзитного трафика, проходящего через контролируемую сеть в разрезе начального и конечного ASN (соответственно, отправителя и получателя трафика). Отчет позволяет выявить пары сетей, интенсивно обменивающихся трафиком через контролируемую сеть или с помощью поиска уточнить объем транзитного трафика от произвольной сети.
BGP-атрибуты → Communities	Отчет показывает входящий и исходящий трафик по отношению к сети или выбранному объекту, с разбивкой по BGP-сообществам на которые или через которые проходит трафик. Отчет позволяет найти BGP-сообщества, с которыми происходит самый интенсивный обмен трафиком или с помощью поиска уточнить объем трафика по произвольному BGP-сообществу.

Отчет	Описание
BGP-атрибуты → Префиксы	Отчет показывает входящий и исходящий трафик по отношению к сети или выбранному объекту, с разбивкой по CIDR-блокам из таблицы маршрутизации роутеров. Для каждой полученной NetFlow-записи используется таблица маршрутизации роутера, с которого она была получена. Отчет позволяет посмотреть самые загруженные направления (CIDR-блоки) маршрутизации. Отчет указывает CIDR-блоки из таблицы маршрутизации актуальной на момент сбора данных (не на время просмотра отчета).

3.3.5 Отчеты по трафику между объектами

3.3.5.1 Введение

Система предоставляет отчеты по трафику, которым объекты обмениваются между собой. Эти отчеты находятся в меню каждого объекта (наблюдаемого или инфраструктурного) в секции «По объектам».

Отчеты могут быть полезны при планировании сети и разработке политики маршрутизации.

Например, оператор сети работает над уменьшением нагрузки на роутер. Посмотрев отчеты по объектам, он может увидеть какие наблюдаемые объекты «клиенты» посылают свой трафик через этот роутер и какое влияние на него оказывают. Другой пример, оператор сети создает наблюдаемый объект «профиль», соответствующий известному онлайн-сервису, создающему значительный трафик в Интернете. С помощью отчета «Клиенты» (Отчеты → Профиль → По объектам → Клиенты) оператор узнает об объеме трафика, которым наблюдаемые объекты «клиенты» обмениваются с этим онлайн-сервисом.

3.3.5.2 Особенности учета трафика между объектами

Существует ряд особенностей учета трафика между объектами (наблюдаемыми и инфраструктурными) в силу того, что наблюдаемые объекты имеют границы учета трафика необязательно пересекающиеся между собой, см. таблицу 20.

Таблица 20 – Учет трафика между объектами

Тип объекта, для которого строится отчет	**Объекты, трафик на которые отслеживается**	**Расположение отчета в меню**	**Особенность учета трафика**
Сеть	Наблюдаемые объекты «клиент» или «профиль»	Отчеты → Состояние сети → По объектам → Клиенты / Профили	Трафик анализируется на глобальной границе сети, без учета локальных границ наблюдаемых объектов, рассматриваются только фильтры наблюдаемых объектов.
Сеть	Роутеры	Отчеты → Состояние сети → По объектам → Роутеры	Трафик анализируется на глобальной границе сети, указываются роутеры, через которые трафик прошел через границу.
Сеть	Интерфейсы	Отчеты → Состояние сети → По объектам → Интерфейсы	Трафик анализируется на глобальной границе сети, указываются интерфейсы глобальной границы.

Тип объекта, для которого строится отчет	**Объекты, трафик на которые отслеживается**	**Расположение отчета в меню**	**Особенность учета трафика**
Наблюдаемый объект «клиент», «профиль» «сосед» или «червь» (в том числе, “темные” IP)	Наблюдаемые объекты «клиент» или «профиль»	Отчеты → (Тип наблюдаемого объекта) → По объектам → Клиенты / Профили	Трафик анализируется на локальной границе наблюдаемого объекта, для которого строится отчет. Границы отслеживаемых объектов «клиентов» и «профилей» не учитываются (рассматриваются только их фильтры). Если отчет строится для «соседа», используется глобальная граница сети. Если отчет строится для «червя» или “темных” IP, используются все интерфейсы.
Наблюдаемый объект «клиент», «профиль» «сосед» или «червь»	Роутеры	Отчеты → (Тип наблюдаемого объекта) → По объектам → Роутеры	Трафик анализируется на всех роутерах, без учета локальных границ наблюдаемых объектов (рассматриваются только их фильтры). Отчет показывает “участие” каждого роутера в передаче трафика объекту. По этой причине, сумма трафика по роутерам, указанным в отчете может быть больше трафика наблюдаемого объекта.

Тип объекта, для которого строится отчет	Объекты, трафик на которые отслеживается	Расположение отчета в меню	Особенность учета трафика
Наблюдаемый объект «сосед»	Интерфейсы	Отчеты → Соседи → Интерфейсы	Трафик анализируется на глобальной границе сети, указываются интерфейсы глобальной границы, через которые происходит обмен трафиком с «соседом».
Наблюдаемый объект «клиент» или «профиль»	Локальные границы	Отчеты → (Тип наблюдаемого объекта) → По объектам → Интерфейсы → Локальные границы	Трафик анализируется на интерфейсах, представляющих локальную границу наблюдаемого объекта, для которого строится отчет.
Наблюдаемый объект «клиент» или «профиль»	Сетевые границы	Отчеты → (Тип наблюдаемого объекта) → По объектам → Интерфейсы → Сетевые границы	Трафик анализируется на глобальной границе сети, указываются интерфейсы глобальной границы, участвующие в передаче трафика объекта.
Наблюдаемый объект «червь» (в том числе, “темные” IP)	Интерфейсы	Отчеты → Червь → По объектам → Интерфейсы	Трафик анализируется на всех интерфейсах (т.к. у «червя» нет локальной границы).

3.3.6 Отчеты по размерам пакетов, соседям, и протоколам

3.3.6.1 Введение

Эти отчеты показывают поток трафика с разбивкой по размеру пакета, соседу и протоколу.

3.3.6.2 Отчеты «Размер пакетов», «Соседи», «Протоколы»

Таблица 21 содержит информацию о следующих отчетах: размер пакетов, соседи, протоколы.

Таблица 21 - Отчеты по размерам пакетов, соседям, протоколам

Отчет	Описание
Размер пакетов	Показывает входящий и исходящий трафик с разбивкой по размерам пакетов.
Сосед	Отчет показывает входящий и исходящий трафик с разбивкой по наблюдаемым объектам типа «Сосед», через которые он идет.
Протокол	Отчет показывает входящий и исходящий трафик с разбивкой по протоколам.

3.3.7 Отчеты по топологии маршрутизации

3.3.7.1 Введение

Отчеты по топологии маршрутизации показывают статистику изменений BGP-маршрутов для объекта.

3.3.7.2 Отчет «BGP-нестабильность»

Отчет показывает информацию о BGP-нестабильности на всех BGP-сессиях с соседними сетями. Отчет можно использовать для идентифицирования типов BGP-нестабильности, которые могут быть в сети.

Отчет доступен как для отдельных роутеров, так и для всей сети, в этом случае цифры по роутерам складываются.

Отчет помогает определить источник BGP-нестабильности и устранить ее причину.

Следует помнить, что при разрыве соединения между Анализатором и роутером и последующем его восстановлении, Анализатор получает с роутера всю таблицу маршрутизации, в этом случае в отчете будет ложная нестабильность, к примеру параметр TUP будет показывать, что в течении нескольких минут добавились сотни тысяч новых префиксов (точнее, полное множество префиксов).

Информация, представленная в отчете по BGP-нестабильности, указана в таблице 22.

Таблица 22 - Отчет по BGP-нестабильности

Данные	Описание
ANN	Количество полученных BGP-сообщений об анонсировании новых маршрутов, изменении маршрутов. Удаление маршрутов в этом параметре не учитывается, см. параметр WITH.
AADIFF	Количество неявно удаленных (замененных на альтернативные для тех же префиксов) маршрутов.
AADUP	Количество неявно удаленных маршрутов, замененных на копию оригинального.
TUP	Количество новых анонсированных префиксов.
TDOWN	Количество маршрутов, удаленных BGP-сообщениями withdrawal.
UPDATES	Общее количество BGP-сообщений. Является суммой ANN и WITH.
WWDUP	Количество дублирующих withdrawal-сообщений.
WITH	Количество BGP-сообщений withdrawal об удалении маршрутов.

3.3.8 Отчеты QoS

3.3.8.1 Введение

Отчеты Quality of Service представляют следующую информацию:

- TOS;
- DTRM;
- IP precedence;
- DSCP.

Используйте эти отчеты для анализа типов обслуживания, которые вызывают проблемы.

3.3.8.2 Отчет «QoS → Тип сервиса»

Отчет «QoS → Тип сервиса» показывает входящий и исходящий трафик с разбивкой по TOS (типу сервиса). Тип сервиса в этом отчете представляется как десятичное число TOS в TCP-заголовке. Отчет представляет следующую информацию:

- тип сервиса;
- входящий трафик;
- исходящий трафик;
- всего.

Замечание: можно установить названия для значений TOS для удобства просмотра отчетов.

3.3.8.3 Отчет «QoS → Тип сервиса (DTRM)»

Отчет «QoS → Тип сервиса (DTRM)» показывает входящий и исходящий трафик с разбивкой по DTRM. DTRM – это 4 бита (3, 4, 5 и 6) из 8 битов TOS.

Описания битов представлены в таблице 23.

Таблица 23 - Описания битов DTRM

Бит	Описание
D	Минимизирует задержку
T	Максимизирует пропускную способность
R	Максимизирует надежность
M	Минимизирует стоимость

3.3.8.4 Отчет «QoS → IP Precedence»

Отчет показывает входящий и исходящий трафик с разбивкой по IP Precedence. Таблица отчета содержит следующую информацию:

- precedent биты;
- целое значение precedent битов;

- входящий трафик;
- исходящий трафик;
- всего.

IP Precedence отображает 3 бита из TCP-заголовка пакета.

Замечание: обычно для внутренних протоколов маршрутизации precedence устанавливается как 111 (7) а для внешних – 110 (6).

3.3.8.5 Отчет «QoS → DSCP»

Отчет «QoS → DSCP» показывает входящий и исходящий трафик с разбивкой по DSCP. Таблица отчета содержит следующую информацию:

- значение DSCP;
- входящий трафик;
- исходящий трафик;
- всего.

DSCP описан в RFC 2474 и используется, чтобы определить поведение пакета для каждого nexthop.

3.4 Наблюдение за сетевой активностью

3.4.1 Введение

В этой главе дается описание как использовать Анализатор для исследования аномальной деятельности в контролируемой сети.

Анализатор детектирует аномалии на основании формируемых пользователем порогов и извещает о любом аномальном поведении.

Используемые в главе термины «аномалия» и «атака» следует различать. Аномалия – это любая аномальная деятельность, зафиксированная в сети. Аномалия может быть атакой. Атака, как частный случай аномалии – это действия, направленные на вывод вычислительной Системы из строя, то есть создание таких

условий, при которых правомерные пользователи Системы не могут получить доступ к предоставляемым Системой ресурсам, либо этот доступ затруднен. Является ли аномалия атакой или нет, решает оператор Системы, основываясь на знаниях о ресурсе (вычислительной системе), в отношении которого зафиксирована аномалия, а также на важности аномалии и параметрах трафика.

3.4.2 Определение потенциальной опасности

3.4.2.1 Введение

Для просмотра аномалий используйте следующие экраны меню «Аномалии»:

- «Текущие DoS-аномалии» (Аномалии → Текущие DoS-аномалии);
- «Прошедшие DoS-аномалии» (Аномалии → Прошедшие DoS-аномалии);
- «Все события» (Аномалии → Все события);
- «Поиск» (Аномалия → Поиск).

3.4.2.2 Пример использования экранов меню «Аномалии»

Ниже приведен пример возможного сценария использования экранов по аномалиям.

1) Оператор сети получает сообщение об аномалии высокого уровня опасности для клиента Клиент-1 на одном из следующих экранов или посредством ленты событий внизу экрана:

- «Текущие DoS-аномалии» (Аномалии → Текущие DoS-аномалии);
- «Прошедшие DoS-аномалии» (Аномалии → Прошедшие DoS-аномалии).

2) Для получения подробностей об аномалии оператор кликает на ID аномалии в таблице. Для аномалии открывается «Детальный отчет».

3) В таблице «Вовлеченные элементы сети» видно, для каких роутеров и на каких интерфейсах превышен трафик.

4) Для получения дополнительной информации о вовлеченных элементах сети оператор нажимает на «Детали» напротив этого элемента. Открывается «Детальный отчет о трафике».

5) Оператор смотрит на IP-адреса источников, чтобы узнать сколько трафика было послано атакующим.

6) Оператор смотрит на адреса получателей, чтобы понять какие именно IP-адреса клиента Клиент-1 были подвергнуты атаке.

7) Оператор смотрит с каких портов был отправлен трафик, чтобы определить где нормальный трафик, а где трафик атаки, например, нормальный трафик отправляется с портов из диапазона 0-4096, а атакующий трафик может быть 0-65535 (используется случайный порт).

8) Оператор смотрит список портов получателя и определяет где нормальный трафик, а где трафик атаки. Например, если трафик посылается на порт TCP 80, где каждый пакет размером 40 байт, то это аномальный трафик.

9) Оператор просматривает TCP-флаги атакуемого трафика.

10) Таким образом, оператор определил профиль атакуемого трафика. Теперь он может предпринять различные действия для подавления атаки.

3.4.3 Описание аномалий

3.4.3.1 Введение

Анализатор может детектировать различные типы аномалий, которые покрывают различные аспекты поведения сети.

3.4.3.2 Типы аномалий

В таблице 24 приведены описания типов аномалий, предупреждения о которых выдаются Анализатором.

Таблица 24 - Типы аномалий

Тип аномалии	Описание
BGP	Нестабильности BGP, подделка BGP, нарушение политик.
Источник данных	Приостановка получения данных с BGP, SNMP, NetFlow, поддельные источники данных BGP, NetFlow.
DoS	Потенциальные DoS-атаки.
События системы	Изменения конфигурации Системы, ошибки на Анализаторе, события мониторинга Системы, ошибки отправки почты, слишком большое количество аномалий.
Загрузка канала	Нарушение установленного порога трафика.
SNMP	Обнаружение замены устройства.

3.4.3.3 Подтипы аномалий

Для каждого вида аномалии, может быть сгенерировано несколько разных подтипов. Описание приведено в таблице 25.

Таблица 25 - Типы предупреждений

Тип аномалии	Тип предупреждения	Когда возникает
BGP	Нарушение политик BGP	Изменяются BGP-атрибуты AS_PATH и NEXT_HOP для указанного префикса.
	Нестабильность BGP	Число BGP-обновлений становится больше заданного.
	Подделка BGP	Чужая автономная система анонсирует префиксы контролируемой нами автономной системы.
	Переполнение буфера BGP-маршрутов, часть принятых от роутера данных утеряна	Большой поток сообщений по протоколу BGP. Увеличьте размер буфера BGP-сообщений.
Источник данных	Задержка связи по BGP	BGP-соединение между роутерами прервано.
	Задержка связи по NetFlow	От роутера нет NetFlow-записей в течение двух минут.

