kaspersky

Kaspersky DDoS Prevention+

Клиентский портал User Guide

ООО «Модель защиты», 100% дочерняя
компания АО «Лаборатория Касперского»

22.04.2022

kaspersky

Оглавление

kaspersky

Введение

Данный документ предназначен для пользователей клиентского портала решения Kaspersky DDoS Prevention+ (или KDP+) и освещает основные механизмы работы и элементы интерфейса, с помощью которых пользователь может управлять и получать информацию о защищаемых ресурсах, просматривать информацию об обнаруженных DDoS-атаках. Для доступа к порталу необходимо иметь активированную лицензию KDP+ и пройти процедуру подключения, по запросу на support@kdp.zone

Глоссарий

Kaspersky DDoS Prevention+	Программное обеспечение, предназначенное для обнаружения и фильтрации DDoS-атак.
DDoS-атака, атака	Распределенная атака на вычислительную систему, выполняемая одновременно с большого числа компьютеров с целью довести вычислительную систему до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен.
Защищаемый ресурс	Сетевой сервис Клиента, определяемый IP-адресом или IP-адресами, в отношении которого оказывается услуга
Личный кабинет, Портал	Компонент Системы, представляющий собой web-приложение, посредством которого сотрудник Клиента взаимодействует с Системой.
Служба эксплуатации KDP	Технический персонал Исполнителя, непосредственно работающий с Системой, занятый в подключении новых Клиентов и обслуживании существующих Клиентов, отражении атак и проведении их анализа.

kaspersky

Назначение Системы

Что такое Kaspersky DDoS Prevention+

Kaspersky DDoS Prevention+ – решение, которое позволяет защитить ресурсы Клиента от DDoS-атак путем перенаправления пользовательского трафика на Центры очистки Исполнителя.

Назначение Системы — обнаружение DDoS-атак, а также очистка (фильтрация) трафика путем выявления и блокирования паразитного трафика, результатом чего является снижение нагрузки на атакуемый ресурс.

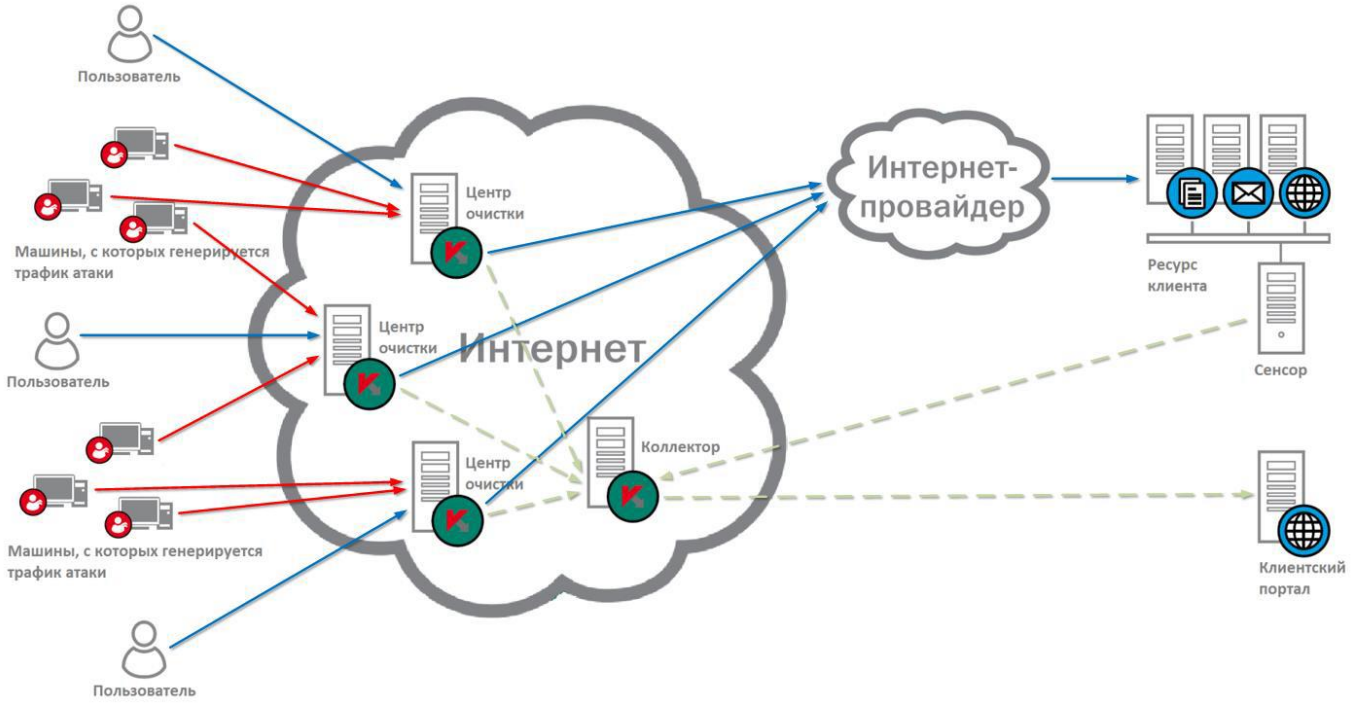
Какие задачи решает Kaspersky DDoS Prevention+

