ГАРДА
ТЕХНОЛОГИИ

ООО "Гарда Технологии"

Руководство пользователя

Модуль Лидер ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 Введение **1**
- 1.1 Аннотация . . . 1
- 1.2 Использование имен, номеров телефонов, сетевых адресов . . . 1
- 1.3 О компании . . . 1
- 1.4 Техническая поддержка . . . 1

2 Назначение **2**

3 Работа с Лидером **3**
- 3.1 Основные функции . . . 3
- 3.2 Общие сведения . . . 3
- 3.3 Аппаратная реализация . . . 4
- 3.4 Включение модуля Лидер . . . 4
- 3.5 Начало работы . . . 4

4 Выявление аномалий и подготовка к противодействию **11**
- 4.1 Общая информация . . . 11

5 Аннотации к аномалии **17**

6 Работа с наблюдаемыми объектами **18**
- 6.1 Общие элементы конфигурации . . . 19
- 6.2 Наблюдаемый объект типа «клиент» . . . 19
- 6.3 Наблюдаемый объект типа «профиль» . . . 20
- 6.4 Наблюдаемый объект типа «червь» . . . 20

1 Введение

1.1 Аннотация

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

1.2 Использование имен, номеров телефонов, сетевых адресов

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

1.3 О компании

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

- защиты от DDoS-атак операторского класса.
- защиты баз данных.
- фрод-мониторинга порядка пропуска трафика операторов связи.
- DLP-систем.

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

1.4 Техническая поддержка

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

- Тел. +7 (831) 422-12-26
- Email: ddos.support@gardatech.ru

2 Назначение

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

Решение данной задачи основано на:

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

3 Работа с Лидером

3.1 Основные функции

- выполняет мониторинг трафика СПД и выявляет аномалии;
- осуществляет непрерывный анализ трафика контролируемой сети;
- при обнаружении атаки выдает команды маршрутизирующему оборудованию на первичную очистку и последующее перенаправление трафика на Очиститель

3.2 Общие сведения

ПК «ПЕРИМЕТР» получает данные о трафике по следующим протоколам:

- Netflow - является основным используемым протоколом, данные, полученные по этому протоколу, используются для:
  - формирования отчетной информации по трафику, проходящему через контролируемую сеть;
  - сопоставления трафика с наблюдаемыми объектами;
  - формирования аналитической информации по наблюдаемым объектам (отчеты по трафику в различных разрезах);
  - выявления аномального поведения трафика с разбиением по типам;
  - формирования аналитической информации по трафику маршрутизирующего оборудования (отчеты по трафику в различных разрезах);
- SNMP - является дополнительным протоколом получения данных, использующихся для:
  - получения информации об интерфейсах маршрутизирующего оборудования (описание, скорость, утилизация и т.п.), которая необходима для выполнения комплексом автоматической классификации интерфейсов;
  - формирования дополнительной отчетной информации по трафику;
  - определения эксплуатационных параметров маршрутизаторов сети;
  - сопоставления данных по объемам трафика с данными по NetFlow;
- BGP - является средством управления маршрутизацией и дополнительным протоколом получения данных о трафике, используемым для:
  - формирования отчетной информации;
  - управления перенаправлением трафика на очистку;
  - управления фильтрацией по FlowSpec и Blackhole;
  - работы с таблицами маршрутизации инфраструктурных элементов сети;
  - выявления аномального поведения маршрутизирующего оборудования в рамках протокола BGP.

3.3 Аппаратная реализация

Каждый модуль комплекса исполнен в виде серверного устройства, устанавливаемого в 19" серверные шкафы и стойки.

Для обеспечения функций сетевого взаимодействия Лидер имеет:

- интерфейсы управления и интерфейсы взаимодействия с модулями Анализатор;
- интерфейсы взаимодействия с элементами инфраструктуры сети;

3.4 Включение модуля Лидер

Модуль Лидер имеет следующие логические интерфейсы:

- Интерфейс управления - обеспечивающий возможность подключения пользователей к web-интерфейсу;
- Интерфейс подключения к технологической сети - предоставляющий возможность взаимодействия модуля Лидер с модулями Анализатор;
- Интерфейс горячего резерва - данный интерфейс применяется для обмена информацией с резервным модулем Лидер, в случае применения режима горячего резерва.

Все логические интерфейсы могут быть исполнены как в рамках одного физического интерфейса, так и нескольких.

3.5 Начало работы

Настройка и администрирование комплекса осуществляется через графический интерфейс пользователя (далее web-интерфейс) в виде набора web-страниц.

Чтобы открыть web-интерфейс:

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

5. Нажмите кнопку Войти.

Примечание: При первом открытии web-интерфейса возможно сообщение о небезопасности сертификата. Следует принять предлагаемый сертификат.

ВАЖНО: Не поддерживается работа браузера Internet Explorer в режиме совместимости.