Тип аномалии	Тип предупреждения	Когда возникает
	Задержка связи по SNMP	Не удалось связаться с роутером по SNMP.
	Подозрение на поддельный источник NetFlow	При подозрении на подделку NetFlow.
	Подозрение на поддельный источник BGP	При подозрении на подделку BGP.
DoS-атака	DNS	Превышение порога по количеству TCP- и UDP-пакетов, идущих на порт 53.
	ICMP	Превышение порога по количеству пакетов ICMP.
	IP NULL	Превышение порога по количеству пакетов с номером протокола, установленным в ноль.
	TCP	Превышение порога по количеству TCP-пакетов.
	TCP-NULL	Превышение порога по количеству TCP-пакетов без флагов.
	TCP-RST	Превышение порога по количеству TCP-пакетов с установленным флагом RESET.
	TCP SYN	Превышение порога по количеству TCP-пакетов с установленным флагом SYN.
	UDP	Превышение порога по количеству UDP-пакетов.
	IP Private (Темные IP)	Превышение порога по количеству пакетов темных IP.
	Превышение трафика для профиля	Превышение порога по профилю детектирования для объектов (кроме червей).
	Общее количество трафика, бит в секунду	Превышение порога в битах в секунду общим трафиком хоста.

Тип аномалии	Тип предупреждения	Когда возникает
	Общее количество трафика, байт в секунду	Превышение порога в пакетах в секунду общим трафиком хоста.
	Превышение порога по трафику для фингерпринта	Превышение порога по трафику для фингерпринта.
Загрузка канала	Маленький трафик на интерфейсе	Трафик на интерфейсе ниже порогового значения.
	Большой трафик на интерфейсе	Трафик на интерфейсе превосходит пороговое значение.
	Маленький трафик от наблюдаемого объекта	Трафик на наблюдаемом объекте ниже порогового значения.
	Большой трафик от наблюдаемого объекта	Трафик на наблюдаемом объекте превосходит пороговое значение.

Тип аномалии	Тип предупреждения	Когда возникает
События системы	– Высокая загрузка CPU; – Угроза переполнения диска; – Угроза переполнения БД; – Мало свободной физической памяти; – Угроза переполнения swap; – Высокая температура CPU.	Мониторинг Системы обнаружил соответствующую неполадку.
	Ошибка процесса	Системный процесс не запущен.
	Обнаружен посторонний процесс	Обнаружен незарегистрированный процесс, возможно – постороннее вмешательство в Систему.
	Превышение количества аномалий для детектора	При обнаружении аномалии если в этот момент времени уже активны больше определенного количества аномалий такого же типа, то новая аномалия не создается. Считается количество несозданных аномалий за минуту и создается аномалия этого вида.
	Проблемы с отправкой почты	Письма в очереди находятся дольше 30 минут.
	Выход показаний датчика за предельные значения	Показания одного из сконфигурированных в Системе датчиков вышли за пределы указанных значений.

Тип аномалии	Тип предупреждения	Когда возникает
	Ошибка опроса датчиков	Система не смогла получить показания с одного из сконфигурированных в Системе датчиков.
	Подозрительное соединение	Зарегистрировано неизвестное сетевое подключение, следует проверить журнал подключений. Если подключение санкционированное, то создать фильтр, если нет – внести его в брандмауэр как запрещенное.
	Превышение количества подозрительных соединений	Зарегистрировано более 5 несанкционированных попыток подключения в течение минуты.
	Ошибка отсылки письма	Произошла ошибка при создании письма для отправки. Обратитесь в службу поддержки.
	Множественные проблемы с отправкой почты	Произошло более 5 ошибок за 10 минут при создании писем для отправки.
	Обнаружена поврежденная таблица в БД	Повреждена таблицы БД. Обратитесь в службу поддержки.
	Автоконфигу - рация, результат	При завершении процесса автоклассификации интерфейсов.
	Прекращение мониторинга BGP-демона из-за множественных ошибок в нем	Аномалия возникает, если BGP-демон был перезапущен три или более раз в течение одного часа. В случае возникновения аномалии, мониторинг состояния BGP-демона прекращается.
Предупреждения Очистителя	Перегрузка модуля вывода	Модуль вывода не успевает обрабатывать пакеты.
	Обнаружение замены устройства.	Поменялось устройство.

Тип аномалии	Тип предупреждения	Когда возникает
	Не удается разрешить MAC-адрес роутера для возврата трафика	Не удается определить MAC-адрес роутера по умолчанию для возврата очищенного трафика. Событие начинается при первой неудачной попытке определить адрес указанного роутера и заканчивается при первой удачной попытке определить этот адрес.
SNMP	Обнаружена замена устройства	Обнаружена замена устройства.

3.4.3.4 Важность аномалии

Аномалии могут иметь разную степень важности. Степень важности оценивается Анализатором в зависимости от того, насколько значения параметров трафика или сети превышают установленные пороги. Описания степеней важности приведено в таблице 26.

Таблица 26 - Степени важности аномалий

Степень важности	Описание
Высокая	Следует немедленно принять меры для подавления атаки
Средняя	Следует проанализировать аномалию, чтобы понять является ли это атакой
Низкая	Принимать какие-либо меры для подавления атаки нет необходимости

3.4.4 Экран «Все события»

3.4.4.1 Введение

Экран «Все события» (Аномалии → Все события) содержит информацию обо всех аномалиях, созданных Анализатором.

3.4.4.2 Экран «Все события»

На экране приведена таблица со всеми аномалиями, созданными Анализатором. Таблица 27 содержит описание полей таблицы экрана.

Таблица 27 - Таблица экрана «Все аномалии»

Поле таблицы	Описание
ID	Идентификатор аномалии.
Время начала	Время, когда была выявлена аномалия.
Время окончания	Время окончания аномалии. Для кратковременных аномалий время окончания может совпадать с временем начала.
Тип аномалии	Тип аномалии.
Информация	Включает в себя некоторую информацию об аномалии, такую как тип предупреждения, объект аномалии, порог и степень превышения порога.

3.4.4.3 Фильтр аномалии

Экран «Все события» позволяет накладывать условия на выводимые аномалии. Например, можно просмотреть только аномалии типа DoS-атака или аномалии, ID которых больше 1000.

Для фильтрации аномалии по типу, выберите тип аномалии в поле «Фильтровать атаки по типу». Если требуются специальные условия фильтрации, нажмите на кнопку «Фильтр» и заполните поля формы.

3.4.4.4 Использование фильтра аномалий

Для фильтрации аномалий по различным критериям используйте фильтр аномалий. Для этого проделайте следующее:

- перейдите на экран со списком аномалий, например, «Все события» или «Текущие/Прошедшие DoS-аномалии»;
- нажмите на кнопку «Фильтр».

Откроется форма с параметрами фильтрации. Описание параметров приведено в таблице 28.

Таблица 28 - Параметры фильтра аномалий

Название графика	Описание
ID	Идентификатор аномалии. Можно задать диапазон индексов аномалии. Например, аномалии с ID, превышающими 1000.
Важность	На сколько процентов трафик (или другой параметр сети или объекта) превышает установленный предел.
Продолжительность	Позволяет показать аномалии с определенной продолжительностью, например, аномалии, длившиеся долее 10 минут.
Возраст	Позволяет показать аномалии, определенного возраста, т.е. возникшие некоторое время назад.
Начало	Позволяет показать аномалии, начинавшиеся в какой-либо промежуток времени, например, аномалии с 1 января по 5 января.
Время начала	Позволяет показать аномалии, закончившиеся в какой-либо промежуток времени, например, аномалии с 1 января по 5 января.
Тип	Позволяет показать аномалии только определенного типа.
Ресурс	Объект, являющийся причиной аномалии, например, наблюдаемый объект, который подвергается атаке.
Роутер	Роутер, участвующий в аномалии. Например, роутер, через который идет повышенный трафик.
Направление	Направление трафика. Входящее/исходящее/неизвестно.
Состояние	Текущие/Завершенные/Все.

Замечание: для некоторых параметров можно задать как начало интервала, так и конец.

3.4.5 Текущие и прошедшие DoS-аномалии

3.4.5.1 Введение

Экран «Текущие DoS-аномалии» (Аномалии → Текущие DoS-аномалии) содержит информацию о текущих DoS-аномалиях. После окончания аномалии,

информация о ней перемещается из экрана «Текущие DoS-аномалий» на экран «Прошедшие DoS-аномалии».

3.4.5.2 Экраны «Текущие DoS-аномалии» и «Прошедшие DoS-аномалии»

Поля таблицы на экранах «Текущие DoS-аномалии» и «Прошедшие DoS-аномалии» описаны в таблице 29.

Таблица 29 - Описание таблицы DoS-аномалий

Название поля	Описание
ID	Идентификационный номер аномалии.
Трафик	Мини-график зависимости аномального трафика (суммированного по всем интерфейсам) от времени.
Важность	Классификация серьезности аномалии (Высокая, Средняя, Низкая).
Влияние	Сумма максимальных значений трафика на всех интерфейсах. Показывает максимальную величину “ущерба” сети от аномалии.
Длительность	Время, в течение которого длилась аномалия.
Время начала	Время начала аномалии.
Направление	Направление аномального трафика: входящее/исходящее относительно ресурса.
Тип	Тип аномалии.
Ресурс	Наблюдаемый объект, объект инфраструктуры или хост, для которого детектирована аномалия.

3.4.6 Детальная информация по DoS-аномалии

3.4.6.1 Введение

Экран «Детальный отчет» позволяет просмотреть особенности трафика DoS-аномалии (потенциальной атаки) и атакуемые сетевые ресурсы. Также, на экране можно выполнить следующие действия:

- подавить атаку;
- записать комментарии к аномалии.

3.4.6.2 Экран «Детальный отчет»

Чтобы попасть на экран «Детальный отчет» выполните следующие действия:

- перейдите на экран «Текущие/Прошедшие DoS-аномалии» или на экран «Все события»;
- кликните на ID DoS-аномалии или введите ID в поле «Перейти по ID».

Экран «Детальный отчет» содержит следующие разделы:

- общая информация;
- характеристика трафика;
- вовлеченные элементы сети;
- комментарии.

3.4.6.3 Общая информация

Информация, содержащаяся в разделе «Общая информация» описана в таблице 30.

Таблица 30 - Поля таблицы «Общая информация»

Название поля	Описание
ID	Идентификационный номер аномалии.
Трафик	Мини-график зависимости аномального трафика (суммированного по всем интерфейсам) от времени.
Важность	Классификация серьезности аномалии (Высокая, Средняя, Низкая).
Влияние	Сумма максимальных значений трафика на всех интерфейсах. Показывает максимальную величину «ущерба» сети от аномалии.
Длительность	Время, в течение которого длилась аномалия.
Время начала	Время начала аномалии.
Направление	Направление аномального трафика: входящее/исходящее относительно ресурса.
Тип	Тип аномалии.
Ресурс	Наблюдаемый объект, объект инфраструктуры или хост, для которого детектирована аномалия.

Название поля	Описание
Время окончания	Время окончания аномалии, если она завершилась.

3.4.6.4 Характеристика трафика

Раздел «Характеристика трафика» содержит суммарную информацию о трафике аномалии:

- диапазоны IP-адресов отправителей с указанием трафика для них;
- диапазоны портов отправителей с указанием трафика для них;
- диапазоны IP-адресов получателей с указанием трафика для них;
- диапазоны портов получателей с указанием трафика для них;
- протоколы с указанием трафика для них;
- список TCP-флагов.

Под трафиком понимается общий объем аномального трафика, прошедшего за все время аномалии по всем интерфейсам.

Диапазоны IP-адресов выводятся в формате:

a.b.c.d/x ? ~ трафик в байтах / трафик в пакетах

При нажатии на ссылку «?» открывается окно с whois-информацией об этой подсети.

Поскольку количество уникальных IP-адресов отправителей и получателей может быть значительным, в Системе используются алгоритмы группировки IP-адресов, позволяющие выявить наиболее активные подсети, на которые приходится основной объем трафика (не менее 1% от общего объема трафика).

В Системе реализованы следующие алгоритмы группировки IP-адресов:

- сложение поддиапазонов;
- выделение общего поддиапазона;
- группировка с приоритетами;

– Top-10;

– Top-10 подсетей, меньших /x.

Сложение поддиапазонов. Этот алгоритм используется по умолчанию. Если одна подсеть полностью входит в другую подсеть, трафик более мелкой подсети добавляется к трафику более крупной подсети – и только она попадает в отбор. Это позволяет быстро оценить, какие наиболее крупные подсети генерируют основной трафик. Для более детального и точного исследования трафика подсетей лучше воспользоваться другими алгоритмами.

Выделение общего поддиапазона. Алгоритм позволяет выделить подсети наименьшего размера, на которые приходится наибольшее количество трафика (не менее 1% от общего объема трафика).

К примеру, если подсеть А генерирует 0,3% трафика, а подсеть Б – 0,8%, и при этом сеть А не входит в подсеть Б, то при использовании предыдущего алгоритма выделения общего поддиапазона ни одна из этих подсетей не попадет в отбор.

Алгоритм выделения общего поддиапазона позволит выделить подсеть В, в которую входят и подсеть А и подсеть Б, и на которую приходится 1,1% от общего трафика.

Группировка с приоритетами. Этот алгоритм является модификацией предыдущего и позволяет дополнительно уменьшить размеры подсетей, на которые приходится наибольшее количество трафика, за счет введения умножающего коэффициента (приоритета) для трафика подсети, обратно пропорционального ее размеру. Чем меньше подсеть, тем больше коэффициент. Алгоритм позволяет минимизировать количество ошибочно заблокированных подсетей при подавлении атаки.

Например, есть две подсети:

– подсеть А a.0.0.0/4 (приоритет 1), на которую приходится 0,8% от общего трафика;

– и подсеть Б a.b.c.0/24 (приоритет 8), на которую приходится 0,2% от общего трафика.

С учетом приоритетов, их трафик составит 0,8% (1×0,8% = 0,8%) и 1,6% (8×0,2% = 1,6%) соответственно, и в отбор попадет подсеть Б.

Top-10. Данный алгоритм по сути не является алгоритмом группирования. Он лишь показывает 10 подсетей, на которые приходится наибольшее количество трафика, при этом никаких дополнительных действий не производится. Метод позволяет быстро оценить масштабы аномалии и насколько могут быть локализованы отправители или получатели трафика.

Top-10 подсетей, меньших /x. Данный алгоритм является модификацией предыдущего. Он позволяет задавать максимальный размер подсети, попадающей в отбор, и показывает 10 подсетей, меньших заданного размера, на которые приходится наибольшее количество трафика. Так, к примеру, при заданном размере подсети /24, в отбор не попадет сеть a.b.0.0/16, даже если на нее приходится 50% трафика.

В списке «Диапазоны портов» представлены как отдельные порты в формате:

порт ~ трафик в байтах / трафик в пакетах

так и диапазоны портов в формате:

начало диапазона..конец диапазона ~ трафик в байтах / трафик в пакетах

трафик которых составляет не менее 10% от общего трафика. Если выделить отдельные порты или поддиапазоны портов не удалось, показывается полный диапазон 0..65535 и весь объем трафика.

3.4.6.5 Вовлеченные элементы сети

Раздел «Вовлеченные элементы сети» показывает все вовлеченные роутеры и интерфейсы. Таблица «Вовлеченные элементы» содержит следующую информацию, см. таблицу 31.

Таблица 31 - Поля таблицы «Вовлеченные элементы сети»

Поле таблицы	Описание
Показать	Показать/скрыть график трафика для этого элемента сети.
Элемент сети	Роутер/интерфейс роутера, который вовлечен в аномальную деятельность.
Опасность	Классификация опасности аномалии (Высокая, Средняя, Низкая).
Ожидаемый трафик	Значение ожидаемого трафика для данного устройства.
Наблюдаемый bps	Среднее/максимальная скорость трафика в bps.
Наблюдаемый pps	Среднее/максимальная скорость трафика в pps.
Детали	Нажмите на кнопку «Детали» для получения дополнительной информации для данного элемента сети.