В ходе работы Система выполняет следующие функции:

- Собирает статистические параметры трафика Защищаемых ресурсов;
- Осуществляет построение профилей легитимного трафика Защищаемых ресурсов и вырабатывает на их основе правила обнаружения аномалий и атак;
- Производит мониторинг возникновения аномалий и атак в трафике Защищаемых ресурсов;
- Осуществляет фильтрацию трафика Защищаемых ресурсов, перенаправленного через Центр очистки, от паразитной составляющей;

Выполняет вспомогательные задачи, обеспечивающие работу перечисленных функций.

Схема работы Системы



Коллектор представляет собой программно-аппаратный комплекс, обеспечивающий сбор и обработку информации о трафике от других программных компонентов Системы, в том числе применение критериев обнаружения аномалий и атак, критериев фильтрации. Назначение Коллектора — обмен информацией о трафике и служебной информацией между всеми программными компонентами Системы.

Центр очистки представляет собой компонент Системы, который осуществляет анализ и фильтрацию проходящего через него трафика сетевых ресурсов Клиента. Располагается на независимой, физически удаленной (от оборудования Клиента) площадке Исполнителя. Назначение Центра очистки — очистка перенаправленного трафика от паразитной составляющей и его доставка до Защищаемых ресурсов. Все Центры очистки объединены в единую распределенную систему.

Сенсор собирает информацию о трафике, направленном к ресурсу Клиента, и агрегирует ее для предоставления Коллектору.

Личный кабинет (Портал) представляет собой web-приложение, через которое Администратор Клиента взаимодействует с Системой. Портал работает с базой данных Коллектора, наполняющейся в ходе работы Системы. Эта база данных служит источником данных для пользователей Портала.

Классификация DDoS-атак

Все DDoS-атаки можно разделить на два типа:

- Атака на полосу пропускания, когда злоумышленник действует путем наполнения каналов связи, выделенных полос пропускания и оборудования большим количеством пакетов.
- Атака на приложения, когда злоумышленник, эксплуатируя особенности поведения протоколов взаимодействия ЭВМ (TCP, HTTP и т.п.), а также поведения сервисов и приложений, захватывает вычислительные ресурсы ЭВМ, на которой функционирует объект атаки, что не позволяет этому объекту обрабатывать легитимные транзакции и запросы.