3.5.1 Web-интерфейс

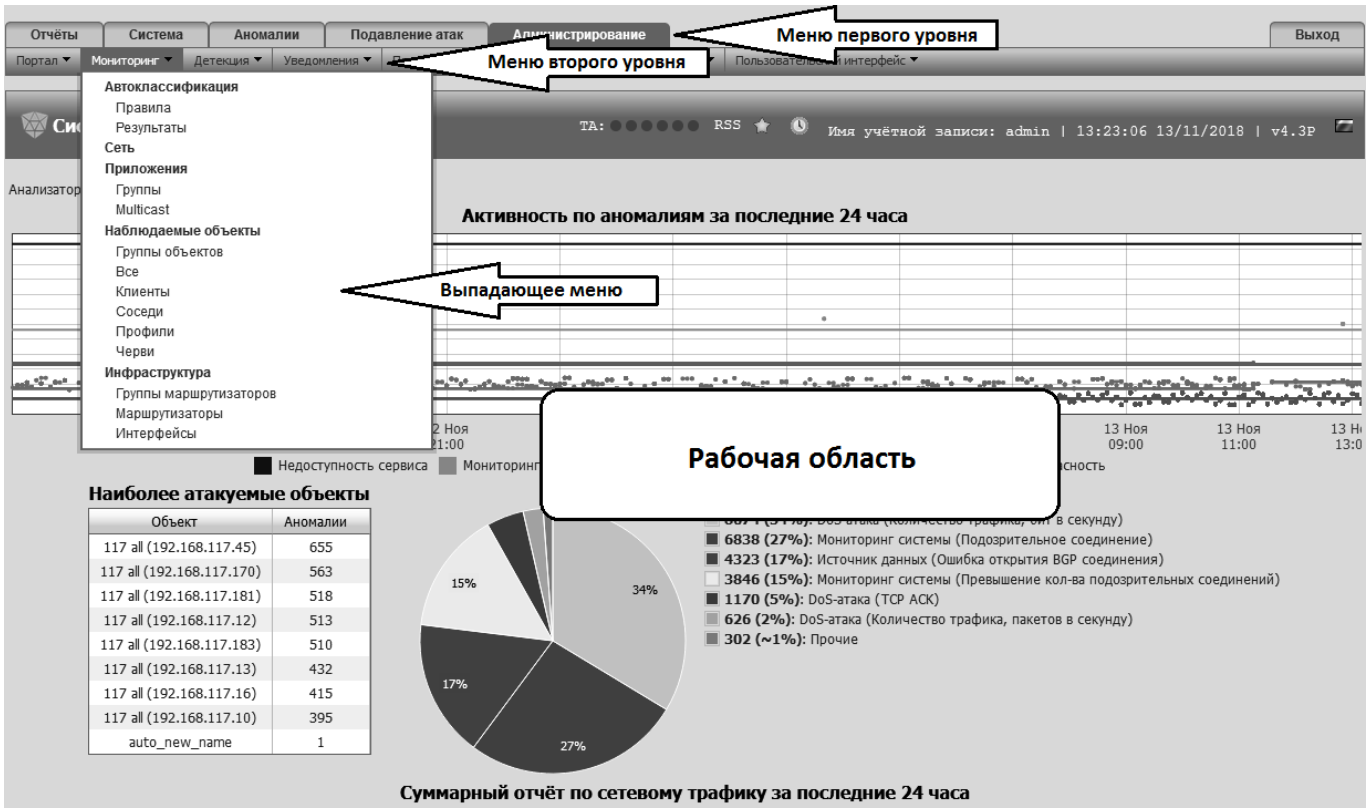

Рис. 1 Пример страницы интерфейса.

Навигация по страницам веб-интерфейса осуществляется с помощью меню 1-го и 2-го уровней, выпадающих меню и элементов управления на страницах.

3.5.2 Главное меню

Строка меню первого уровня содержит главные разделы элементов использования и администрирования АПК «Периметр». Меню второго уровня меняет свое содержание в соответствии с выбранным разделом меню первого уровня и содержит его подразделы. Если подраздел не может быть описан одним пунктом меню, то он содержит выпадающее меню, со всеми пунктами подраздела.

Строка меню первого уровня содержит следующие разделы:

Пункт меню 1-го уровня	Содержит ...
Отчёты	аналитическую информацию в виде отчётов, доступ к сбору и просмотру «сырых» данных netflow
Система	информацию о состоянии системы в целом, её отдельных модулей и компонентов
Аномалии	информацию о текущих и прошедших DoS-атаках, а также событиях, зафиксированных системой
Подавление атак	страницы для просмотра, настройки и управления средствами противодействия атакам
Администрирование	страницы управления и настройки системы

3.5.3 Глобальные настройки web-интерфейса

Глобальными настройками web-интерфейса называются параметры, определяющие его внешний вид и функциональность для всех пользователей.

Данные настройки можно выполнить на странице пользовательского интерфейса «Администрирование / Пользовательский интерфейс / Глобальные настройки».

3.5.4 Задание системных настроек

В разделе «Системные настройки» задаются следующие параметры:

- Электронный адрес технической поддержки - это адрес электронной почты, на который система пересылает все заявки и вопросы пользователей. Отправка письма по указанному адресу возможна при включенной RSS-ленте, путем нажатия на гиперссылку «Техподдержка» в правой части RSS-ленты. Данная гиперссылка доступна только при условии, что в глобальных настройках указан адрес технической поддержки;
- Время бездействия учётной записи - время бездействия пользователя в web-интерфейсе, по истечении которого для продолжения работы системой будет запрошена повторная аутентификация учётной записи;
- Период обновления статусной страницы - временной интервал автоматического обновления страницы «Система / Статус / Суммарный отчет», используемой в качестве стартовой страницы по умолчанию;
- Адрес сайта - URL, используемый для ссылок в отправляемых системой письмах и экспортированных отчётах;
- Название анализатора - название анализатора, отображаемое в заголовке окна web-браузера;
- Максимальное количество сообщений в почтовой очереди - если количество сообщений в почтовой очереди оказывается больше, чем заданное, система выявляет аномалию отправки почтовых сообщений;
- Количество отображаемых сообщений в ленте событий - максимальное количество отображаемых сообщений в RSS-ленте в свернутом состоянии;

- Часовой пояс - часовой пояс, который система по умолчанию использует при создании учётных записей пользователей;
- Кодировка возвращаемых файлов - параметры кодировки фалов/списков, получаемых при работе с заданиями очистки (поддерживаются кодировки UTF-8 и ANSI);
- Ограничение на количество комментариев в PDF-экспорте митигации - данный параметр устанавливает максимальное количество комментариев, которые будут отображены в PDF-файле, создаваемом при экспорте задания очистки;
- Ограничение на количество записей в почтовых отчетах - максимальное количество строк в таблицах при формировании почтовых уведомлений;
- Выделять аномалии при превышении опасности - данный параметр задает значение превышения порога опасности DoS-аномалии, при достижении которого аномалия помечается красным шрифтом.