3.4.6.6 Детальная информация о трафике элемента сети

Экран «Детальный отчет о трафике» позволяет оценить особенности трафика DoS-аномалии (потенциальной атаки) для конкретного элемента сети.

Экран содержит следующие разделы:

- общая информация;
- элемент сети;
- выбор временного интервала;
- подробная информация по трафику.

Разделы «Общая информация» и «Элемент сети» полностью аналогичны соответствующим разделам экрана «Детальный отчет», описанным в главах «Общая информация» и «Вовлеченные элементы сети».

Выбор временного интервала.

Изменение временного интервала оказывает влияние на содержимое таблицы подробной информации по трафику. Можно выбрать одно из заранее заданных значений:

- за все время аномалии;
- первые 10 минут;
- последние 10 минут;
- последняя минута;

Можно задать произвольный интервал, выбрав «Другой интервал» и указав начало и конец диапазона.

По нажатию на кнопку «Обновить», в таблицу подробной информации о трафике будет загружена информация о трафике за указанный интервал времени.

Подробная информация о трафике.

Таблица «Подробная информация о трафике» содержит следующую информацию, см. таблицу 32.

Таблица 32 - Поля таблицы «Подробная информация о трафике»

Поле таблицы	Описание
Раздел	Раздел, к которому относятся значения последующих полей.
Тип информации	Элементы, относительно которых представлена информация о трафике. В зависимости от раздела это могут быть IP-адреса отправителей и получателей, порты отправителей и получателей для протоколов TCP и UDP, протоколы, флаги TCP и интерфейсы.
Байт всего	Общее количество трафика в байтах для данного элемента.

Поле таблицы	Описание
Пакетов всего	Общее количество трафика в пакетах для данного элемента.
Среднее число байт в пакете	Среднее число байт в пакете для данного элемента, вычисленное по формуле Байт всего / Пакетов всего.
Бит в секунду	Средняя скорость трафика в bps.
Пакетов в секунду	Средняя скорость трафика в pps.
%	Количество трафика в процентах, приходящееся на данный элемент, от общего количества трафика аномалии.
Фильтровать	Фильтровать трафик данного элемента при подавлении атаки. При открытии экрана первые 10 элементов в каждом разделе автоматически помечены для фильтрации.

В случае интенсивной аномалии количество строк в этой таблице может быть значительным. Чтобы облегчить анализ трафика и выделить только основные элементы, на которые приходится основной объем трафика, следует воспользоваться фильтром, находящимся справа вверху от таблицы. С помощью него можно задать минимальный порог трафика для элементов. Все элементы, трафик которых меньше порога, по нажатию на кнопку «Обновить» будут скрыты.

При открытии экрана в таблице содержатся только элементы, трафик которых больше 1% от общего объема.

3.4.6.7 Комментарии

Раздел «Комментарии» позволяет вводить и сохранять комментарии для аномалии.

Для добавления комментария выполните следующие действия:

- введите текст комментария;
- если для аномалии подходит стандартная аннотация, выберите ее из списка «Стандартная аннотация»;

- дополнительно можно выбрать ситуацию, чтобы уточнить обстоятельства: «Позвонил клиент», «Критическая атака» или «Атака обострилась».

3.4.7 Подавление аномалий

3.4.7.1 Введение

После того, как Анализатор детектировал аномалию, являющуюся атакой, можно анализировать данные о ней и выбирать действия для подавления.

3.4.7.2 Выбор способа подавления атаки из детального отчета

Для выбора способа подавления аномалии выполните следующие действия:

1) перейти на страницу «Детальный отчет» о DoS-аномалии;

2) нажмите «Подавить».

Появится список способов подавления атаки. Анализатор предлагает следующие действия:

- подавление с помощью Очистителя;
- blackhole-маршрутизация;
- flow specification;
- скрипт;
- сгенерировать фильтр;
- фингерпринт.

3.4.7.3 Подавление аномалий с помощью Blackhole

Этот способ подавления аномалий позволяет с помощью роутеров перенаправить трафик «в никуда». Чтобы подавить аномалию с помощью BlackHole выполните следующие действия:

1) Перейдите на страницу «Детальный отчет» для DoS-аномалий.

2) Нажмите «Подавить».

3) В поле желаемое действие выберите «Blackhole» и нажмите «Подавить». Откроется окно создания blackhole задания.

4) Закончите настройку задания.

3.4.7.4 Подавление аномалий с помощью Flow specification

Этот способ подавления аномалий позволяет создавать фильтры на основе параметров трафика. Чтобы подавить аномалию с помощью Flow specification выполните следующие действия:

1) Перейдите на страницу «Детальный отчет» для DoS-аномалий.

2) Нажмите «Подавить».

3) В поле желаемое действие выберите «Flow specification» и нажмите «Подавить». Откроется окно создания фильтра Flow specification.

4) Закончите настройку задания.

3.4.7.5 Подавление атак с помощью фильтра

Анализатор позволяет автоматически сгенерировать ACL-фильтр для роутера.

3.4.7.6 Создание фингерпринта на основе аномалии

Анализатор позволяет создать фингерпринт для отслеживания трафика, указанного в аномалии. Для фингерпринта можно задать пороговые значения и в дальнейшем Анализатор будет детектировать аномалии для этого трафика. Преимущества фингерпринта в том, что он может быть передан другим Анализаторам. Для создания фингерпринта выполните следующие действия:

1) Перейдите на страницу «Детальный отчет» для DoS-аномалий.

2) Нажмите «Подавить».

3) В поле желаемое действие выберите «Фингерпринт» и нажмите «Подавить». Откроется окно создания фингерпринта.

4) Закончите настройку фингерпринта.

3.4.8 Поиск аномалий

3.4.8.1 Введение

Используйте экран «Поиск» (Аномалии → Поиск) для поиска аномалий по IP-адресам, наблюдаемым объектам и объектам инфраструктуры.

3.4.8.2 Экран «Поиск»

Поиск полезно использовать для проверки, причастен ли какой-либо IP-адрес или наблюдаемый объект к каким-либо аномалиям или нет. Поиск можно выполнять по следующим критериям:

- IP-адреса;
- наблюдаемые объекты;
- объекты инфраструктуры.

Замечание: для IP-адресов можно искать префиксы, более специфичные, нежели введенный, либо – менее.

Замечание: также можно ограничить поиск списком текущих аномалий или аномалий, которые уже закончились.

Для того чтобы осуществить поиск по аномалиям, выполните следующие действия:

1) Перейдите на экран «Поиск» (Аномалии → Поиск).
2) Выберите объект поиска (IP-адрес, наблюдаемый объект, объект инфраструктуры).
3) В строку поиска введите критерий поиска, например, диапазон IP-адресов или часть названия наблюдаемого объекта.
4) Для диапазона IP-адресов выберите специфичность диапазонов IP-аномалии: более специфичные, чем введенные, менее специфичные, или точное совпадение.
5) Выберите состояние аномалии: текущие, прошедшие или и те, и другие.

6) Нажмите «Найти».

Появится список аномалий, удовлетворяющий введенным критериям.

3.4.9 Использование аннотаций для аномалий

3.4.9.1 Введение

Аннотации – это заранее определенные шаблоны комментариев для использования оператором при работе с DoS-аномалиями. Аннотации позволяют ускорить и упростить работу, уменьшить количество ошибок, стандартизировать комментарии.

3.4.9.2 Примеры аннотаций

Далее приведены примеры аннотаций:

- обсуждение с клиентом деталей аномалии;
- усиление активности аномалии;
- запуск задания подавления атаки.

3.4.9.3 Создание шаблона аннотации

Для создания текстового шаблона аннотации выполните следующие действия:

1) Перейдите на экран «Аннотации для аномалий» (Администрирование → Детекция → Аннотации для аномалий).
2) Нажмите «Добавить аннотацию».
3) Заполните поля.
4) Нажмите «Сохранить».

3.4.9.4 Удаление шаблона аннотации

Для удаления шаблона аннотации выполните следующие действия:

1) Отметьте флажками аннотации, которые нужно удалить.
2) Нажмите «Удалить выбранные».

3.4.10 Создание, редактирование и удаление групп уведомлений

3.4.10.1 Введение

Группы уведомлений используются для логического объединения адресов электронной почты, на которые производится рассылка уведомлений Системы о различных событиях, таких как DoS-аномалии, аномалии мониторинга Системы, BGP-ловушки.

Можно назначить группу уведомлений по умолчанию для получения всех событий или создать группу для получения, например, DoS-аномалий, идущих на выбранный объект или CIDR-блок.

3.4.10.2 Экран «Группы уведомлений»

Экран «Группы» (Администрирование → Уведомления → Группы) позволяет управлять группами уведомлений, которые Анализатор использует для отправки уведомлений.

Экран содержит таблицу со следующей информацией, см. таблицу 33.

Таблица 33 – Экран «Группы уведомлений»

Колонка	Описание
☑	Служит для выделения группы.
Наименование	Наименование группы уведомлений.
Описание	Описание группы уведомлений.
E-mail адреса	E-mail адреса группы уведомлений.

3.4.10.3 Создание и редактирование групп уведомлений

Для создания или редактирования группы уведомлений выполните следующие действия:

1) Перейдите на экран «Группы» (Администрирование → Уведомления → Группы).
2) Выполните одно из следующих действий:

– нажмите «Создать новую группу»;

– кликните на название существующей группы.

3) В открывшемся экране редактирования группы заполните необходимые поля.
4) Нажмите «Сохранить».

Замечание: почтовые уведомления могут быть высланы в следующих форматах:

- текст;
- XML;
- Excel XML;
- HTML;
- PDF;
- CSV.

Для получения уведомлений в нужном формате, необходимо ввести e-mail адреса в соответствующее поле экрана редактирования группы.

3.4.10.4 Удаление групп уведомлений

Для удаления группы уведомлений выполните следующие действия:

1) Перейдите на экран «Группы» (Администрирование → Уведомления → Группы).
2) Поставьте флажки для групп, которые нужно удалить.
3) Нажмите «Удалить выбранные».

Замечание: перед удалением группы необходимо удалить ассоциированные с ней правила. При удалении группы Анализатор не удаляет связанные с ней правила автоматически.

3.4.11 Создание, редактирование и удаление правил уведомлений

3.4.11.1 Введение

Анализатор позволяет настроить следующие почтовые уведомления:

- для аномалий, связанных с заданными CIDR-блоками и наблюдаемыми объектами, с помощью экрана «Правила» (Администрирование → Уведомления → Правила);

- при срабатывании BGP-ловушек, с помощью экрана «Ловушки» (Администрирование → Детекция → BGP → Ловушки);
- для аномалий мониторинга Системы, с помощью экрана «Аномалии мониторинга Системы».

3.4.11.2 Экран «Правила»

Экран Правила (Администрирование → Уведомления → Правила) позволяет сконфигурировать правила уведомлений для CIDR-блоков и наблюдаемых объектов.

Экран содержит таблицу со следующей информацией, см. таблицу 34.

Таблица 34 – Экран «Правила»

Колонка	Описание
☑	Служит для выделения правила
Название	Название правила
Ресурс	Ресурс, ассоциированный с правилом
Важность	Уровень важности аномалии, для которой должно быть послано уведомление. Уведомление посылается для указанного уровня и более высоких уровней.
Группа уведомлений	Группа уведомлений, список e-mail адресов на которые будет производиться рассылка.

3.4.11.3 Соответствие CIDR-блоков правил источникам аномалий

Когда Анализатор находит соответствие аномалии определенному правилу уведомлений, он отправляет сообщение адресатам, заданным в правиле. Аномалии, касающиеся большего адресного пространства (в которое входят CIDR-блоки, заданные в правиле) не приведут к генерации уведомлений.

Пример:

Если Анализатор детектирует DoS-аномалию, идущую на CIDR-блок 192.168.10.100/32 и в Системе создано правило с CIDR-блоком 192.168.0.0/16, то Анализатор отправит уведомление адресатам, заданным в правиле.

3.4.11.4 Создание и редактирование правил уведомлений

Для добавления или редактирования правила уведомлений выполните следующие действия:

1) Перейдите на экран «Правила» (Администрирование → Уведомления → Правила).
2) Выполните одно из следующих действий:
   - нажмите «Создать новое правило»;
   - кликните на ссылку с названием существующего правила.
3) Введите название правила в поле «Название правила».
4) В поле «Ресурс» укажите CIDR-блок и/или выберите из раскрывающегося списка наблюдаемый объект, сконфигурированный в Системе.
5) Выберите группу уведомлений.
6) Выберите уровень важности.
7) Нажмите «Сохранить».

3.4.11.5 Удаление правил уведомлений

Для удаления правила уведомления необходимо сделать следующее:

1) Перейдите на экран «Правила» (Администрирование → Уведомления → Правила).
2) Поставьте флажки для правил, которые нужно удалить.
3) Нажмите «Удалить выбранные».

3.4.11.6 Уведомления о срабатывании BGP-ловушек

Для получения почтовых уведомлений в случае, когда Анализатор детектировал срабатывание BGP-ловушки, используйте экран «Ловушки» (Администрирование → Детекция → BGP → Ловушки), укажите группу в настройках ловушки.

3.4.11.7 Уведомления мониторинга Системы

Для получения почтовых уведомлений об аномалиях мониторинга Системы используйте экран «Аномалии мониторинга Системы» (Администрирование → Уведомления → Аномалии мониторинга системы). Для настройки выполните следующие действия:

1) Перейдите на экран «Аномалии мониторинга системы» (Администрирование → Уведомления → Аномалии мониторинга системы).
2) Установите флажки для тех аномалий, для которых необходимо получать почтовые уведомления.
3) Нажмите «Сохранить».

Рассылка уведомлений об аномалиях данного типа производится группе по умолчанию.

Замечание: убедитесь, что соответствующие детекторы для мониторинга Системы включены и настроены правильно.

3.5 Детектирование атак с помощью фингерпринтов

3.5.1 Работа с фингерпринтами

3.5.1.1 Введение

Фингерпринты позволяют видеть потенциальные угрозы, полученные на основе опыта других организаций, благодаря чему можно предотвратить возникновение этих угроз в контролируемой сети.

3.5.1.2 Об экране «Фингерпринты»

Экран «Фингерпринты» (Аномалии → Фингерпринты) используется для создания, редактирования, экспорта и удаления фингерпринтов, а также перечисляет все фингерпринты, с которыми можно работать (принимать/активировать, запускать, останавливать, отклонять).

Это позволяет быть в курсе событий, происходящих с выбранными адресами, портами, протоколами, роутерами, интерфейсами, TCP-флагами, и ICMP-типами и кодами.

Можно создавать фингерпринты следующими способами:

- вручную, с использованием мастера фингерпринтов;
- на основе аномалий;
- загружать фингерпринты, предоставленные другими организациями.

Экран «Фингерпринты» отображает следующую информацию, см. таблицу 35.