Системой различаются следующие виды атак:

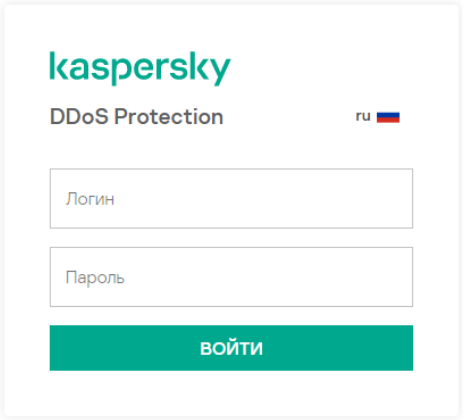
Вид	Описание
Mixed	Смешанная атака, имеющая признаки атак обоих типов.
TCP short packet	Атака короткими пакетами по протоколу TCP. Нацелена на переполнение канала связи или исчерпание ресурсов TCP-стека жертвы.
TCP Data	Атака длинными пакетами по протоколу TCP, как правило, без установки соединения. Нацелена на переполнение канала связи.
UDP	Атака по протоколу UDP, как правило, большими пакетами. Нацелена на переполнение канала связи.
ICMP	Атака по протоколу ICMP, как правило, большими пакетами. Нацелена на переполнение канала связи.
HTTP flood	Атака по протоколу HTTP. Нацелена на перегрузку сервера в целом или приложения, обрабатывающего HTTP запросы.
Connect flood	Установка множества соединений без передачи или с медленной передачей данных с целью исчерпать ресурсы TCP-стека жертвы.

Работа с Порталом Kaspersky DDoS Prevention+

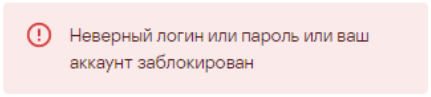
Авторизация пользователя

Для пользования Порталом **Kaspersky DDoS Prevention+** необходимо авторизоваться в Системе. Для авторизации выполните следующие действия:

- Введите в адресной строке браузера адрес Портала **Kaspersky DDoS Prevention+**:
  Откроется страница входа:



- Введите логин и пароль в соответствующие поля и нажмите **Войти**.
  - Если логин или пароль не введен или если введен неверный логин или пароль появляется следующее сообщение:

    Это же сообщение выводится, если страница авторизации долго оставалась открытой, но никакие действия на ней не производились. В этом случае нужно повторно ввести пароль и нажать кнопку Войти.
  - Если логин и пароль введены правильно, открывается одна из страниц интерфейса.
    При первом входе в систему пользователю необходимо сменить пароль.

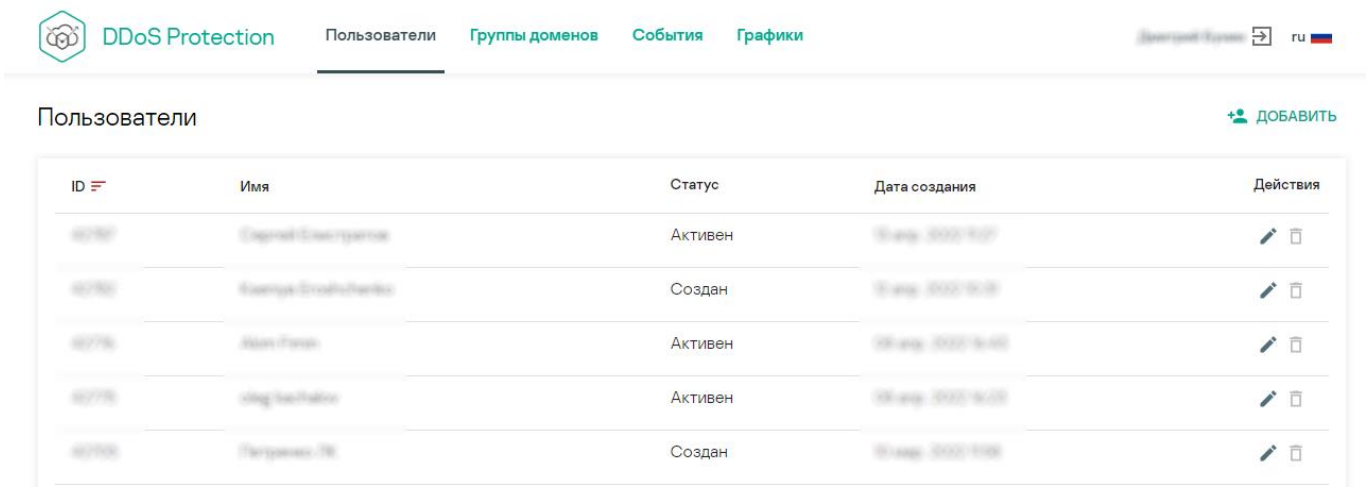
Работа с пользователями

Изменение личных данных пользователя

Чтобы изменить личные данные пользователя, нажмите **Пользователи** в главном меню;

В меню **Пользователи** можно производить сортировку по столбцам:

- ID;
- Имя пользователя;
- Статус;
- Дата создания.