Чтобы изменить один или несколько из вышеперечисленных параметров необходимо:

1. Перейти на страницу глобальных настроек пользовательского интерфейса «Администрирование / Пользовательский интерфейс / Глобальные настройки»;
2. Внести необходимые изменения;
3. Нажать кнопку «Сохранить», расположенную в нижней части рабочей области страницы.

3.5.5 Учетные записи

Web-интерфейс предоставляет доступ ко всей функциональности системы. Для того чтобы предоставить доступ и разграничить права пользователей в зависимости от решаемых ими задач, в системе реализована функция создания учётных записей пользователей с разными правами и объединения их в группы.

Работа с учётными записями пользователей осуществляется на странице учётных записей «Администрирование / Доступ / Учётные записи». Данные по уже имеющимся учётным записям представлены на странице в виде таблицы со следующими полями:

Поле	Описание
Имя учётной записи	Имя учётной записи пользователя
Настоящее имя	Отображаемое имя пользователя
Группа	Группа пользователей, к которой принадлежит учётная запись пользователя
Адрес электронной почты	Адрес электронной почты пользователя
Последний IP	IP-адрес хоста, с которого была выполнена аутентификация учётной записи пользователя в последний раз. Так же в этом поле отображается доменное имя, если его получилось разрешить по IP-адресу
Последний вход в систему	Дата и время последней аутентификации учётной записи пользователя в системе
Заблокирован	Заблокирована ли учётная запись пользователя
На сайте	Работает ли пользователь с web-интерфейсом в данный момент
Тип аутентификации	Тип аутентификации учётной записи пользователя для доступа к графическому интерфейсу и API

3.5.6 Права доступа

Права доступа используются в системе для разграничения набора доступных функций различным группам пользователей. Набор прав может быть назначен как обычной группе пользователей, так и группе ограниченных пользователей. Вся работа с настройкой прав доступа осуществляется на странице интерфейса «Администрирование / Доступ / Права доступа» (рисунок 27). На данной странице присутствует возможность выбора набора прав доступа и его настройки посредством элементов древовидного графа.

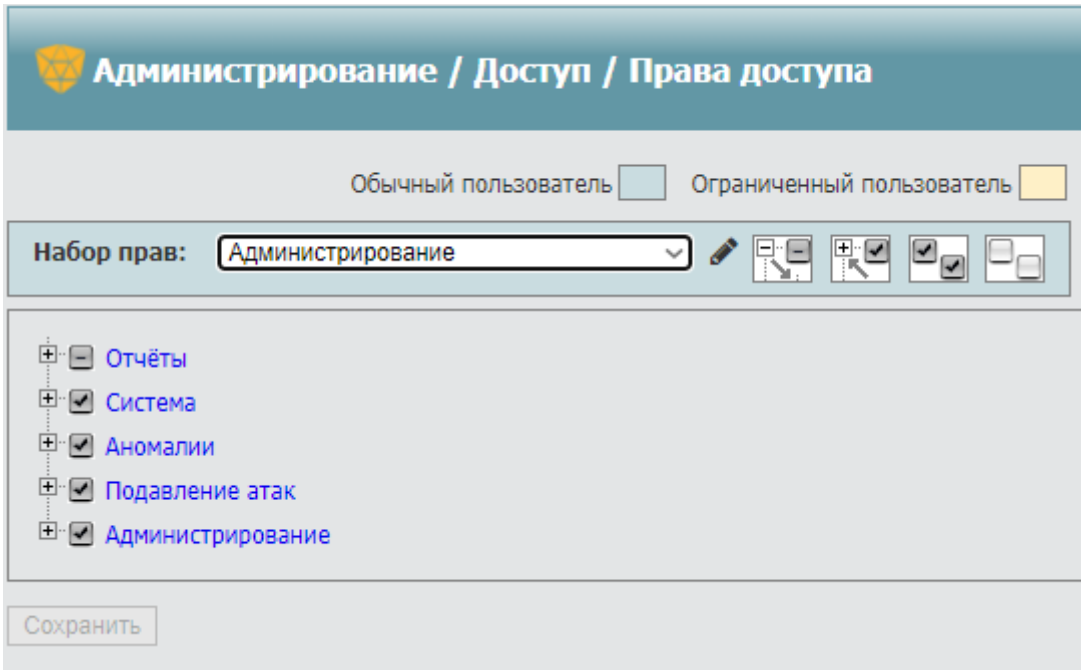

Рис. 2 Экран настройки прав доступа.

Чтобы настроить права доступа необходимо:

1. Перейти на страницу настроек прав доступа «Администрирование / Доступ / Права доступа»;
2. Выбрать один из набора прав в раскрывающемся списке. Система содержит наборы прав для
   - обычных пользователей - позволяет выбрать список экранов, на которые пользователи группы с данным набором прав имеют доступ;
   - ограниченных пользователей - содержит ограниченный набор доступных для пользователя экранов;
3. Нажать кнопку «Сохранить».

Примечание: Для облегчения работы с древовидным меню можно воспользоваться кнопками, описание которых дано ниже.

Кнопка	При нажатии ...
Развернуть все	разворачивает все ветви древовидного меню
Свернуть все	сворачивает все ветви древовидного меню
Выбрать все	устанавливает все флажки в древовидном меню
Снять все выбранные	снимает все флажки в древовидном меню

3.5.7 Ограниченные пользователи

Для Клиентов (абонентов оператора связи), желающих принимать непосредственное участие в борьбе с сетевыми угрозами, в системе предусмотрена функция создания учётных записей с ограниченными правами доступа к личному кабинету.

