NetPolice.ru

Инструкция по установке NetPolice Pro на компьютер с установленными антивирусами Dr.Web, Avast либо Kaspersky

Если на компьютере установлен антивирус Kaspersky

Для правильного функционирования программы NetPolice Pro необходимо в настройках антивируса Kaspersky отключить компонент «Веб-контроль». Сделать это можно либо в "политиках" центральной консоли управления Kaspersky, либо, в случае локальной установки - на компьютере в настройках антивируса.

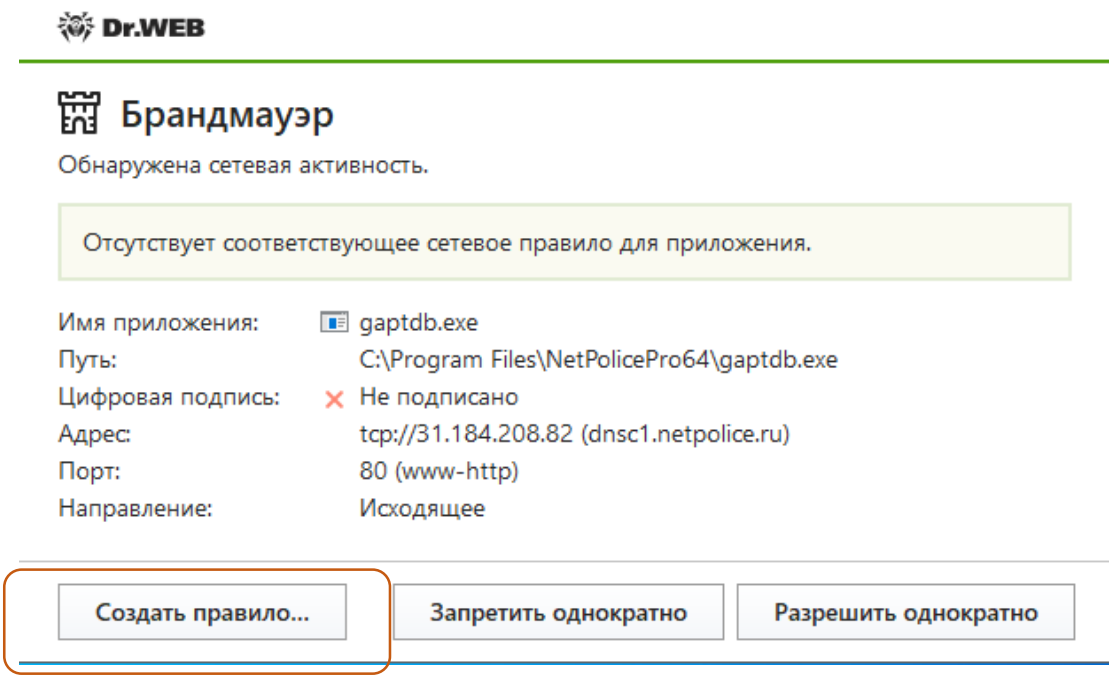
Компонент «Веб-контроль» должен оставаться неактивным во время использования фильтров NetPolice.