Найдите пользователя в списке и нажмите на значок редактировать в соответствующей строке. На появившейся странице можно изменить данные пользователя:

- Имя пользователя;
- Адрес электронной почты;
- Язык;
- Телефон;
- Временную зону;
- Пароль;
- Комментарий;
- Заблокировать пользователя;

Любые введенные изменения сохраняются после нажатия кнопки **Сохранить**. При нажатии **сохранить** введенные значения проверяются; при обнаружении некорректных данных или отсутствии обязательных данных выдается предупреждение, и форма остается открытой.

Чтобы закрыть форму, не изменяя данных пользователя, перейдите по ссылке лиц в нижней части страницы.

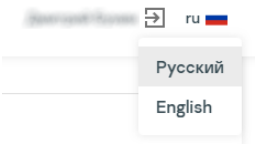
Удаление пользователя

Чтобы удалить существующего пользователя, нажмите **Пользователи** в главном меню.

Найдите пользователя в списке и нажмите на кнопку удалить в соответствующей строке. Появится всплывающее окно со следующим предупреждением:

Изменение языка интерфейса Портала

Для переключения языка интерфейса системы Kaspersky DDOS Prevention воспользуйтесь выпадающим списком в верхнем правом углу:



kaspersky

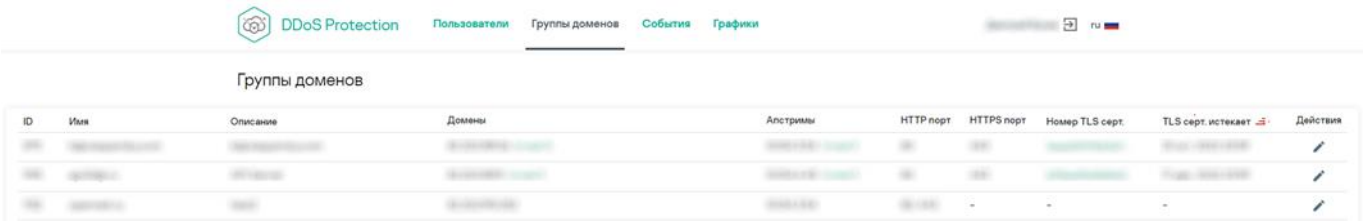
Работа с защищаемыми ресурсами

Чтобы перейти в раздел по работе с ресурсами, нажмите **Группы доменов** в главном меню.

Вам отобразится таблица со списком групп доменов доступных для управления.

Список можно сортировать по колонкам:

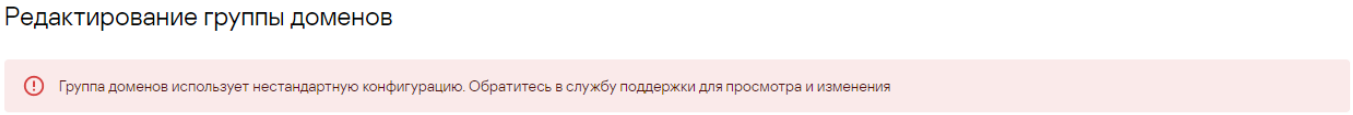
- ID
- Имя
- Описание
- Номер TLS сертификата
- Срок истечения TLS сертификата



Редактирование защищаемых ресурсов

Что бы перейти к редактированию ресурса, нажмите **Группы доменов** в главном меню, выберете необходимую Группу доменов и нажмите кнопку редактировать в соответствующей строке.