Учётная запись, создаваемая для абонентов оператора связи, носит название «ограниченный пользователь». Ограниченные пользователи могут просматривать информацию и работать с системой, не имеют возможности изменять её параметры. Права ограниченного пользователя определяются правами группы пользователей, к которой он принадлежит.

Разграничение доступа ограниченных пользователей осуществляется как к страницам веб-интерфейса, так и к наблюдаемым объектам. Ограниченные пользователи не могут получить доступ к отчётам или страницам инфраструктурных объектов (интерфейсами, маршрутизаторами и т.д.), даже если доступ к этим страницам разрешён настройками прав доступа.

Работа с группой ограниченных пользователей полностью аналогична работе с группой обычных пользователей, за исключением процедуры создания группы ограниченных пользователей.

3.5.8 Мониторинг учётных записей пользователей

3.5.8.1 История учётных записей

Комплекс осуществляет автоматическую запись в базу данных информации по всем учётным записям пользователей, работающих с комплексом через web-интерфейс.

Данные доступны на странице истории учётных записей пользователей «Система / Статус / Устройства / История пользователей». Данные представлены в виде таблицы со следующими столбцами:

- Учетная запись - имя учетной записи, выполнявшей действия;
- IP-адрес - адрес хоста, с которого был осуществлён вход в систему. Дополнительно в поле указывается доменное имя хоста, если его удалось разрешить по адресу;
- Событие - действия, выполненные под учетной записью. На данном экране отслеживаются действия:
- Вход в систему - факт авторизации пользователя в системе. В случае неуспешной попытки входа, в поле детали будет отображаться факт ошибки;
- Создание учетной записи - указывает на то, что данным пользователем было выполнено создание учетной записи, имя которой указано в поле «Детали»;
- Изменение учетной записи - указывает на то, что данным пользователем было выполнено изменение учетной записи, имя которой указано в поле «Детали»;
- Удаление учетной записи - указывает на то, что данным пользователем было выполнено удаление учетной записи, имя которой указано в поле «Детали»;
- Время входа в систему - время последней аутентификации пользователя в системе;
- Продолжительность - длительность последнего сеанса работы учётной записи пользователя. Если пользователь работает с системой, то в поле «Детали» будет значение «сейчас в системе»;

- Детали - дополнительная информация к записи в журнале.

На данной странице есть возможность просмотра только ошибочных попыток авторизации в системе (параметр «Показывать только ошибки авторизации»), а также возможность использования фильтра по имени учетной записи и временному периоду.

3.5.8.2 История посещений

На странице истории посещений «Система / Интерфейс пользователя» содержится информация об учётных записях пользователей и страницах, которые они посещали. Данные представлены в виде таблицы со следующими столбцами:

Столбец	Описание
Дата	Дата и время посещения страницы
Пользователь	Учётная запись пользователя, посещавшего страницу
IP-адрес	IP-адрес хоста, с которого посещалась страница. Дополнительно в поле указывается доменное имя хоста, если его удалось разрешить по адресу
Страница	URL страницы, которую посещал пользователь
Время	Время загрузки страницы в секундах

Блок фильтра позволяет указать учетную запись и временной диапазон для отображения данных о посещении страниц веб-интерфейса заданным пользователем за выбранный интервал времени.

3.5.9 Ограничение доступа к управлению

Функция ограничения доступа к управлению ПК «ПЕРИМЕТР» позволяет разрешать или запрещать подключение к графическому интерфейсу пользователя из различных сетевых сегментов. Сегменты сети в списках доступа задаются IPv4 префиксами (CIDR-блоками).

Настройка списков доступа производится через меню «Администрирование / Доступ / Сетевые подключения / Ограничение доступа к порталу».

Поддерживаются два режима управления доступом:

- Черный список — запрет доступа к графическому интерфейсу пользователя с IPv4 адресов, входящих в префиксы списка, при условии отсутствия более специфичного префикса в «белом списке»;
- Белый список — разрешение доступа к графическому интерфейсу пользователя с IPv4 адресов, входящих в префиксы списка, даже при условии присутствия менее специфичных префиксов в «черном списке».

Изменения, вносимые в список, необходимо в обязательном порядке подтверждать нажатием кнопки «Сохранить», находящейся в том же разделе страницы. В противном случае, они не будут применены.

В каждой строке списка после указания IP адреса допустимо указывать однострочный комментарий, начинающийся с символа # и отделенный от IP адреса как минимум одним пробелом.

4 Выявление аномалий и подготовка к противодействию

4.1 Общая информация

Системный журнал (syslog) содержит информацию о событиях, возникающих в работе комплекса. Доступ к системным журналам осуществляется на странице интерфейса «Система / Системный журнал». На странице необходимо выбрать необходимый системный журнал из выпадающего списка «Syslog». Выбранный системный журнал отобразится на странице.

Поле Фильтр (regexp) служит для ограничения выводимой информации регулярным выражением. Отображенный на странице системный журнал будет содержать только те строки, для которых заданное выражение является истинным.

Примечание. На странице веб-интерфейса отображаются последние 200кб журнала syslog.

4.1.1 Типы аномалий

ПК «ПЕРИМЕТР» выполняет выявление аномалий следующих типов:

- DoS-атака - набор векторов атак, направленных на хост или наблюдаемый объект;
- BGP-аномалии - отклонения параметров маршрутизации трафика от нормальных;
- Аномалии загрузки канала - потенциальные перегрузки каналов передачи данных;
- Аномалии источников данных - поддельные данные, получаемые от маршрутизаторов, либо отсутствие этих данных;
- Аномалии системы - сбои в нормальной работе АПК;
- Аномалии очистителя (предупреждения очистителя) - сбои в работе программных модулей очистителя;
- SNMP-аномалии - замена физических устройств СПД;
- 1+1 - события, связанные с функционалом горячего резервирования.