Таблица 35 – Экран «Фингерпринты»

Колонка	**Описание**
ID/UUID	Внутренний идентификатор фингерпринта (ID) или уникальный идентификатор фингерпринта (UUID). Для переключения режимов нажмите «Показать ID» (если сейчас видны UUID) «Показать UUID» (если сейчас видны ID).
Статус	Статус фингерпринта - ПОЛУЧЕН, СОЗДАН, АКТИВЕН, ОТКЛОНЕН, УДАЛЕН. Если выбран один из фильтров «Статус», колонка может отсутствовать.
Название	Название фингерпринта
Определение	Определение фингерпринт
Время изменения	Время последнего изменения фингерпринта – момент, когда с ним производились какие-либо действия вручную или автоматически.
Источник	Источник фингерпринта. Если фингерпринт создан пользователем, источник локальный, если импортирован – устройство, с которого пришел фингерпринт. Для редактирования списка устройств перейдите к экрану "Администрирование → Подавление атак → Обмен фингерпринтами → Устройства".

Колонка	Описание
Активность	Время последних запуска и остановки фингерпринта, либо время запуска и сообщение о том, что фингерпринт идет в данный момент. Если фингерпринт еще не запускался, поля остаются пустыми. Если фингерпринт запущен в данный момент, содержит сообщение "Идет в данный момент" и время запуска.
Действия	Серия кнопок, отображающих действия по изменению статуса фингерпринта.
☐	Отметка для групповых операций.

3.5.1.2.1 Возможные изменения статуса фингерпринта

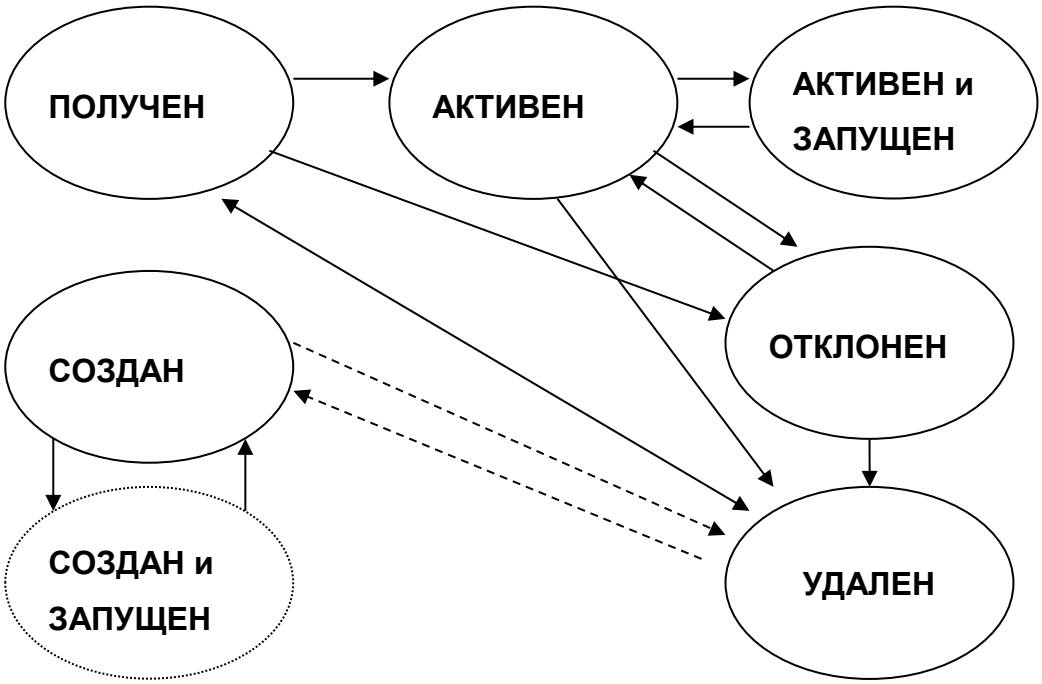


Рисунок 7 – Схема возможных изменений статуса фингерпринта

Существует четкое разграничение фингерпринтов по происхождению.

Если фингерпринт локальный, он находится в состоянии СОЗДАН и может быть запущен или удален. После восстановления он снова возвращается в состояние СОЗДАН.

Если фингерпринт получен с другой Системы, он находится в состоянии ПОЛУЧЕН и может быть принят, отклонен или удален. После восстановления он снова возвращается в состояние ПОЛУЧЕН.

Полный список переходов указан в таблице 36.

Таблица 36 – Таблица переходов статуса фингерпринта

Исходное состояние	**Действие**	**Результирующее состояние**
ПОЛУЧЕН	 Активировать	АКТИВЕН
	 Отклонить	ОТКЛОНЕН
	 Удалить	УДАЛЕН
АКТИВЕН	 Запустить	АКТИВЕН, ЗАПУЩЕН
	 Отклонить	ОТКЛОНЕН
	 Удалить	УДАЛЕН
АКТИВЕН, ЗАПУЩЕН	 Остановить	АКТИВЕН
ОТКЛОНЕН	 Активировать	АКТИВЕН
	 Удалить	УДАЛЕН
СОЗДАН	 Запустить	СОЗДАН, ЗАПУЩЕН
	 Удалить	УДАЛЕН
СОЗДАН, ЗАПУЩЕН	 Остановить	СОЗДАН
УДАЛЕН (внешний)	 Восстановить	ПОЛУЧЕН
УДАЛЕН (локальный)	 Восстановить	СОЗДАН

Внешний фингерпринт от локального отличается наличием у внешнего фингерпринта источника.

Запущенный фингерпринт не может быть удален, поэтому перед удалением фингерпринт необходимо остановить или дождаться окончания его работы.

3.5.1.2.2 Групповые операции над фингерпринтами

Для того чтобы сменить состояние нескольких фингерпринтов сразу, отметьте фингерпринты, состояние которых собираетесь менять, затем используйте серию кнопок "Групповые операции над фингерпринтами". Кнопки расположены под таблицей. Кнопки всегда показывают только групповые операции, доступные хотя бы для одного фингерпринта в таблице. Правила изменения состояния при групповых операциях – те же, что и для одиночных фингерпринтов. Перед изменением состояния будет выведено предупреждение со списком фингерпринтов, состояние которых можно изменить, либо разъяснение, почему невозможно это сделать.

Например, для остановки всех фингерпринтов можно выбрать всю таблицу, установив флажок в заголовке последнего столбца и нажать «Остановить отмеченные». При этом будет выведено предупреждение со списком названий фингерпринтов, которые действительно можно остановить и после подтверждения действия они будут остановлены.

3.5.1.2.3 Фильтрация списка фингерпринтов

Над списком фингерпринтов имеются два независимых фильтра, представляющих собой две строки со ссылками на состояние и числом фингерпринтов в этом состоянии. Если в каком-то состоянии фингерпринтов нет, ссылка отсутствует. Активный фильтр выделен красным шрифтом.

Для просмотра фингерпринтов в одном выбранном состоянии (полученные, созданные, принятые, отклоненные или удаленные), кликните на ссылку с данным состоянием.

Для просмотра только запущенных фингерпринтов, кликните на «Запущенные». Для того чтобы увидеть только остановленные фингерпринты, кликните на «Остановленные». При этом фильтр по состоянию остается актуальным.

Для того чтобы отключить фильтр по состоянию, кликните на ссылку «Все» строки с заголовком «Статус».

Для того чтобы отключить фильтр по запущенным/остановленным фингерпринтам, кликните на ссылку «Все» строки с заголовком «Состояние».

При открытии экрана в списке оба фильтра отключены и показываются все фингерпринты во всех состояниях.

3.5.1.3 О создании фингерпринта по результатам аномалии

Фингерпринт может быть создан на основе определения фингерпринт выражения или на основе существующей аномалии. Если фингерпринт основан на аномалии, основная часть создания практически завершена.

3.5.1.4 Создание и редактирование фингерпринта

Выполните одно из следующих действий:

- кликните по названию или номеру (ID/UUID) фингерпринта в списке;
- нажмите «Создать фингерпринт»;
- введите ID или UUID фингерпринта в поле «Перейти по ID/UUID»;
- нажмите «Перейти».

Примечание: редактировать можно только созданные и не запущенные фингерпринты. Фингерпринты полученные извне и фингерпринты в запущенном состоянии можно только просматривать. У активных, но не запущенных фингерпринтов можно изменять только желаемое время работы.

3.5.1.4.1 Заполнение редактируемых свойств фингерпринта

Выполните следующие действия:

1) Введите название фингерпринта в поле «Название». Название не должно содержать кавычек, угловых скобок и спецсимволов.
2) Для выделения типов трафика, которые включает в себя фингерпринт, выполните одно из следующих действий:

- введите определение фингерпринта в поле «Определение»;
- нажмите «Использовать мастер фингерпринтов» для создания фингерпринта по выражению фингерпринт. Созданное выражение будет добавлено к существующему (к имеющемуся в поле «Определение») через условие AND.

3) Чтобы разрешить экспорт, установите флажок «Экспортировать на другие Анализаторы».

4) Введите или выберите из списка номер аномалии в поле «Аномалия, по которой создан данный фингерпринт». Для этого выполните одно из следующих действий.

   - Чтобы увидеть краткий список свойств выбранной аномалии – ID, время начала, время окончания, тип аномалии и краткую информацию, нажмите «Обновить таблицу».
   - Нажмите на кнопку «Выбрать аномалию из списка», чтобы увидеть список 100 последних аномалий, отсортированный по времени. Если какая-то аномалия уже была выбрана, она будет присутствовать в списке, даже если она не входит в число 100 последних. Выбранная аномалия будет подсвечена красным цветом в списке аномалий.
   - Нажмите на кнопку «Свойства выбранной аномалии», чтобы увидеть подробную информацию об аномалии. Если подробная информация отсутствует, будет выдано предупреждение. Если ID аномалии в списке показано в виде ссылки, кликните на эту ссылку, чтобы увидеть подробную информацию об аномалии. Информация будет показана в новом окне.
   - Оставьте поле пустым, если фингерпринт не связан ни с какой аномалией.

5) Введите пороговые значения, при превышении которых будет сгенерирована аномалия. Для этого выполните следующие действия:

- введите порог срабатывания в битах в секунду в поле «Порог срабатывания, бит в секунду», выберите множитель для введенного числа (bps, Kbps, Mbps, Gbps);
- введите порог срабатывания в пакетах в секунду в поле «Порог срабатывания, бит в секунду», выберите множитель для введенного числа (pps, Kpps, Mpps, Gpps).

6) Введите пороговые значения, относительно которых будет оцениваться опасность аномалии. Для этого выполните следующие действия:
   - введите порог опасности в битах в секунду в поле «Порог опасности, бит в секунду», выберите множитель для введенного числа (bps, Kbps, Mbps, Gbps);
   - введите порог опасности в пакетах в секунду в поле «Порог опасности, пакетов в секунду», выберите множитель для введенного числа (pps, Kpps, Mpps, Gpps).
7) Введите время, по истечении которого запущенный фингерпринт будет автоматически остановлен, в поле «Желаемое время работы фингерпринта». Затем выберите единицу измерения интервала времени (часы или минуты). Если время задано, то единица измерения времени – обязательный параметр.

Примечания:

- Обязательными для ввода свойствами фингерпринта являются «Название» и «Определение».
- Поле «Желаемое время работы фингерпринта» можно оставить пустым. В этом случае время работы будет считаться бесконечным и фингерпринт можно будет остановить только вручную.
- Для всех пороговых значений:
  - значение может быть указано числом и множителем;

- значимыми являются первые 12 цифр числа;
- если задан порог срабатывания в bps, то обязательно должен быть задан порог опасности в bps;
- если задан порог срабатывания в pps, то обязательно должен быть задан порог опасности в pps;
- оставьте поле пустым или введите ноль для отключения порога.

3.5.1.4.2 Нередактируемые свойства фингерпринта

Кроме редактируемых свойств, на экране свойств фингерпринта имеются свойства, которые можно только посмотреть:

- ID: внутренний номер фингерпринта на Анализаторе (присваивается фингерпринту при создании или при получении от другой Системы).
- UUID: уникальный номер фингерпринта (присваивается фингерпринту при создании и никогда не изменяется, у одного и того же фингерпринта одинаков для всех Анализаторов).
- Статус: текущее состояние фингерпринта, может быть изменен в списке фингерпринтов. Импортированные фингерпринты в момент создания имеют статус ПОЛУЧЕН, созданные на текущем Анализаторе – статус СОЗДАН.
- Источник: происхождение фингерпринта: "локальный", если создан на текущем Анализаторе, и имя Анализатора, если создан на другом Анализаторе.
- Активность: момент последнего запуска и остановки.

3.5.1.4.3 Сохранение изменений

Нажмите «Сохранить» для сохранения сделанных изменений. В случае если ошибки не обнаружено, фингерпринт будет создан (если он создавался) или изменен (если он редактировался) и произойдет возврат к списку фингерпринтов. При

обнаружении каких-либо ошибок или несоответствий, редактирование будет продолжено, а список обнаруженных ошибок будет выведен на экран.

Нажмите кнопку «Отмена» для возврата в вписок фингерпринтов. Никаких изменений внесено не будет.

3.5.1.5 Удаление фингерпринта

Для удаления фингерпринта выполните следующие действия:

1) Перейдите на экран «Фингерпринты» (Аномалии → Фингерпринты).
2) Отметьте фингерпринты, которые необходимо удалить, галочками в правой части таблицы.
3) Нажмите «Удалить отмеченные».
4) Нажмите «ОК» для подтверждения удаления.

Примечания:

- Запущенные фингерпринты удалять нельзя. Перед удалением их необходимо остановить или дождаться завершения их работы.
- Для просмотра списка удаленных фингерпринтов выберите фильтр «Удаленные».

3.5.1.6 Запуск фингерпринта

Для запуска одного или нескольких фингерпринтов выполните следующие действия:

1) Перейдите на экран «Фингерпринты» (Аномалии → Фингерпринты).
2) Отметьте фингерпринты, которые необходимо запустить, галочками в правой части таблицы.
3) Нажмите «Запустить отмеченные».
4) Нажмите «ОК» для подтверждения запуска.

Для запуска одного фингерпринта выполните следующие действия:

1) Нажмите  у запускаемого фингерпринта.

2) Нажмите «ОК» для подтверждения запуска.

Примечания:

- Можно запускать только фингерпринты в состоянии СОЗДАН или АКТИВЕН.
- Для просмотра списка запущенных фингерпринтов выберите фильтр "Запущенные".

3.5.1.7 Остановка фингерпринта

Для остановки одного или нескольких фингерпринтов выполните следующие действия:

1) Перейдите на экран «Фингерпринты» (Аномалии → Фингерпринты).

2) Отметьте фингерпринты, которые необходимо остановить, галочками в правой части таблицы.

3) Нажмите «Остановить отмеченные».

4) Нажмите «ОК» для подтверждения остановки.

Для остановки одного фингерпринта выполните следующие действия:

5) Нажмите  у останавливаемого фингерпринта.

6) Нажмите «ОК» для подтверждения остановки.

Примечания:

- Можно остановить только запущенные фингерпринты.
- Для просмотра списка остановленных фингерпринтов выберите фильтр "Остановленные".

3.5.1.8 Активация фингерпринта

Для активации одного или нескольких фингерпринтов выполните следующие действия:

1) Перейдите на экран «Фингерпринты» (Аномалии → Фингерпринты).
2) Отметьте фингерпринты, которые необходимо активировать, галочками в правой части таблицы.
3) Нажмите «Активировать отмеченные».
4) Нажмите «ОК» для подтверждения активации.

Для активации одного фингерпринта выполните следующие действия:

1) Нажмите  у активируемого фингерпринта.
2) Нажмите «ОК» для подтверждения активации.

Примечание: можно активировать только импортированные фингерпринты (фингерпринты в состоянии ПОЛУЧЕН или ОТКЛОНЕН).