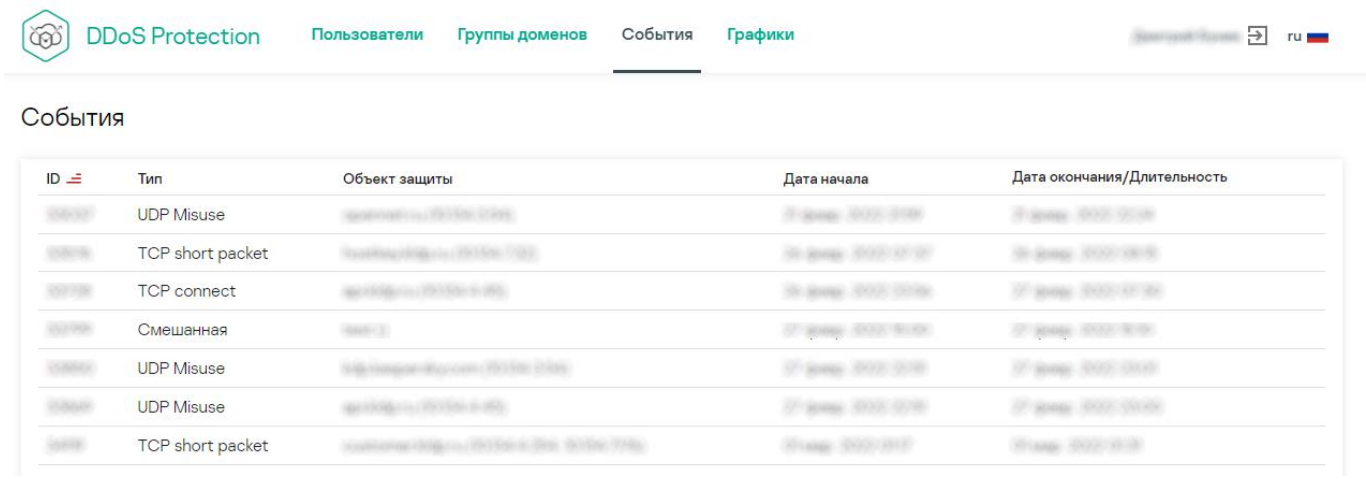
Если ресурс имеет не стандартную конфигурацию, к сожалению редактирование будет не возможно, о чем вы получите сообщение.



Работа с Атаками

Чтобы перейти в раздел по работе с атаками, нажмите События в главном меню. Вам будет отображена таблица со списком атак на все защищаемые ресурсы. Список возможно сортировать по следующим полям:

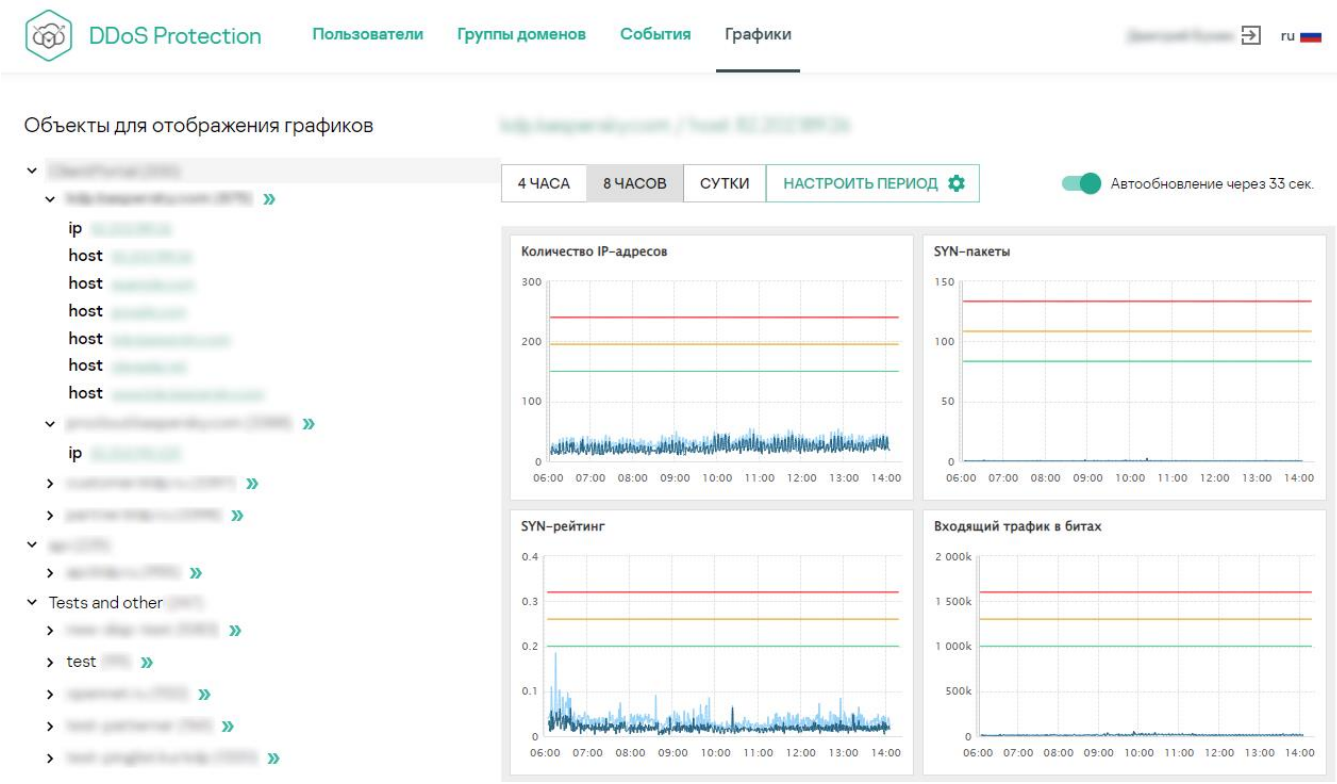
- ID
- Тип
- Объект защиты
- Дата начала