4.1.2 Выявление аномалий по данным протоколов семейства Netflow

Использование информации о трафике, передаваемой от маршрутизаторов в ПК «ПЕРИМЕТР» по протоколам семейства netflow, позволяет выявлять аномалии без прямого анализа трафика, что очень важно для сетей операторского уровня с большими объемами трафика. Информация о трафике анализируется независимо для каждого маршрутизатора, а также консолидируется с целью получения обобщенной информации о трафике, проходящем через контролируемую сеть, в целом или его отдельных частей, определяемых настройками ПК «ПЕРИМЕТР».

Маршрутизаторы СПД передают информацию о трафике не постоянно, а при соблюдении некоторых условий:

- end of flow (IPFIX code 3) — маршрутизатор обнаружил, что поток данных (сессия или соединение) завершен, следовательно, необходимо завершить сбор данных для этого потока и отправить информацию о трафике;
- idle timeout (IPFIX code 1) — данные не передавались в течение установленного интервала idle timeout, поэтому маршрутизатор завершает сбор данных для этого потока и отправляет информацию о трафике;
- active timeout (IPFIX code 2) — данные передаются в течение установленного интервала active timeout, маршрутизатор продолжает сбор данных для этого потока и отправляет информацию о трафике на момент превышения active timeout;
- forced end (IPFIX code 4) — принудительное завершение сбора данных для этого потока и отправка информации о трафике на момент завершения;
- lack of resources (IPFIX code 5) — информация о трафике отправляется вне очереди, в связи с недостаточностью ресурсов на маршрутизаторе;
- unknown (IPFIX code 0) — причина отправки информации о трафике не указана.

Протоколы семейства netflow не обязывают маршрутизатор указывать причину отправки информации о трафике. Стандартизованные коды причины отправки существуют только для протокола IPFIX. Поэтому наличие такого кода является лишь дополнительным фактором при принятии решения о методе обработки netflow-записи подсистемой выявления аномалий ПК «ПЕРИМЕТР».

Важно понимать, что информация о трафике поступает в ПК «ПЕРИМЕТР» уже после того, как трафик прошел через маршрутизатор. Причем задержка поступления этой информации достигает величин, определяемых на маршрутизаторах интервалами idle timeout и active timeout.

Выявление аномалий подразумевает анализ трафика на определенном интервале - интервале детектирования (по умолчанию в ПК «ПЕРИМЕТР» интервал детектирования составляет 5 секунд).

Получив netflow-запись от маршрутизатора, ПК «ПЕРИМЕТР» принимает решение о том каким образом она будет учитываться при выявлении аномалий:

- netflow-запись будет учтена в текущем интервале детектирования полностью без каких-либо условий — применяется для netflow-записей, не содержащих фрагментированный трафик, в случае, если причина отправки отсутствует или причина отправки не равна active timeout;
- netflow-запись будет учтена в текущем и последующих интервалах детектирования (количество последующих интервалов зависит от длительности потока данных, но не превышает количества интервалов, определяемых параметром active timeout маршрутизатора) — применяется для netflow-записей, не содержащих фрагментированный трафик, при условии, что причина отправки равна active timeout, либо для netflow-записей, содержащих фрагментированный трафик с длительностью потока превышающей интервал детектирования.

Примечание. Указанное поведение может быть изменено путем редактирования конфигурационных файлов Комплекса. За подробной информацией необходимо обращаться в службу технической поддержки.

Если нетфлоу не парсится из-за ошибок, то в лог выводятся сообщения о статистике обнаруженных ошибочных датаграмм, которые можно отследить командой grep «Netflow parser stats»

4.1.3 Особенности учета трафика при выявлении DoS-атак

ПК «ПЕРИМЕТР» производит выявление аномалий трафика и учет трафика в аналитической подсистеме, используя flow-записи, для которых определен факт пересечения заданной в конфигурации виртуальной границы. Граница может быть глобальной (совпадает с границей контролируемой сети), а также, локальной для наблюдаемого объекта (использует индивидуальный набор интерфейсов).

При определении факта пересечения границы, для каждой flow-записи ПК «ПЕРИМЕТР» определяет направление трафика, основываясь на следующих характеристиках flow-записи:

- информация об интерфейсах маршрутизаторов (inbound ifIndex, outbound ifIndex);
- информация о принадлежности IP адресов адресному пространству контролируемой сети или наблюдаемому объекту (source IP, destination IP);
- расположение наблюдаемого объекта относительно контролируемой сети (внешний, внутренний).