3.5.1.9 Отклонение фингерпринта

Для отклонения одного или нескольких фингерпринтов выполните следующие действия:

1) Перейдите на экран «Фингерпринты» (Аномалии → Фингерпринты).
2) Отметьте фингерпринты, которые необходимо отклонить, галочками в правой части таблицы.
3) Нажмите «Отклонить отмеченные».
4) Нажмите «ОК» для подтверждения отклонения.

Для отклонения одного фингерпринта выполните следующие действия:

1) Нажмите  у отклоняемого фингерпринта.
2) Нажмите «ОК» для подтверждения отклонения.

Примечание:

- Можно отклонить только импортированные фингерпринты (фингерпринты в состоянии ПОЛУЧЕН).
- Для просмотра списка отклоненных фингерпринтов выберите фильтр «Отклоненные».

3.5.1.10 Восстановление удаленного фингерпринта

Для восстановления одного или нескольких фингерпринтов выполните следующие действия:

1) Перейдите на экран «Фингерпринты» (Аномалии → Фингерпринты).
2) Отметьте фингерпринты, которые необходимо восстановить, галочками в правой части таблицы.
3) Нажмите «Восстановить отмеченные».
4) Нажмите «ОК» для подтверждения восстановления.

Для восстановления одного фингерпринта выполните следующие действия:

1) Нажмите  у восстанавливаемого фингерпринта.
2) Нажмите «ОК» для подтверждения восстановления.

Примечания:

- Можно восстановить только удаленные фингерпринты (фингерпринты в состоянии УДАЛЕН).
- Локальный фингерпринт восстанавливается в состоянии СОЗДАН, импортированный – в состоянии ПОЛУЧЕН.

3.5.2 Устройства для обмена фингерпринтами

3.5.2.1 Об экране «Устройства»

Экран «Устройства» (Администрирование → Подавление атак → Обмен фингерпринтами → Устройства) перечисляет все устройства (Анализаторы,

отличные от текущего), с которых могут быть импортированы фингерпринты, а также позволяет добавить новое устройство, отредактировать информацию о существующих или удалить существующие устройства.

Экран «Устройства» отображает информацию, представленную в таблице 37:

Таблица 37 – Таблица «Устройства»

Колонка	Описание
Наименование хоста	Наименование стороннего Анализатора.
Описание	Описание стороннего Анализатора.
IP	IP-адрес стороннего Анализатора.
Импорт разрешен	Могут ли с устройства поступать фингерпринты.
Время синхронизации	Время последней связи с устройством.

3.5.2.2 Фильтрация списка устройств

На экране имеется фильтр, позволяющий найти устройство или группу устройств по совпадению в наименовании, описании или IP-адресе. Для фильтрации списка выполните следующие действия:

1) Выберите область поиска в выпадающем списке «Поиск».
2) Введите один из следующих критериев поиска в зависимости от области:
   - название или часть названия для поиска по названию устройства;
   - описание или часть описания для поиска по описанию устройства;
   - точный IP-адрес для поиска по IP-адресу устройства.
3) Нажмите «Найти».

Для отмены фильтрации оставьте поле пустым.

3.5.2.3 Добавление и редактирование устройства

Для добавления устройства нажмите «Добавить устройство».

Для редактирования устройства кликните по названию устройства в списке.

Заполните следующие параметры устройства на экране для редактирования устройства:

1) Введите название устройства в поле «Название».
2) Введите описание устройства в поле «Описание».
3) Введите IP устройства в поле «IP».
4) Введите или скопируйте из места хранения ключа закрытый ключ пользователя в поле «Закрытый ключ пользователя».
5) Введите или скопируйте из места хранения ключа открытый ключ устройства в поле «Открытый ключ хоста».
6) Выберите, разрешен ли импорт фингерпринтов с редактируемого/добавляемого устройства, в списке «Импорт разрешен».
7) Нажмите «Сохранить» для сохранения введенной информации.

Примечания:

- Если один из параметров введен неправильно, сообщение об этом появится около неправильно введенного поля.
- Для возвращения к списку устройств без сохранения информации, нажмите «Отмена».

3.5.2.4 Удаление устройства

Для удаления одного или нескольких устройств выполните одно из следующих действий:

- отметьте удаляемые устройства в списке устройств слева от имени;
- нажмите «Удалить выбранные»;
- нажмите «ОК» или «Да» для подтверждения удаления.

Примечание: фингерпринты, импортированные с удаленного устройства, становятся локальными.

3.6 Подавление атак с помощью Flow Specification

3.6.1 Введение

Метод подавление атак Flow Specification – это фильтрация трафика с помощью средств роутеров. Фильтры трафика создаются Анализатором и рассылаются посредством BGP-протокола роутерам сети. Можно использовать Flow Specification, чтобы создать брандмауэр или для управления доступом к ресурсам внутри сети. Фильтр позволяет описать следующее:

- диапазоны IP-адресов получателя;
- диапазоны IP-адресов отправителей;
- протокол (UDP, ICMP, TCP);
- порты;
- ICMP-тип и код;
- TCP-флаги;
- DSCP-флаг;
- флаг фрагментации.

Можно комбинировать разные фильтры в одном задании подавления атаки и определить для задания действие роутера (пропустить, отбросить, шейпинг).

Метод работает только для роутеров с настроенными BGP параметрами.

3.6.2 Пример использования Flow specification

При возникновении аномалии, в которой говорится, что хост посылает большой поток UDP-пакетов на DNS-сервер, и после ее анализа определите параметры трафика: адрес источника-192.168.1.35/32, протокол UDP, порт отправителя 6667, адрес получателя 172.16.20.100/32, порт получателя 53.

Подавление атаки с помощью FlowSpec задания наиболее простой и эффективный способ подавить атаку данного вида. Для создания FlowSpec подавления атаки выполните следующие действия:

1) Находясь в «Детальном отчет» DoS-аномалии нажмите «Подавить».
2) В поле «Желаемое действие» выберите «Flow specification».
3) Нажмите «Подавить».

Откроется экран создания BGP FlowSpec задания подавления атаки. В поле названия подавления атаки будет указан идентификатор аномалии и ID оповещения.

1) Перейдите на вкладку «Анонс». На этой вкладке выберете роутеры и автономные системы, которым будет анонсировано данное задание:
   - выберите роутер или группу роутеров, которым нужно анонсировать задание;
   - введите сообщества, которым нужно анонсировать задание;
   - выберите параметры, ограничивающие действие фильтра.
2) Перейдите на вкладку «Фильтр».
3) Введите, полученную в результате анализа, информацию об аномалии.
   - в поле «Получатели» введите 172.16.20.100/32;
   - в поле «Отправители» введите 192.168.1.35/32;
   - в поле «Протоколы» введите 17;
   - в поле «Порты отправителей» введите 6667;
   - в поле «Порты получателей» введите 53;
   - остальные поля можно оставить пустыми.
4) Перейдите на вкладку «Действие».
5) В поле «Действие» выберите желаемое действие: отбросить, пропустить, шейпинг. Если выбран шейпинг, необходимо указать скорость ограничения трафика.
6) Нажмите «Создать».
7) Запустите созданное задание.

После запуска Анализатор анонсирует правила всем роутерам, с которыми установлено BGP соединение. Каждый роутер после получения анонса выполняет заданные действия с трафиком, соответствующим фильтру.

3.6.3 Управление BGP FlowSpec заданиями подавления атак

3.6.3.1 Экран BGP FlowSpec

На экране «BGP FlowSpec» (Подавление атак → BGP FlowSpec) отображаются все задания подавления атак этого типа. Экран позволяет создать, запустить, остановить или удалить задания.

Список заданий выводится в виде таблицы, поля таблицы описаны в таблице 38.

Таблица 38 – Список BGP FlowSpec

Поле таблицы	Описание
Название	Название задания подавления атаки. Ссылка на экран редактирования задания.
Описание	Описание задания подавления атаки.
Правило	Диапазоны IP, протоколы, порты, участвующие в задании.
Состояние	Отображает состояние задания (запускается, запущено, ошибка, останавливается, остановлено).

3.6.3.2 Создание и редактирование FlowSpec задания подавления атаки

Для добавления или редактирования FlowSpec задания подавления атаки выполните следующие действия:

1) Перейдите на экран «BGP FlowSpec» (Подавление атак →BGP FlowSpec).

2) Находясь на экране выполните одно из следующих действий:

   – для создания нового задания нажмите «Добавить»;

   – для редактирования задания кликните на название задания.

3) Заполните необходимые поля формы. Описание полей вкладок экрана смотрите далее.

3.6.3.3 Редактирование описания FlowSpec задания подавления атаки

1) Перейдите на вкладку «Описание».
2) Введите название задания в поле «Название».
3) Введите описание задания в поле «Описание».

3.6.3.4 Редактирование настроек анонсирования FlowSpec задания подавления атаки

1) Перейдите на вкладку «Анонс».
2) Нажмите «Выбрать роутеры» для выбора роутеров, к которым будет применено данное задание.
3) В поле «Сообщества» введите список BGP-сообществ, для которых будет анонсироваться маршрут.
4) При необходимости поставьте флажок напротив следующих предопределенных сообществ. Описание приведено в таблице 39.

Таблица 39 – Выбор сообществ

Сообщество	Описание
LOCAL_AS	Маршрут анонсируется только локальной автономной системе.
NO_ADVERTISE	Маршрут не должен объявляться другим BGP-узлам.
NO_EXPORT	Маршрут не должен быть объявлен за пределами AS.
NO_PEER	Маршрут не должен быть объявлен соседям eBGP.

3.6.3.5 Редактирование настроек фильтра FlowSpec задания подавления атаки

1) Перейдите на вкладку «Фильтр».
2) Введите диапазон IP-адресов получателей для фильтрации в поле «Получатели».

3) Введите диапазон IP-адресов отправителей для фильтрации в поле «Отправители».

4) Введите номера или диапазоны номеров протоколов (например, 6,17,8000-8080) для фильтрации в поле «Протоколы».

5) Введите номер порта или диапазон портов для фильтрации в поле «Порты» (например, 53,80, 24-30).

Замечание: используйте это поле для того, чтобы отфильтровать и порты отправителя, и порты получателя одновременно. Если нужно отфильтровать только одно направление, используйте поля «Порты отправителей» и «Порты получателей».

6) Введите номер порта или диапазон портов отправителя для фильтрации в поле «Порты отправителей» (например, 53,80, 24-30).

7) Введите номер порта или диапазон портов получателей для фильтрации в поле «Порты получателей» (например, 53,80, 24-30).

8) Введите номера или диапазоны номеров ICMP-типов (например, 2, 16-255) в поле «ICMP-типы».

9) Введите номера или диапазоны номеров ICMP-кодов (например, 2, 16-255) в поле «ICMP-коды».

10) Введите номер TCP-флагов для фильтрации (1=fin, 2=syn, 4=rst, 8=psh, 16=ack, 32=urg, 64=ece, and 128=cwr) в поле «TCP-флаги».

11) Введите размер или диапазон размеров пакета в поле «Размеры».

12) Введите номер или диапазон номеров DSCP для фильтрации в поле «DSCP».

13) Введите целое число от 0 до 3 для задания битовой маски в поле «Фрагментация». (0 – не фрагментирован, 1 – пакет является фрагментом, 2 – пакет является первым фрагментом, 2 – пакет является последним фрагментом).

3.6.3.6 Редактирование настроек действия FlowSpec задания подавления атаки

1) Перейдите на вкладку «Действие».
2) Выберите действие, которое будет выполнено над отфильтрованным трафиком. Список действий и описание приведено в таблице 40.

Таблица 40 – Действия при подавлении атаки

Задача	Дествия
Пропустить трафик, соответствующий фильтру	Выберите «пропустить» в поле выбора «Действие». **Замечание:** не блокирует трафик, но ведет статистику для данного вида трафика.
Блокировать трафик, соответствующий фильтру	Выберите «отбросить» в поле выбора «Действие».
Ограничить трафик	Выберите «шейпинг» в поле выбора действия.

3) Нажмите «Сохранить».

3.6.3.7 Запуск FlowSpec заданий подавления атаки

Для запуска FlowSpec задания подавления атаки выполните следующие действия:

1) Перейдите на экран «BGP FlowSpec» (Подавление атак → BGP FlowSpec).
2) Выберите флажками задания для запуска.
3) Нажмите «Запустить выбранные».

3.6.3.8 Остановка FlowSpec заданий подавления атаки

1) Перейдите на экран «BGP FlowSpec» (Подавление атак → BGP FlowSpec).
2) Выберите задания для остановки.
3) Нажмите «Остановить выбранные».

3.6.3.9 Удаление FlowSpec заданий подавления атаки

1) Перейдите на экран «BGP FlowSpec» (Подавление атак → BGP FlowSpec).

2) Выберите нужные задания для запуска.

3) Нажмите «Остановить выбранные».

3.6.4 Статус задания подавления атаки

3.6.4.1 Введение

Экран «Информация» (BGP FlowSpec → Информация) позволяет просмотреть информацию о статусе задания подавления атаки, просмотреть характеристики задания, а также добавить комментарий к заданию.

Экран содержит следующие секции:

- общая информация;
- детальная информация;
- комментарии.

3.6.4.2 Переход на экран статуса задания подавления атаки

Для перехода на страницу «Информация» (BGP FlowSpec → Информация) выполните следующие действия:

Способ 1:

1) Перейдите на экран «BGP FlowSpec» (Подавление атак → BGP FlowSpec).

2) Нажмите на кнопку «Статус» для нужного задания подавления атак.

Способ 2:

1) Перейдите на экран «Текущие» (Подавление атак → Текущие).

2) Посмотрите в колонку «Тип» и выберите задания типа BGP FlowSpec.

3) Кликните на название или ID нужного задания подавления атаки.

3.6.4.3 Описания секции «Общая информация»

Секция «Общая информация» содержит таблицу с базовой информацией о задании подавления атаки. Описание информации, содержащейся в этой секции см. таблицу 41.

Таблица 41 – Секция «Общая информация»

Параметр	Описание
Название задания	Название FlowSpec задания подавления атаки.
ID задания	Идентификатор задания.
Продолжительность задания	Продолжительность задания.
Время запуска задания	Время и дата, когда было запущено задание.
ID аномалии	Идентификатор аномалии, для которой было создано задание. Если задание не было создано на основе аномалии, то поле остается пустым.
Описание	Описание задания подавления атаки.
Сообщества	Список сообществ задания подавления атаки.

3.6.4.4 Секция «Детальная информация»

Секция «Детальная информация» содержит описание параметров фильтрации и действий задания подавления атаки. Информация, содержащаяся в этой секции, описана в таблице 42.

Таблица 42 – Детальная информация

Параметр	Описание
Получатели	Диапазоны IP-адресов получателей, заданные в фильтре задания подавления атаки.
Отправители	Диапазоны IP-адресов отправителей, заданные в фильтре задания подавления атаки.
Протоколы	Протоколы, заданные в фильтре задания подавления атаки.
Порты	Порты, заданные в фильтре задания подавления атаки.

Параметр	Описание
Порты отправителей	Порты отправителей, заданные в фильтре задания подавления атаки.
Порты получателей	Порты получателей, заданные в фильтре задания подавления атаки.
ICMP-типы	ICMP-типы, заданные в фильтре задания подавления атаки.
ICMP-коды	ICMP-коды, заданные в фильтре задания подавления атаки.
Размеры	Размеры пакета.
DSCP	Значение DSCP, заданные в фильтре задания подавления атаки.
TCP-флаги	TCP-флаги, заданные в фильтре задания подавления атаки.
Фрагментация	Параметры фрагментации, заданные в фильтре задания подавления атаки.
Действие	Действие, заданное в задание подавления атаки.