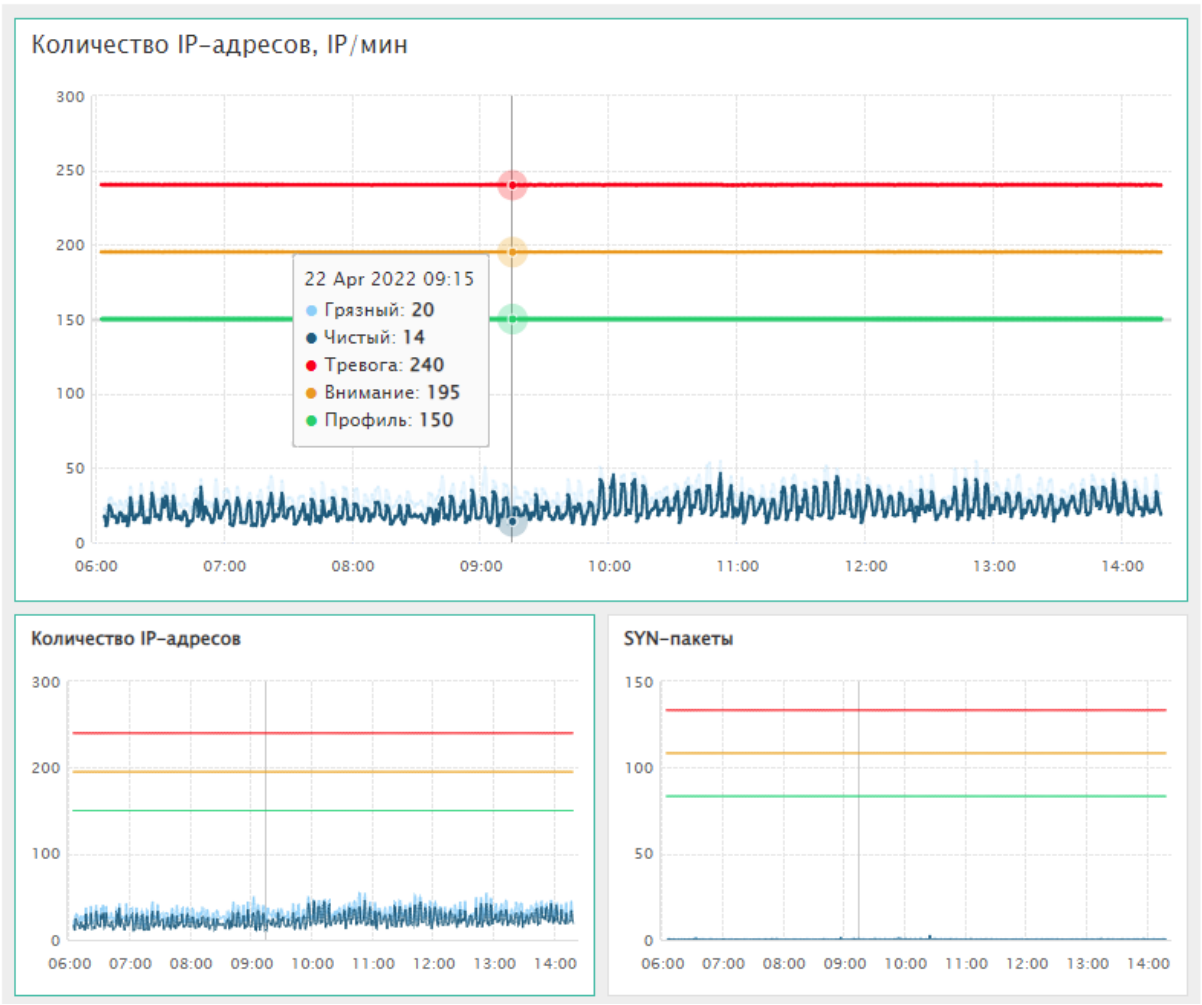
Работа с графиками

Для просмотра графиков измеряемых параметров защищаемых ресурсов нажмите **Графики** в главном меню. Вам будет отображена страница со списком объектов для отображения графиков в левой части и сами графики в правой части. Для отображения доступны следующие типы измеряемых параметров:

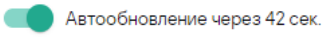
- Количество IP-адресов;
- SYN-пакеты;
- SYN-рейтинг;
- Входящий трафик в битах;
- Входящий трафик в пакетах;
- Исходящий трафик в битах;
- Исходящий трафик в пакетах;
- Входящий UDP-трафик;
- Входящий ICMP-трафик;
- Входящий TCP-траифик;
- HTTP запросы;
- HTTPS запросы;



Набор измеряемых параметров может изменяться от ресурса к ресурсу, в зависимости от связанных с ними настроек Системы. Чтобы увеличить виджет, нажмите на него, и он появится в области над графиками в увеличенном масштабе:



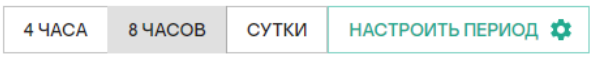
При наведении курсора на график в области редактирования отображается значение параметра в конкретной точке. На странице производится авто обновление графиков раз в 1мин, его можно отключить переключателем в области редактирования:



Задание периода построения графиков и диаграмм

Чтобы задать период построения графиков измеряемых параметров ресурса в области редактирования над графиком выберите длительность промежутка отображения из возможных значений:

- 4 часа;
- 8 часов;
- Сутки.



Либо по нажатию кнопки **Настроить период** задайте положение промежутка в форме:

Графики на всех виджетах будут перестроены автоматически. Общие сведения о данных, отображаемых в интерфейсе

На графике любого измеряемого параметра синей линией отображаются реальные значения трафика. Если для данного параметра задано ведение профиля (это настраивается индивидуально для каждого параметра и каждого ресурса сотрудниками Службы эксплуатации KDP), то отображаются также:

- Зеленая линия – нормальный уровень;
- Желтая линия – уровень внимания;
- Красная линия – уровень тревоги.

При прохождении трафика Защищаемого ресурса через центры очистки на графике отображаются также величины параметра для трафика до фильтрации – голубые линии.

Выход из системы

1. Кнопка расположена в правой верхней части страницы.
2. При нажатии на кнопку «Выйти» осуществляется выход из интерфейса Партнерского портала.