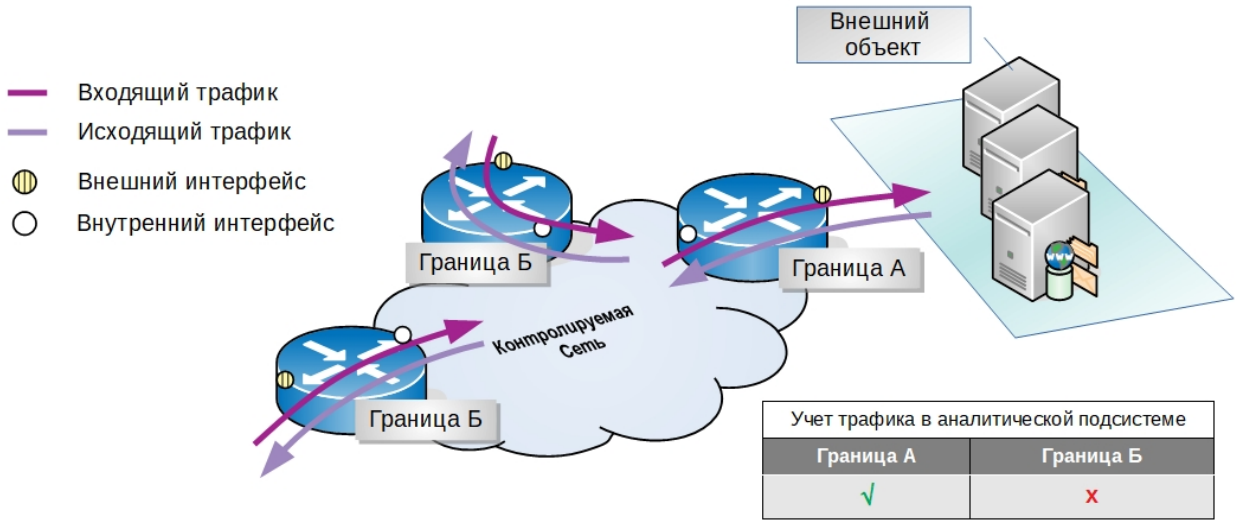

Рис. 3 Пересечение трафиком нескольких границ.

Для наблюдаемых объектов с внешним расположением ПК «ПЕРИМЕТР» выявляет аномалии трафика на двух виртуальных границах (Рисунок 33:

- Граница А — направление трафика, определенное по интерфейсам маршрутизаторов, указанных во flow-записи, не противоречит направлению трафика, определенному по IP адресам, указанным во flow-записи;
- Граница Б — существует противоречие между направлением трафика, определенным по интерфейсам маршрутизаторов, указанных во flow-записи, и определенным по IP адресам, указанным во flow-записи.

Для исключения двойного учета трафика в аналитической подсистеме учитывается только трафик на границе А. Выявление аномалий осуществляется одновременно на двух границах.

Возможные варианты расположения виртуальных границ в зависимости от расположения наблюдаемого объекта относительно контролируемой сети приведены в таблице 1

Таблица 1

Расположение объекта	Граница А	Граница Б
Внутренний	- вход трафика в контролируемую сеть по направлению к наблюдаемому объекту - выход трафика из контролируемой сети по направлению от наблюдаемого объекта	- вход трафика в контролируемую сеть по направлению от наблюдаемого объекта - выход трафика из контролируемой сети по направлению к наблюдаемому объекту
Внешний	- вход трафика в контролируемую сеть по направлению от наблюдаемого объекта - выход трафика из контролируемой сети по направлению к наблюдаемому объекту	- вход трафика в контролируемую сеть по направлению к наблюдаемому объекту - выход трафика из контролируемой сети по направлению от наблюдаемого объекта

4.1.4 Выявление аномалий по профилю поведения

Выявления аномалий по профилю поведения - это определение аномального поведения трафика на основе превышения пороговых значений количества и/или объёма трафика в рамках объекта в целом. Комплекс позволяет настроить как общие параметры выявления по профилю поведения, применяемые ко всем наблюдаемым объектам, так и индивидуальные параметры для каждого объекта. Пороговые значения могут задаваться как в ручном, так и автоматическом режимах. Информация о трафике наблюдаемого объекта для расчета пороговых значений формируется из данных, полученных по протоколу Netflow за предшествующие периоды.

Настройка глобальных параметров детектора по профилю поведения производится в разделе «Профили» меню «Администрирование / Детекция / Глобальные настройки». Для входа в режим настроек детектора по профилю поведения необходимо активировать детектор, переведя переключатель в разделе «Профили - Настройки по умолчанию» в положение «Включено», и нажать кнопку «Редактировать».

Настройка параметров детектирования по профилю поведения для наблюдаемого объекта производится в разделе «Настройки детектирования» вкладки «Детекция», доступной в режиме редактирования параметров наблюдаемого объекта, при этом, доступен режим «По умолчанию (использовать глобальные настройки)», который включает детектирование по профилю поведения с настройками, сконфигурированными глобально. Также доступен режим «Всегда включено», при выборе которого возможно индивидуальное конфигурирование параметров детектора для наблюдаемого объекта. Вход в режим редактирования пороговых значений осуществляется нажатием соответствующей кнопки. Для отключения выявления аномалий по профилю поведения выбранного наблюдаемого объекта необходимо воспользоваться режимом работы детектора «Всегда выключено».

Параметры детекторов могут быть заданы вручную, загружены из предварительно сохраненного шаблона настроек детектирования (кнопка «Загрузить из шаблона», а также сохранены

в виде шаблона (кнопка «Сохранить в шаблон»).

Для вступления в силу измененных параметров детектора необходимо нажать кнопку «Сохранить» на экране «Администрирование / Детекция / Глобальные настройки» при задании глобальных значений, или, в случае изменения параметров наблюдаемого объекта, на экране редактирования его параметров.

Примечание. При попытке использовать метод «По умолчанию» для настроек детектора наблюдаемого объекта, в случае если соответствующий детектор отключен в глобальных настройках детектирования, конфигурационный параметр будет сопровожден предупреждающей пиктограммой.

4.1.5 Выявление аномалий по шаблонным пакетам

Выявления аномалий по шаблонным пакетам - это определение аномального поведения трафика на основе превышения пороговых значений в рамках хостов наблюдаемых объектов, наблюдаемых объектов в целом и хостов, не принадлежащих наблюдаемым объектам, по отдельным типам пакетов, задаваемым сигнатурами DoS-атак. Комплекс позволяет настроить как общие параметры выявления по шаблонным пакетам, применяемые ко всем наблюдаемым объектам, так и индивидуальные параметры для каждого объекта. Пороговые значения могут задаваться как в ручном, так и автоматическом режимах. Информация о трафике наблюдаемого объекта для расчета пороговых значений формируется из данных, полученных по протоколу Netflow за предшествующие периоды.