3.6.4.5 Добавление комментария

Для добавления комментария к заданию подавления атаки выполните следующие действия:

1) Если для задания подавления атаки подходит стандартная аннотация, то выберите ее в поле «Стандартная аннотация» и текст аннотации добавится в поле комментария.

2) В поле комментария введите текст комментария.

3) Выберите один или несколько причин комментария:

- позвонил клиент;
- критическая атака;
- атака обострилась.

4) Нажмите «Сохранить комментарий» и комментарий добавится к заданию подавления атаки.

3.7 Подавление атак с использованием скриптов

3.7.1 Введение

Анализатор позволяет запускать произвольные скрипты на удаленных хостах при возникновении аномалий.

3.7.1.1 Экран «Скрипты для отражения атак»

Экран «Скрипты для отражения атак» (Администрирование → Подавление атак → Скрипты для отражения атак) содержит список скриптов, которые могут быть вызваны в случае атаки. Этот экран позволяет редактировать, удалять и создавать скрипты. Описание полей списка скриптов приведено в таблице 43.

Таблица 43 – Скрипты отражения атак

Поле	Описание
Название	Название скрипта.
Команда	Команда для запуска скрипта.
Пользователь	Имя пользователя для доступа на удаленный хост.
Хост	Хост, на котором будет запущен скрипт.
Порт	Порт на удаленном хосте, для подключения.

3.7.1.2 Создание и редактирование скриптов

Для создания или редактирования скрипта выполните следующие действия:

1) Перейдите на экран «Скрипты для отражения атак» (Администрирование/Подавление атак/Скрипты для отражения атак).
2) Нажмите «Добавить скрипт» или кликните на название существующего скрипта в списке.
3) Введите название скрипта в поле «Название».

4) Введите команду запуска скрипта в поле «Команда».

5) Введите имя пользователя для доступа на удаленный хост в поле «Пользователь».

6) Введите адрес хоста, на котором нужно запустить скрипт в поле «Хост».

7) Введите порт для подключения скрипта в поле «Порт».

8) Введите закрытый ключ пользователя в поле «Закрытый ключ пользователя».

9) Введите открытый ключ хоста в поле «Открытый ключ хоста».

10) Нажмите «Сохранить».

3.7.1.3 Экран «Скрипты для отражения атак»

Экран «Скрипты для отражения атак» (Подавление атак → Скрипты для отражения атак) содержит список скриптов для отражения атак. Этот экран позволяет редактировать, удалять и создавать скрипты. Описание полей списка скриптов приведено в таблице 44.

Таблица 44 – Экран «Скрипты для отражения атак»

Поле	Описание
Название	Название задания отражения атаки.
Создатель	Пользователь, который создал задание подавления атаки.
Последний запуск	Дата и время последнего запуска задания.
Действие	Запустить/остановить скрипт.

3.7.1.4 Создание и редактирование заданий скриптов отражения атак

Для создания или редактирования задания скрипта отражения атак выполните следующие действия:

1) Перейдите на экран «Скрипты для отражения атак» (Подавление атак → Скрипты для отражения атак).

2) Нажмите «Добавить скрипт» или кликните на название существующего скрипта в списке.
3) Введите название скрипта в поле «Название».
4) Если скрипт создан на основе аномалии, то в поле ID аномалии будет записан ее номер.
5) Введите описание в поле «Описание».
6) Выберите скрипт. Для этого нажмите на стрелочку рядом с полем «Скрипт».
7) Поля «Скрипт», «Пользователь», «Хост» заполнятся автоматически после выбора скрипта.
8) Введите параметры запуска скрипта.
9) Чтобы запустить скрипт, нажмите «Запустить» или нажмите «Создать»/«Сохранить» для сохранения скрипта.

3.8 Подавление атак с помощью Blackhole-маршрутизации

3.8.1 Введение

Blackhole-маршрутизация перенаправляет поток трафика на другой NextHop.

Существуют два основных вида blackhole-маршрутизации:

- Null-маршрутизация – роутер отбрасывает весь трафик, идущий на заданный префикс.
- Offramp-маршрутизация – роутер перебрасывает на заданный хост весь трафик, идущий на заданный префикс.

Blackhole-маршрутизация позволяет эффективно бороться с DoS и DDoS-атаками.

3.8.2 Пример подавления атаки с помощью blackhole-маршрутизации

Blackhole-маршрутизация позволяет отбрасывать весь трафик, идущий через роутеры контролируемой сети и направленный на указанные префиксы. Обычно это требуется, когда количество трафика, входящее в сеть от атакующего, превосходит количество трафика, которое позволяет обработать сетевое оборудование

Пример: провайдер назначает клиенту CIDR-блок /24, а также /32 хост, на который проводится атака. Количество трафика от атакующего полностью забивает канал атакуемого клиента. В таком случае провайдер может подавить атаку с помощью blackhole-маршрутизации, отбрасывая весь трафик на атакуемый /32 хост непосредственно в момент его входа в контролируемую сеть. Это не позволит трафику с атакующего хоста доходить до сетевого оборудования клиента, в то время как остальной трафик будет доставлен нормально.

Замечание: blackhole-маршрутизация завершит DoS-атаку, но в то же время клиент не сможет предоставлять сервисы с атакуемого /32 хоста, пока задание подавления атаки не будет остановлено.

3.8.3 Экран со списком заданий подавления атак с помощью blackhole-маршрутизации («Blackhole-роутинг»)

3.8.3.1 Введение

Для доступа к экрану выберите в главном меню «Подавление атак» → «Blackhole-роутинг». Здесь отображаются все задания подавления атак с помощью blackhole-маршрутизации. На этом экране можно создавать новые задания, просматривать и удалять существующие, а также запускать неактивные задания и останавливать активные.

В таблице со списком заданий очистки представлена следующая информация, см. таблицу 45.

Таблица 45 – Поля таблицы на экране «Blackhole-роутинг»

Колонка	Описание
Название	Имя задания по подавлению атаки.
Создатель	Пользователь, создавший задание.
Blackhole	Префикс и nexthop задания.
Состояние	Состояние задания.

Замечание: на экране «Blackhole-роутинг» не отображаются задания очистки «BGP Flowspec», для них есть отдельный экран.

3.8.3.2 Создание / редактирование задания подавления атаки

Для создания нового задания подавления атаки либо редактирования существующего выполните следующие действия:

1) Перейдите на экран «Blackhole-роутинг» («Подавление атак» → «Black-hole роутинг»).
2) Выполните одно из следующих действий:
   - нажмите «Добавить», чтобы создать новое задание;
   - найдите задание в списке и кликните на соответствующей гиперссылке в колонке «Название» для редактирования.
3) Введите название задания в поле «Название».
4) Если необходимо, добавьте описание в поле «Описание».
5) Если задание подавления атаки автоматически создано из аномалии, в поле «ID аномалии» будет указан идентификатор аномалии.
6) В поле «Префикс» укажите CIDR-блок, трафик на который будет подвергнут очистке либо перенаправлению.
7) В поле «Действие» выберите один из типов blackhole-маршрутизации:
   - «Ответвление по умолчанию» – трафик будет перенаправлен на заранее определенный адрес, заданный на конфигурационном экране «Blackhole-роутинг» («Администрирование» → «Подавление атак» →

«Blackhole-роутинг») в поле «IP-адрес BGP-ответвления по умолчанию».

– «NULL-маршрутизация» – трафик будет формально отброшен, а фактически перенаправлен на заранее определенный адрес, заданный на конфигурационном экране «Blackhole-роутинг» («Администрирование» → «Подавление атак» → «Blackhole-роутинг») в поле «IP-адрес NULL-маршрутизации».

– «Другое» – трафик будет перенаправлен на устройство, заданное в поле NextHop.

8) Поле «Роутеры» назначает список роутеров, для которых определяется blackhole-маршрутизация. Список изменяется при помощи интерактивного окна, появляющегося при нажатии «Выбрать роутеры».

9) В поле «Сообщества» можно задать BGP-сообщества, для которых справедливо данное задание очистки. Ниже перечислены специальные сообщества:

– LOCAL_AS – роутер не должен сообщать данный маршрут любому eBGP-соседу, включая соседей в SubAS из той же самой BGP-конфедерации;

– NO_ADVERTISE – роутер не должен сообщать данный маршрут ни одному из своих соседей, какого бы типа они не были;

– NO_EXPORT – роутер не должен сообщать данный маршрут любому из своих внешних соседей по eBGP. Однако он может сообщать данный маршрут своим соседям по eBGP внутри BGP-конфедерации;

– NO_PEER - роутер не должен сообщать данный маршрут соседям eBGP.

10) Выбрав «Добавить сообщества», можно открыть интерактивное окно выбора заранее заданных BGP-сообществ.

11) В поле «Продолжительность» необходимо задать длительность задания очистки - время в минутах, на которое будет запущено данное задание.

12) Выберите «Создать» чтобы завершишь создание / редактирование задания очистки. Выбор пункта «Отмена» осуществит возврат на предыдущий экран без сохранения.

3.8.3.3 Удаления задания подавления атаки

Для удаления задания подавления атаки выполните следующие действия:

1) Перейдите на экран «Blackhole-роутинг» («Подавление атак» → «Blackhole-роутинг»).
2) Найдите задание в списке, отметьте его галочкой.
3) Нажмите «Удалить выбранные».

3.8.3.4 Запуск задания подавления атаки

Для запуска задания подавления атаки выполните следующие действия:

Метод 1.

1) Перейдите на экран «Blackhole-роутинг» («Подавление атак» → «Blackhole-роутинг»).
2) Найдите задание в списке, отметьте его галочкой в первой колонке таблицы.
3) Нажмите «Запустить выбранные».

Замечание: таким способом можно запустить сразу несколько заданий.

Метод 2.

1) Перейдите на экран «Blackhole-роутинг» («Подавление атак» → «Blackhole-роутинг»).
2) Найдите задание в списке, нажмите «Статус» во второй колонке таблицы.
3) На открывшемся экране статуса задания очистки нажмите «Запустить».

3.8.3.5 Остановка задания подавления атаки

Для остановки задания подавления атаки выполните следующие действия:

Метод 1.

1) Перейдите на экран «Blackhole-роутинг» («Подавление атак» → «Blackhole-роутинг»).
2) Найдите задание в списке, отметьте его галочкой в первой колонке таблицы.
3) Нажмите «Остановить выбранные».

Замечание: таким способом можно остановить сразу несколько заданий.

Метод 2.

1) Перейдите на экран «Blackhole-роутинг» («Подавление атак» → «Blackhole-роутинг»).
2) Найдите задание в списке, нажмите «Статус» во второй колонке таблицы.
3) На открывшемся экране статуса задания очистки нажмите «Остановить».

Метод 3.

1) Перейдите на экран активных заданий подавления атак «Текущие» («Подавление атак» → «Текущие»).
2) Найдите задание в списке по идентификатору либо имени, кликните на гиперссылку в поле «ID» или «Название».
3) На открывшемся экране статуса задания очистки нажмите «Остановить».

3.8.4 Экран статуса заданий подавления атаки с помощью blackhole-маршрутизации

3.8.4.1 Введение

Экран «Информация» позволяет просматривать статус заданий очистки трафика, а также добавлять к ним комментарии.

3.8.4.2 Доступ к экрану

Для доступа к экрану «Информация» выполните следующие шаги:

1) Перейдите на экран активных заданий подавления атак «Текущие» («Подавление атак» → «Текущие»), либо завершенных заданий «Прошедшие» («Подавление атак» → «Прошедшие»).

2) В колонке «Тип» таблицы будет указан тип задания. Задания очистки с использованием blackhole-маршрутизации имеют тип «Blackhole».

3) Для доступа к экрану статуса задания очистки кликните на гиперссылку в поле «ID» или «Название».

Для каждого задания подавления атаки отображается следующая информация, см. таблицу 46.

Таблица 46 – Поля таблицы на экране «Информация»

Колонка	Описание
Название	Имя задания по подавлению атаки.
ID задания	Идентификатор, присвоенный заданию.
Префикс	Префикс для очистки.
NextHop	Nexthop задания. Если используется null-маршрутизация, за ним будет указана пометка «NULL».
Время начала	Время запуска задания.
Состояние	Состояние задания.
Сообщества	Сообщества, назначенные при создании задания.
Описание	Комментарий к заданию.

3.8.4.3 Остановка задания подавления атаки

Для остановки задания подавления атаки выполните следующие действия:

1) Перейдите на экран активных заданий подавления атак «Текущие» («Подавление атак» → «Текущие»).

2) Найдите задание в списке по идентификатору либо имени, кликните на гиперссылку в поле «ID» или «Название».

3) На открывшемся экране статуса задания нажмите «Остановить».

3.8.4.4 Добавление комментария к заданию подавления атаки

Для добавления комментария к заданию подавления атаки выполните следующие действия:

1) Находясь на экране «Информация», заполните соответствующее поле текстом комментария.

2) Для ускорения ввода можно воспользоваться списком стандартных комментариев, выбрав необходимый в выпадающем списке «Стандартная аннотация».

3) Можно отметить один из трех флажков, отображающих причину добавления комментария: «Позвонил клиент», «Критическая атака», «Атака обострилась».

4) Нажмите «Сохранить комментарий».

3.8.5 Установка значений NextHop «по умолчанию» для blackhole-маршрутизации

3.8.5.1 Введение

При создании нового задания очистки с помощью blackhole-маршрутизации возможно указать как новый NextHop для перенаправления трафика, так и использовать заранее заданные значения для Offramp или NULL-маршрутизации. Эти значения задаются на экране настроек blackhole-маршрутизации («Администрирование» → «Подавление атак» → «Blackhole-роутинг»).

3.8.5.2 Установка значений NextHop «по умолчанию»

Для установки значений NextHop «по умолчанию» выполните следующие действия:

1) Перейдите на экран «Blackhole-роутинг» («Администрирование» → «Подавление атак» → «Blackhole-роутинг»).
2) В поле «IP-адрес BGP-ответвления по умолчанию» введите адрес, на который будет перенаправляться трафик при Offramp-маршрутизации.
3) В поле «IP-адрес NULL-маршрутизации» введите адрес, который будет использован для отбрасывания трафика (NULL-маршрутизации).
4) Выберите «Сохранить» для подтверждения введенных значений, либо «Отмена» для выхода с экрана.

3.9 Отражение атак с помощью ACL-фильтров

3.9.1 Введение

ACL обозначает Access Control List, то есть дословно «контроль доступа по списку». ACL-фильтры позволяют отражать DDoS-атаки (распределенные атаки отказа в обслуживании), некритично влияющие на функционирование контролируемой сети. ACL-фильтр позволяет указать роутеру какие пакеты следует фильтровать и дополнительно задать скорость потока для включения фильтрации.

3.9.2 Отражение атаки с помощью ACL-фильтра

Для отражения DoS-атаки с помощью ACL-фильтра, выполните следующие действия:

1) Перейдите на экран со списком DoS-аномалий «Текущие DoS-аномалии» («Аномалии» → «Текущие DoS-аномалии»).
2) Выберите атаку, которую необходимо отразить и перейдите на детальный отчет по ней, кликнув на колонку с идентификатором аномалии («ID»).

3) Выберите «Подавить».

4) В выпадающем списке выберите «Сгенерировать фильтр» и подтвердите выбор, выбрав «Подавить».