Настройка глобальных параметров детектора по шаблонным пакетам производится в разделе «Шаблонные пакеты» меню «Администрирование / Детекция / Глобальные настройки». Параметры детектора для наблюдаемых объектов и для остальных хостов настраиваются независимо. Для входа в режим настроек детектора по шаблонным пакетам необходимо активировать детектор, переведя переключатель в разделе «Шаблонные пакеты - Настройки для хостов наблюдаемых объектов» или «Шаблонные пакеты - Настройки для остальных хостов» в положение «Включено», и нажать кнопку «Редактировать».

Настройка параметров детектирования по шаблонным пакетам для наблюдаемого объекта производится в разделе «Настройки детектирования» вкладки «Детекция», доступной в режиме редактирования параметров наблюдаемого объекта, при этом, доступен режим «По умолчанию (использовать глобальные настройки)», который включает детектирование по шаблонным пакетам с настройками, сконфигурированными глобально в разделе «Шаблонные пакеты - Настройки для хостов наблюдаемых объектов». Также доступен режим «Всегда включено», при выборе которого возможно индивидуальное конфигурирование параметров детектора для наблюдаемого объекта. Вход в режим редактирования пороговых значений осуществляется нажатием соответствующей кнопки. Для отключения выявления аномалий по шаблонным пакетам выбранного наблюдаемого объекта, необходимо воспользоваться режимом работы детектора «Всегда выключено».

Параметры детекторов могут быть заданы вручную, загружены из предварительно сохраненного шаблона настроек детектирования (кнопка «Загрузить из шаблона», а также сохранены в виде шаблона (кнопка «Сохранить в шаблон»).

Для вступления в силу измененных параметров детектора необходимо нажать кнопку «Сохранить» на экране «Администрирование / Детекция / Глобальные настройки» при задании глобальных значений, или, в случае изменения параметров наблюдаемого объекта, на экране редактирования его параметров.

Примечание. При попытке использовать метод «По умолчанию» для настроек детектора наблюдаемого объекта, в случае если соответствующий детектор отключен в глобальных настройках детектирования, конфигурационный параметр будет сопровожден предупреждающей пиктограммой.

При переключении детектора в режим «По умолчанию» из режима «Всегда включено», настройки детектора, заданные пользователем, не сохраняются и заменяются настройками по умолчанию.

4.1.6 Настройка параметров DoS-атак

DoS-атака имеет активное состояние пока существует хотя бы один активный вектор атаки. АПК «ПЕРИМЕТР» не завершает атаку сразу после окончания последнего вектора атаки. Атака остается активной в течении интервала времени, определенного параметром «Задержка закрытия DOS-атак», доступным через меню «Администрирование / Детекция / Глобальные настройки». Наличие задержки позволяет объединить в одну атаку векторы, активность которых имеет периодический характер.

Меню «Администрирование / Детекция / Глобальные настройки» содержит также параметр «Минимально допустимая глубина вычисления автопорога (секунд)», который позволяет определить временной интервал, за который необходимо иметь данные о трафике для расчета автоматических порогов. Если необходимые для расчета данные отсутствуют, то автоматические пороги не вычисляются, что предотвращает появление ложных DoS-атак.

Каждой выявленной DoS-атаке АПК «ПЕРИМЕТР» может сопоставить один из трех классов опасности. Класс опасности определяется по максимальному относительному превышению выявленного значения трафика атаки относительно порогового значения. Глобальное определение классов опасности настраивается через меню «Администрирование / Детекция / Глобальные настройки» в разделе «Классы опасности». Относительные превышения задаются в процентах.

5 Аннотации к аномалии

Аннотация - это шаблон комментария к DoS-аномалиям. Аннотации позволяют ускорить и упростить работу с аномалиями, уменьшить количество ошибок и стандартизировать комментарии.

Все аннотации к аномалиям содержатся на странице аннотаций к аномалиям «Администрирование / Детекция / Аннотации к аномалиям». Данные представлены в виде таблицы со следующими столбцами:

Столбец	Описание
Название	Название аннотации
Текст	Текст аннотации

Аннотации к аномалиям используются для упрощения написания комментариев при изучении детальной информации по аномалиям.

6 Работа с наблюдаемыми объектами

Наблюдаемый объект - это совокупность физических объектов сети и трафика, рассматриваемая анализатором как единый объект. Наблюдаемые объекты задаются для осуществления мониторинга трафика данных объектов и выявления в нем аномального поведения.

После создания наблюдаемого объекта, данные протокола NetFlow сопоставляются с его конфигурацией и, в случае соответствия, дополняют статистику и участвуют в выявлении аномалий по данному объекту. Наблюдаемые объекты могут быть как глобальные, так и локальные. Под глобальными понимаются те объекты, сопоставление трафика с которыми выполняется на всех анализаторах. Под локальными понимаются объекты, привязанные к конкретному анализатору.

Примечание. Если объект привязан к анализатору, трафик объекта учитывается только на указанном анализаторе, иначе он учитывается на всех анализаторах и суммируется при просмотре отчётов. Аномалии по объекту детектируются по суммарному трафику, полученному со всех анализаторов.