5) В открывшемся диалоге в разделе «Критерий фильтрации» указаны параметры фильтрации, которые будут использованы для создания фильтра.

6) В поле «Имя» можно изменить названия фильтра, сгенерированное Системой по умолчанию.

7) В выпадающем списке «Производитель» выберите тип роутера.

8) В поле «Ограничение полосы» можно задать лимит пропускной способности, при превышении которого будет работать фильтр. Если поле оставить пустым, фильтр будет работать постоянно.

9) Нажмите «Сформировать».

В открывшемся окне будет сгенерирован текст фильтра. Также будут указаны команды, с помощью которых можно применить данный фильтр на роутере.

3.10 Соседские отношения

3.10.1 Введение

В работе над повышением эффективности сети с точки зрения эффективности по передаче и транзиту трафика первостепенное значение играет детальная информация о взаимодействии с соседними сетями. В этой главе дается описание специального типа наблюдаемых объектов - соседей, а также рассказывается, как создавать объекты этого типа и следить за их трафиком.

3.10.2 Отчеты по соседям

Меню отчетов по соседям Отчеты → Соседи содержит отчеты по трафику и маршрутам для наблюдаемых объектов соседей. Эти отчеты позволяют увидеть соседский трафик, новых потенциальных соседей (в плане заключения соглашений

об обмене трафиком) и решить с кем следует поддерживать соседские отношения, а с кем отказаться от них. Следует помнить, что Система не располагает полной информацией о трафике соседских сетей, так как наблюдения производятся из контролируемой сети, а не из изучаемой сети. В связи с этим, известны данные только о том трафике соседей, который проходил через контролируемую сеть.

3.10.3 Отчет «Диаграмма AS»

Отчет «Диаграмма AS» (Отчеты → Утилиты → Соседи → Диаграмма AS) показывает в графическом формате самые значимые по объему трафика отношения с соседними сетями. Отчет изображает на диаграмме каждую AS как независимый объект с линиями, идущими на соседние AS в соответствии с объемом трафика. Используйте легенду к диаграмме для получения подробной информации во время работы.

Замечание: диаграмма AS показывает только самые значимые взаимосвязи между AS.

Диаграмма AS показывает диаграмму потоков трафика, направленного с и на локальные и внешние AS. Входящий и исходящий трафик на диаграмме указан относительно AS. Первая диаграмма после открытия экрана отображает вашу сеть в виде круга в центре, локальные AS вашей сети, через которые трафик идет с и на соседские AS отображены квадратиками на первой окружности вокруг круга. Соседские AS отображены на второй окружности. Для отображения трафика соседей кликните на соответствующий AS. При этом указанный AS будет перемещен в центр диаграммы, а две окружности вокруг будут представлять AS, с которыми он обменивается трафиком.

Объем трафика, передаваемого между AS отображается линиями соответствующей толщины и разного цвета. Весь объем трафика (входящий плюс исходящий), которым обменивается ваша сеть с внешним миром принимается за 100%, на первой диаграмме видно, как распределяется этот трафик по вашим локальным AS. Если у вас только один AS, тогда весь объем трафика во внешний мир идет через него.

Диаграмма показывает трафик между внешними AS только если он был получен (или был сгенерирован или транзитный) в вашей сети и не показывает никакой другой трафик между внешними AS, т.к. информация о нем не доступна из вашей сети.

Замечание: для удобства просмотра отчета цифровые значения AS могут отображаться как названия, для этого необходимо произвести соответствующую настройку.

3.10.4 Отчет «Оценка договоренностей с соседями»

3.10.4.1 Введение

Отчет «Оценка договоренностей с соседями» (Отчеты → Соседи → Утилиты → Оценка договоренностей с соседями) предоставляет сводку по трафику, которым контролируемая сеть обменивается со всеми AS в Интернете, в том числе сети, заданные как наблюдаемые объекты. Используйте этот отчет для проверки эффективности партнерских соглашений о передаче трафика и для поиска новых кандидатов для партнерства.

3.10.4.2 Отчет «Оценка договоренностей с соседями»

Таблица отчета содержит следующую информацию, см. таблицу 47.

Таблица 47 – Оценка договоренностей с соседями

Колонка	Описание
Ранг	Положение в рейтинге по объему трафика, которым сеть обменивается трафиком с этим ASN. Чем меньше число, тем больший объем.
ASN	Внешний для сети AS с которым происходит обмен трафиком. Если AS не задан как наблюдаемый объект, то доступен детальный отчет по трафику при клике на AS.
Имя	Название AS если задано.
Отношение	Для AS, настроенных как наблюдаемые объекты, указывается тип объекта
Входящий в сеть	Объем трафика, поступающего в сеть с AS, в bps

Колонка	Описание
Исходящий из сети	Объем трафика, исходящего из сети на AS, в bps
Всего	Суммарный объем трафика, которым сеть обменивается с AS, в bps

Можно скрыть AS настроенные как наблюдаемые объекты в Системе, для этого используйте флаг «Скрыть НО».

Для получения whois-информации об AS кликните на знак вопроса около его имени. При запросе информации делается запрос к whois-серверу, заданному на экране «Внешние сервера».

Для исследования, через какие наблюдаемые объекты происходит обмен трафиком с каким-либо AS из таблицы, кликните на него.

3.10.4.3 Детальный отчет «Разбивка по соседям для AS»

Отчет «Разбивка по соседям для AS» показывает через какие соседние сети, заданные на Анализаторе как наблюдаемые объекты, контролируемая сеть получает (и передает) трафик с исследуемого AS, см. рисунок 8. Отчет показывает как общий трафик через наблюдаемые объекты, так и долю трафика исследуемого AS. Отчет помогает в принятии решения о заключения партнерских соглашений или создании прямого подключения к исследуемому AS. Также, зная долю его трафика в трафике наблюдаемых объектов соседей, можно спрогнозировать, насколько уменьшится трафик соседей в случае создания прямого подключения.

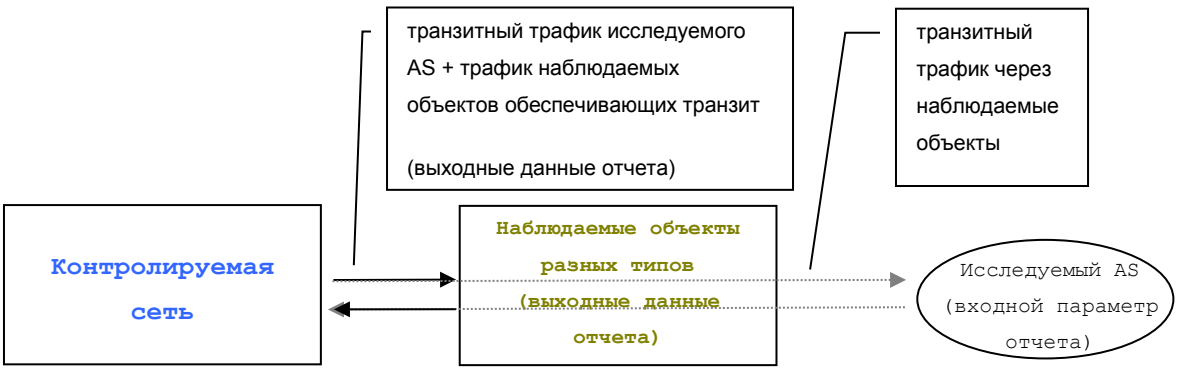


Рисунок 8 – Отчет «Разбивка по соседям для AS»

Для просмотра отчета выполните следующие шаги:

10) Перейдите на отчет «Оценка договоренностей с соседями» (Отчеты → Соседи → Утилиты → Оценка договоренностей с соседями).

11) Кликните на интересующий вас AS.

Замечание: в отчете показывается разбивка трафика, исследуемого AS через наблюдаемые объекты, которые пересекают эти потоки трафика. Эти наблюдаемые объекты обозначены в таблице как соседи, но в действительности они могут быть разных типов: клиенты, профили, соседи.

Кликните на наблюдаемый объект в таблице для получения детального отчета по маршрутам трафика, идущим через объект на исследуемый AS.

3.10.4.4 Детальный отчет «Разбивка трафика AS по маршрутам через соседа»

Отчет показывает, по каким AS маршрутам, идущим через выбранного соседа, контролируемая сеть обменивается трафиком с исследуемым AS, см. рисунок 9. Отчет помогает в принятии решений о маршрутизации трафика.

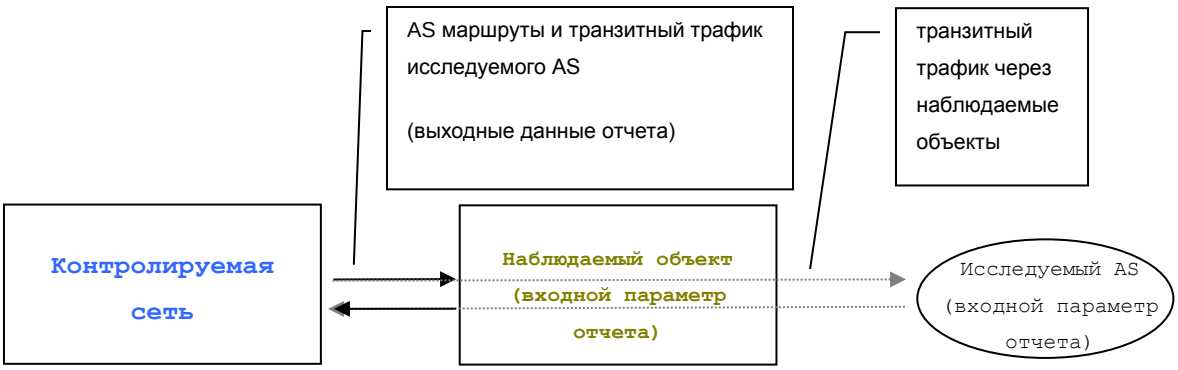


Рисунок 9 – Отчет «Разбивка трафика AS по маршрутам через соседа»

Для просмотра отчета выполните следующие шаги:

1) Перейдите на отчет «Оценка договоренностей с соседями» (Отчеты → Соседи → Утилиты → Оценка договоренностей с соседями).

2) Кликните на интересующий вас AS. Откроется отчет «Разбивка по соседям для AS».

3) Кликните на интересующего вас соседа (наблюдаемый объект).

3.10.5 Отчет по соседу и сравнение соседей

3.10.5.1 Введение

Возможен просмотр объемов трафика всех соседей одновременно для сравнения и просмотр трафика одного выбранного соседа, используя следующие отчеты:

- «Сравнение соседей» (Отчеты → Соседи → Суммарный отчет → Сравнение соседей);
- «Сосед» (Отчеты → Соседи → Суммарный отчет → Соседи).

3.10.5.2 Отчет «Сравнение соседей»

Отчет «Сравнение соседей» (Отчеты → Соседи → Суммарный отчет → Сравнение соседей) показывает следующую информацию в табличном виде, см. таблицу 48.

Таблица 48 – Сравнение соседей

Колонка	Описание
Сосед	Название наблюдаемого объекта соседа.
Входящий	Входящий трафик в сеть соседа. Этот трафик был сгенерирован в вашей сети или прошел транзитом через вашу сеть.
Исходящий	Исходящий трафик из сети соседа. Этот трафик был получен вашей сетью или прошел транзитом через вашу сеть.
Всего	Общий объем трафика, которым сеть обменивается с соседом. Сумма входящего и исходящего трафика.

Для просмотра информации только по соседям, входящим в определенную группу наблюдаемых объектов выберите название группы в поле «Группа».

Для перехода к детальному отчету по одному соседу, включающему отброшенный трафик кликните на название соседа.

3.10.5.3 Отчет «Сосед»

Отчет «Сосед» (Отчеты → Соседи → Суммарный отчет → Соседи) показывает такую же информацию, как и отчет «Сравнение соседей», но только для одного соседа. Дополнительно отчет показывает объем отброшенного трафика.

Отброшенный трафик соседа – это трафик, который направлен на соседа или с соседа, но один из роутеров вашей сети отбросил его.

Замечание: в отброшенный трафик попадает multicast-трафик, если не настроен учет multicast-трафика.

3.10.6 Отчет «Интерфейсы соседей»

Отчет «Интерфейсы соседей» (Отчеты → Соседи → Интерфейсы) показывает объем трафика соседа с разбивкой по интерфейсам.

В список интерфейсов попадают следующие интерфейсы:

- интерфейс, для которого назначен ASN соседа. Весь трафик этого интерфейса считается трафиком соседа;
- интерфейсы, на которых был трафик с AS маршрутами, проходящими через ASN соседа.

3.10.7 Детальные отчеты по соседям

3.10.7.1 Введение

Детальные отчеты расположены в меню отчетов по соседям «Отчеты → Соседи».

3.10.7.2 Типы детальных отчетов по соседям

Существуют следующие типы детальных отчетов по соседям:

- суммарный трафик;
- утилиты;
- приложения;
- BGP-атрибуты;
- по объектам;
- по размеру пакетов;
- QoS;
- протоколы;
- топология роутинга.

3.10.8 Настройка наблюдаемого объекта «Сосед»

3.10.8.1 Введение

Соседние сети могут быть настроены на Анализаторе как наблюдаемые объекты с целью детального наблюдения за их трафиком. Экран «Соседи» (Администрирование → Мониторинг → Наблюдаемые объекты → Соседи) перечисляет все созданные наблюдаемые объекты «Соседи».

3.10.8.2 О фильтрах для задания наблюдаемого объекта «Сосед»

Для создания наблюдаемого объекта «Сосед» могут быть использованы фильтры, указанные далее:

- соседние ASN-ы;
- фингерпринт выражение.

3.10.8.3 Создание и редактирование наблюдаемого объекта «Сосед»

Для создания или редактирования наблюдаемого объекта «Сосед» выполните следующие действия:

1) Перейдите на экран «Соседи» (Администрирование → Мониторинг → Наблюдаемые объекты → Соседи).
2) Выполните одно из следующих действий:
   - кликните по названию объекта в списке;
   - нажмите «Добавить наблюдаемый объект».
3) Введите название в поле «Название».
4) Введите описание в поле «Описание».
5) Нажмите «Сохранить».

3.10.8.4 Настройка фильтров для наблюдаемого объекта «Сосед»

Фильтры служат для указания Системе, какой трафик следует считать трафиком наблюдаемого объекта. Для создания фильтра выполните следующие действия:

1) Перейдите на вкладку «Конфигурация».
2) Выберите тип фильтра в поле «Фильтр 1».
3) Дальнейшие действия зависят от типа фильтра. См. таблицу 49.

Таблица 49 – Действия, зависящие от типа фильтра

Тип фильтра	Действия
ничего	трафиком соседа будет считаться весь трафик, прошедший через указанные граничные интерфейсы. Перейдите на вкладку «Границы» и выберите подходящий тип границы.
соседние ASN-ы	введите ASN (или ASN-ы) соседней сети, трафик которой необходимо отслеживать.
фингерпринт	введите фингерпринт выражение описывающее трафик соседней сети. **Замечание:** использование фингерпринт выражений уменьшает производительность Системы. Наблюдайте за загрузкой ЦПУ при их использовании.

4) При необходимости задайте второй фильтр, указав его тип в поле «Фильтр 2». Трафиком объекта будет являться трафик, соответствующий одновременно обоим фильтрам.

5) Нажмите «Сохранить».

3.10.8.5 Использование глобальной границы сети для наблюдаемого объекта «Сосед»

1) Перейдите на вкладку «Границы».

2) Выберите «Нет (глобальный peer, игнорировать правила)» в поле «Тип».

3) Нажмите «Сохранить».

3.10.8.6 Использование правил автоконфигурации для определения границы наблюдаемого объекта «Сосед»

1) Перейдите на вкладку «Границы».

2) Выберите «На основе правил» в поле «Тип».

3) В списке «Правила автоконфигурации» будут перечислены уже существующие правила, соответствующие этому наблюдаемому объекту. Для управления ими используйте специализированный экран «Правила автоконфигурации». Можно создать новое правило, которое будет соответствовать этому наблюдаемому объекту нажав «Добавить».

4) Нажмите «Сохранить».

3.10.8.7 Использование интерфейсов и правил автоконфигурации для определения границы наблюдаемого объекта «Сосед»

1) Перейдите на вкладку «Границы».

2) Выберите «Интерфейсы и правила» в поле «Тип».

3) Выберите режим конфигурации граничных интерфейсов объекта в поле «Тип граничного интерфейса». Возможны следующие варианты.

   – Простой режим. Граничные интерфейсы пропускают трафик, как на объект, так и от объекта. В этом режиме просто укажите список граничных интерфейсов в поле «Граничные интерфейсы» нажав на «Выбрать интерфейсы».

   – Расширенный режим. Граничные интерфейсы делятся на два типа:

     o обращенные к объекту – трафик через этот интерфейс будет считаться входящим трафиком объекта, когда интерфейс будет являться выходным для потока трафика;

     o обращенные от объекта (к backbone) – трафик через этот интерфейс будет считаться исходящим трафиком объекта, когда интерфейс будет являться выходным для потока трафика.

В этом режиме укажите оба списка граничных интерфейсов в полях «Интерфейсы, обращенные к объекту» и «Интерфейсы, обращенные к backbone».

4) В списке «Правила автоконфигурации» будут перечислены уже существующие правила, соответствующие этому наблюдаемому объекту. Для управления ими используйте специализированный экран «Правила автоконфигурации». Можно создать новое правило, которое будет соответствовать этому наблюдаемому объекту нажав «Добавить».

5) Нажмите «Сохранить».

3.10.8.8 Детекция аномалий по шаблонным пакетам для наблюдаемого объекта «Сосед»

1) Перейдите на вкладку «Детекция».

2) В поле «По шаблонным пакетам» выберите один из вариантов работы детектора.

   – «Всегда выключено». Детектор отключен.

   – «По умолчанию (использовать глобальные настройки)». Используются настройки по умолчанию.

   – «Всегда включено». Детектор включен. Нажмите «Редактировать» и проведите настройку параметров детектора. Настройки аналогичны глобальным настройкам детектора.

3) Нажмите «Сохранить».

3.10.8.9 Детекция аномалий по профилю поведения для наблюдаемого объекта «Сосед»

1) Перейдите на вкладку «Детекция».

2) В поле «По профилю поведения» выберите один из вариантов работы детектора:

   – «Всегда выключено». Детектор отключен.

   – «По умолчанию (использовать глобальные настройки)». Используются настройки по умолчанию.

   – «Всегда включено». Детектор включен. Нажмите «Редактировать» и проведите настройку параметров детектора. Настройки аналогичны глобальным настройкам детектора.

3) Нажмите «Сохранить».

3.10.8.10 О детекции аномалий по порогам трафика наблюдаемого объекта «Сосед»

Анализатор позволяет установить граничные значения по трафику для наблюдаемого объекта. При превышении объема трафика верхней границы или если трафик упадет ниже нижней границы, Система создаст аномалию с высокой важностью, без направления.

3.11 Мониторинг работы Системы

3.11.1 Введение

Используйте раздел меню «Система» для просмотра статуса использования Анализатора.

3.11.2 Экран «Суммарный отчет»

3.11.2.1 Введение

Экран «Суммарный отчет» (Система → Статус → Суммарный отчет) отображает активность по аномалиям за последние 24 часа, суммарный отчет по сетевому трафику за последние 24 часа и 5 текущих и прошедших аномалий: DoS и системных событий. Информация на этом экране автоматически обновляется с фиксированной периодичностью, конфигурируемой на экране глобальных настроек пользовательского интерфейса (параметр «Период обновления статусной страницы»).

3.11.2.2 Графики суммарного отчета

График «Активность по аномалиям за последние 24 часа» показывает, сколько аномалий и какого типа было зафиксировано в указанный промежуток времени. График позволяет быстро оценить ситуацию с аномалиями в контексте всей Системы. Аномалии одного типа визуально группируются на графике в один горизонтальный слой, не пересекающийся со слоем аномалий другого типа. Ось X – ось времени. Каждая аномалия изображена горизонтальным отрезком. Длина отрезка отражает длительность аномалии. Чем длиннее отрезок, тем дольше длилась аномалия. При наведении мыши на начальные или конечные точки отрезков

отображается всплывающая подсказка с информацией об аномалии и времени начала или окончания аномалии, соответственно. Очень короткие аномалии могут выглядеть как точка. Вертикальные линии символизируют события изменения конфигурации Системы. При наведении на конечную точку (самая верхняя точка вертикальной линии) отображается информация о реконфигурации Системы.

Суммарный график по сетевому трафику отражает общий, входящий, отброшенный, исходящий и multicast-трафик в контролируемой сети за последние 24 часа. Ось Y отражает количество трафика, ось X - время.

3.11.2.3 Таблица «Топ 5 текущих и прошедших аномалий»

Таблица содержит следующую информацию, см. таблицу 50.

Таблица 50 – Поля таблицы аномалий

Колонка	Описание
ID	Уникальный идентификатор аномалии, назначенный Системой. При наличии подробной информации об аномалии, является гиперссылкой на экран с соответствующей информацией.
Время начала	Время, когда Анализатор впервые зафиксировал аномалию.
Время окончания	Время окончания аномалии. Если аномалия продолжается, пишется «Идет в данный момент». **Замечание**: для мгновенных аномалий, время начала и окончания могут совпадать.
Тип аномалии	Тип аномалии, кодированный цветом.
Информация	Информация об аномалии. Краткий текстовый комментарий к аномалии, отражающий ее суть. К примеру, сообщение о поврежденном роутере или интерфейсе.

3.11.3 Экран «DoS-аномалии»

3.11.3.1 Введение

На экране «DoS-аномалии» (Система → Статус → Аномалии) представлена общая информация по аномалиям, график аномалий за прошедшие 24 часа и список из пяти наиболее опасных аномалий, идущих в данный момент.

3.11.3.2 Общая информация

Общая информация по аномалиям представлена сводной таблицей по текущим и завершенным аномалиям, а также аномалиям, зафиксированным за последние 24 часа в разбивке по уровню важности.

Для текущих и завершенных аномалий общее количество аномалий (указанное в квадратных скобках возле каждой категории), а также количество по каждому уровню важности, являются гиперссылками на экран с информацией по всем аномалиям данной категории.

3.11.3.3 График аномалий за последние 24 часа

График аномалий за последние 24 часа показывает активность аномалий по категориям за последние 24 часа. Логика графика соответствует логике графика на экране «Суммарный отчет», описанного в предыдущем разделе, за тем лишь исключением, что на графике аномалий за последние 24 часа показаны исключительно DoS-аномалии. Красным показаны наиболее опасные DoS-аномалии, желтым – аномалии средней опасности, и зеленым - низкой.

Замечание: ограниченным пользователям на графике показываются только аномалии, касающиеся их сети, а не все текущие аномалии.

3.11.3.4 Таблица «Топ 5 текущих DoS-аномалий»

Таблица показывает 5 наиболее опасных аномалий, идущих в данный момент, которые детектировал Анализатор.

Таблица содержит следующую информацию, см. таблицу 51.

Таблица 51 – Поля таблицы аномалий

Колонка	Описание
ID	Уникальный идентификатор аномалии, назначенный Системой. При наличии подробной информации об аномалии, является гиперссылкой на экран с соответствующей информацией.
Трафик	Эскиз графика трафика аномалии. Позволяет быстро оценить текущую активность аномалии. При наличии подробной информации об аномалии, график так же является гиперссылкой на экран с соответствующей информацией.
Важность	Уровень важности аномалии и процент максимального пикового уровня трафика от верхнего порога детектирования аномалии.
Влияние	Максимальный трафик на граничном интерфейсе для трафика, соответствующего сигнатуре аномалии.
Длительность	Время продолжительности аномалии.
Время начала	Время, когда Анализатор впервые зафиксировал аномалию.
Направление	Направление трафика аномалии: входящее, исходящее или неизвестное.
Тип	Тип аномалии.
Ресурс	IP-адрес устройства или сети, для которых зафиксирована аномалия. Если известно имя клиента или профиля - оно отобразится в виде гиперссылки. При наведении на гиперссылку показывается всплывающее меню, позволяющее перейти на суммарный отчет для данного объекта или на экран редактирования параметров объекта. **Замечание**: если IP-адрес ресурса 0.0.0.0/0, Система напишет: «Весь трафик».
Информация	Текстовый комментарий к аномалии, отражающий ее суть.

3.11.4 Экран «Сравнение SNMP/ NetFlow»

3.11.4.1 Введение

Экран Сравнение SNMP/ NetFlow показывает трафик SNMP и NetFlow по каждому интерфейсу выбранного роутера.

3.11.4.2 Экран «Сравнение SNMP/ NetFlow»

На экране «Сравнение SNMP/NetFlow» (Система → Сравнение SNMP/ NetFlow) отображается таблица, содержащая следующую информацию, см. таблицу 52.

Таблица 52 – Поля таблицы отчета

Колонка	Описание
◉	Определяет, трафик какого интерфейса отображать на графике.
Рейт	Вычисляемый рейт потока SNMP-трафика по данному интерфейсу.
Интерфейс	Название интерфейса.
SNMP-индекс	Индекс интерфейса.
Входящий (Flow/SNMP)	Входящий NetFlow и SNMP-трафик.
Исходящий (Flow/SNMP)	Исходящий NetFlow и SNMP-трафик.
Всего (NetFlow)	Суммарный (входящий плюс исходящий) NetFlow-трафик.
Всего (SNMP)	Суммарный (входящий плюс исходящий) SNMP-трафик.

3.11.5 Мониторинг устройств анализа и очистки

3.11.5.1 Введение

Экран «Статус устройств» (Система → Статус → Устройства Syn → Статус устройств) отражает информацию о статусе каждого устройства Syn индивидуально в реальном времени. Каждое из этих устройств можно использовать для мониторинга общего состояния Системы, загрузки и планирования возможностей.

3.11.5.2 Вкладки экрана «Статус устройств»

Экран «Статус устройств» (Система → Статус → Устройства Syn → Статус устройств) имеет следующие вкладки:

Информация на экране разбита по следующим вкладкам:

1) «Общая информация». Позволяет диагностировать состояние всех устройств Системы по заданному периоду времени.

2) «Интерфейс пользователя». Позволяет диагностировать состояние всех устройств пользовательского интерфейса по заданному периоду времени.

3) «Датчики». Отображает состояние датчиков, сконфигурированных в Системе.

3.11.5.3 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.

3.11.5.4 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:

- кол-во Flow-записей в секунду, полученных Анализатором;
- поток NetFlow, бит в секунду;
- поток NetFlow, пакетов в секунду;
- загрузку процессора, %;
- использование диска, %;
- использование памяти, %;
- использование виртуальной памяти, %;
- количество необработанных Flow-записей в секунду;
- количество Flow-записей в секунду, полученных с нарушением последовательности;
- перегрузку Анализатора, %.

Таблица содержит следующую информацию по каждому устройству, см. таблицу 53.

Таблица 53 – Поля таблицы экрана

Колонка	Описание
◉	Определяет, информацию о каком устройстве отображать на графике.
Название	Название устройства.
Статус	Статус устройства.
BGP	Количество роутеров, с которыми в данный момент установлено соединение BGP и общее число роутеров с поддержкой BGP.
Заданий	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.
Память	Процент использования оперативной памяти.
Процессор	Процент использования процессора.
Диск	Процент заполнения жесткого диска.
Время включения	Дата и время включения устройства.

3.11.5.5 Вкладка «Интерфейс пользователя» экрана «Статус устройств»

Вкладка «Интерфейс пользователя» экрана «Статус устройств» (Система → Статус → Устройства Syn → 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.

Таблица содержит следующую информацию, см. таблицу 54.

Таблица 54 – Список полей таблицы

Параметр	Описание
Название	Название устройства.
Активные пользователи	Количество активных пользователей.
Время загрузки страницы	Среднее время загрузки страницы.
Просмотрено отчетов	Количество просмотренных отчетов.
Загружено страниц	Количество загруженных страниц.
Вошли в систему	Количество пользователей, вошедших в Систему.
Вышли из системы	Количество пользователей, вышедших из Системы.

3.11.5.6 Вкладка «Датчики» экрана «Статус устройств»

Вкладка «Датчики» экрана «Статус устройств» (Система → Статус → Устройства Syn → Статус устройств) показывает графики зависимости показаний датчиков от времени. Для просмотра данных выполните следующие действия:

1) Перейдите на экран «Статус устройств» («Система» → «Статус» → «Статус устройств»).
2) Перейдите на вкладку «Датчики».
3) Выберите датчик в выпадающем списке «Датчик».
4) Нажмите «Обновить график».

Можно включить автоматическое обновление графика галочкой «Автообновление текущих данных каждые 15 секунд».

4. СООБЩЕНИЯ ОПЕРАТОРУ

Анализатор трафика является серверным программным обеспечением и не работает в интерактивном режиме. Пользователь может проводить настройку Анализатора в соответствии с разделом 3.

ПРИЛОЖЕНИЕ 1

ПЕРЕЧЕНЬ ТЕРМИНОВ

В настоящем документе применяют следующие термины с соответствующими определениями.

Автономная система	Система IP-сетей и маршрутизаторов, управляемая одним или несколькими операторами и имеющая единую политику маршрутизации с Интернетом.
Детектор аномалий	Программный модуль, реализующий набор алгоритмов для обнаружения аномалий определенного типа и имеющий набор конфигурационных параметров.
Инфраструктурные элементы СПД	Набор устройств и сервисов, обеспечивающих функционирование сети, в том числе: – устройства маршрутизации и пакетной коммутации; – пакетные брандмауэры, анализаторы трафика, системы обнаружения атак; – центры обработки данных и сервера приложений; – беспроводные контроллеры и точки доступа; – устройства обеспечения физической безопасности.

Наблюдаемый объект	Совокупность объектов сети, потоков трафика и сетевых сервисов, рассматриваемая анализатором трафика как единое целое в контексте задач мониторинга обнаружения сетевых угроз.
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.
Сетевые сервисы	Приложение или функциональность, поддерживаемая и обеспечиваемая инфраструктурными элементами СПД.
NetFlow	Семейство протоколов, поддерживаемых маршрутизаторами, для предоставления "слепков" трафика.

ПРИЛОЖЕНИЕ 2

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

СПД	Сеть передачи данных.
ACL	Access Control List (список управления доступом).
AS	Autonomous system (автономная система).
BGP	Border Gateway Protocol.
DoS-атака	Атака типа Denial-Of-Service (отказ обслуживания).
DDoS-атака	Атака типа Distributed Denial-Of-Service (распределенная атака отказа обслуживания).
SNMP	Simple Network Management Protocol.
XML	eXtensibe Markup Language, универсальный текстовый формат для хранения и передачи структурированных данных.

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм	измененных	замененных	новых	аннулированных					
1	-	2-149	-	-	150	ИИ АЦВТ.05-14	-		11.09.14
2									