В системе работа осуществляется со следующими типами объектов:

- «Клиент» - наблюдаемый объект, используемый для контроля трафика элементов, расположенных внутри контролируемой сети. Как правило это клиенты оператора связи и различные его сервисы;
- «Профиль» - универсальный наблюдаемый объект, используемый для контроля трафика элементов, расположенных как внутри контролируемой сети, так и вне ее. Также данный объект можно использовать для отслеживания трафика определенного типа;
- «Сосед» - наблюдаемый объект, представляющий внешнюю сеть передачи данных, непосредственно подключенную к контролируемой сети;
- «Червь» - наблюдаемый объект, предназначенный для контроля трафика сети, заданного сигнатурой. Как правило данный объект применяется для отслеживания трафика, используемого вредоносными ПО.

Примечание: автоматический запуск подавления атак разрешен только для наблюдаемого объекта «Клиент».

Все наблюдаемые объекты, сконфигурированные в системе, доступны на странице «Администрирование / Мониторинг / Наблюдаемые объекты / Все».

На экране присутствуют: фильтр выбора объектов и информация по ним.

Информация по объектам отображена в виде таблицы со следующими полями:

- название - название наблюдаемого объекта;
- тип - тип наблюдаемого объекта;
- конфигурация объекта - критерии, определяющие конфигурацию наблюдаемого объекта;
- граница - тип задания виртуальной границы наблюдаемого объекта;
- теги - набор именованных маркеров, позволяющих быстро отбирать сходные группы наблюдаемых объектов;
- анализатор - имя анализатора к которому привязан объект. В случае если анализатор удален или неизвестен, в поле будет отображена информация об этом факте;

- описание (дополнительное поле) - описание наблюдаемого объекта.

Фильтр позволяет отбирать наблюдаемые объекты по части названия объекта, описание объекта или конфигурация объекта; по типу объекта; по анализатору, к которому привязаны объекты; по тегам объекта. Флаг «Использовать PCRE», при установке которого в текстовые поля фильтра можно вводить регулярные выражения в формате PCRE.

На данном экране присутствует возможность удаления объектов. Для удаления необходимо установить флажок в строке с выбранным объектом и нажать кнопку «Удалить выбранные».

6.1 Общие элементы конфигурации

6.1.1 Расположение объекта

Расположение наблюдаемого объекта определяется относительно виртуальной границы контролируемой СПД и влияет на определенное системой направление трафика. Предусмотрены два типа расположения наблюдаемого объекта: внутренний и внешний.

По умолчанию анализатор классифицирует наблюдаемый объект типа клиент как внутренний, наблюдаемые объекты типов «профиль» и «сосед» - как внешние. Наблюдаемый объект типа «червь» анализатором не классифицируется.

6.2 Наблюдаемый объект типа «клиент»

Наблюдаемый объект типа «клиент» предназначен для контроля трафика элементов, расположенных внутри контролируемой сети. Как правило это клиенты оператора связи и различные его сервисы.

Все наблюдаемые объекты типа «клиент» содержатся на странице наблюдаемых объектов типа «клиент» «Администрирование / Мониторинг / Наблюдаемые объекты / Клиенты». Данные представлены в виде таблицы со следующими полями:

- название наблюдаемого объекта;
- конфигурация наблюдаемого объекта;
- граница - тип задания виртуальной границы объекта;
- теги - набор именованных маркеров, позволяющих быстро отбирать сходные группы наблюдаемых объектов;
- анализатор - модуль анализатор, к которому привязан наблюдаемый объект;

а также дополнительными полями:

- описание наблюдаемого объекта;
- шаблоны детектирования - связанные с объектом шаблоны детектирования DoS-атак по шаблонным пакетам и по профилю поведения;
- автоподавление - состояние автоматического подавления атак для наблюдаемого объекта;
- шаблоны подавления - шаблоны подключения и настройки методов, связанные с объектом;

- дочерние объекты - список дочерних объектов;
- расположение - логическое положение объекта относительно контролируемой сети.

6.3 Наблюдаемый объект типа «профиль»

Наблюдаемый объект типа «профиль» предназначен для мониторинга трафика и выявления аномалий в подсетях контролируемой сети передачи данных или любой другой сети, а также на сетевых сервисах.

Вся работа с наблюдаемыми объектами типа «профиль» производится на странице интерфейса «Администрирование / Мониторинг / Наблюдаемые объекты / Профили». Данные по объектам представлены в виде таблицы со следующими полями:

- название наблюдаемого объекта;
- конфигурация наблюдаемого объекта;
- граница - тип задания виртуальной границы объекта;
- теги - набор именованных маркеров, позволяющих быстро отбирать сходные группы наблюдаемых объектов;
- анализатор - модуль анализатор, к которому привязан наблюдаемый объект;

а также дополнительными полями:

- описание наблюдаемого объекта;
- шаблоны детектирования - связанные с объектом шаблоны детектирования DoS-атак по шаблонным пакетам и по профилю поведения;
- автоподавление - состояние автоматического подавления атак для наблюдаемого объекта;
- шаблоны подавления - шаблоны подключения и настройки методов, связанные с объектом;
- дочерние объекты - список дочерних объектов;
- расположение - логическое положение объекта относительно контролируемой сети.

Работа с наблюдаемым объектом типа «профиль» полностью аналогична работе с наблюдаемым объектом типа «клиент», за исключением настройки подавления атак. Объект «профиль» не может быть использован для автоматического подавления атак.

6.4 Наблюдаемый объект типа «червь»

Наблюдаемые объекты типа «червь» предназначены для выявления вредоносного трафика и степени его влияния на контролируемую сеть передачи данных.

Вся работа с объектами типа «червь» производится на странице интерфейса «Администрирование / Мониторинг / Наблюдаемые объекты / Черви».

Данные представлены в виде таблицы со следующими полями:

- название наблюдаемого объект;
- конфигурация наблюдаемого объекта;

- теги - набор именованных маркеров, позволяющих быстро отбирать сходные группы наблюдаемых объектов;
- анализатор, к которому привязан наблюдаемый объект;
- описание (дополнительное поле).