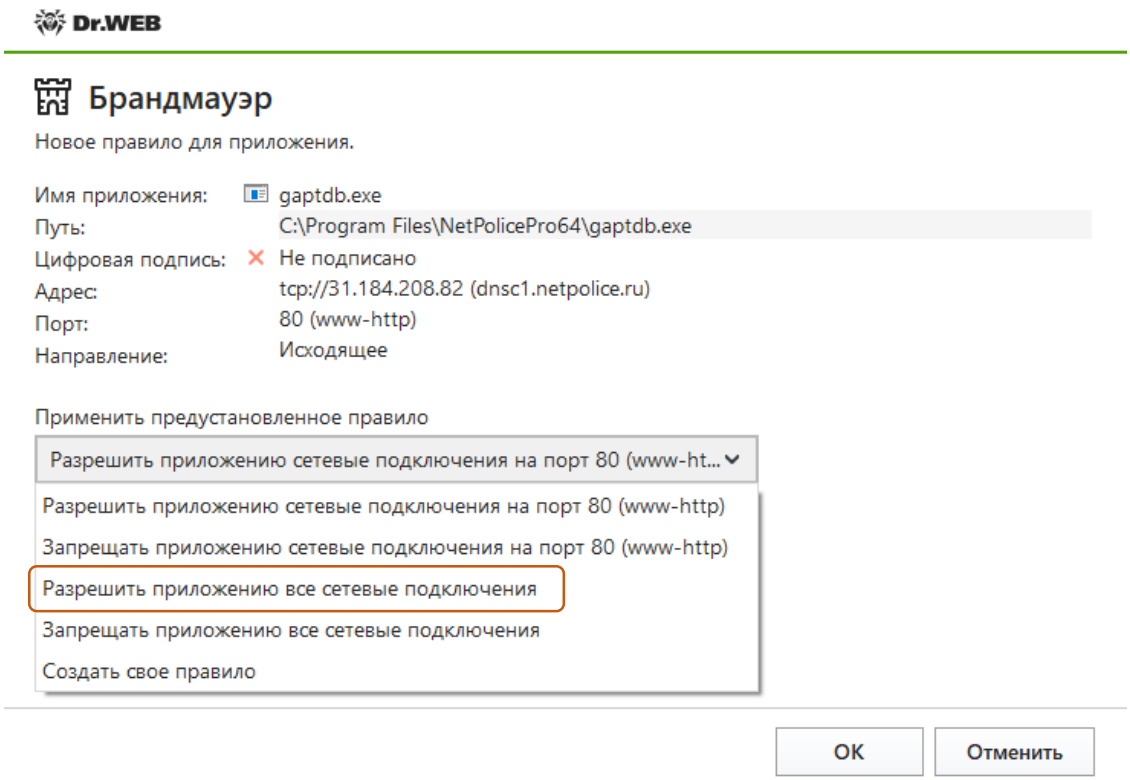
Если на компьютере установлен антивирус Avast

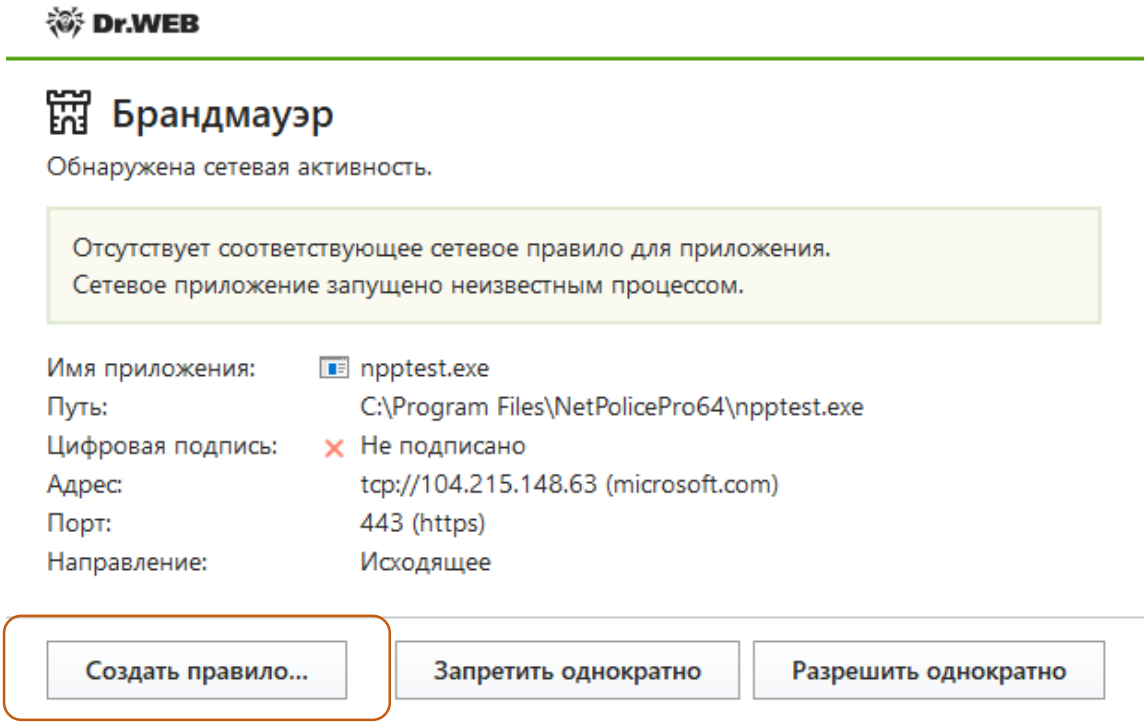
Рекомендуем перед установкой NetPolice Pro временно приостановить работу антивируса Avast. Для этого кликните правой кнопкой мыши по значку Avast на панели уведомлений. В открывшемся меню выберите «Управление экранами Avast», далее выберите «Отключить на 10 минут».

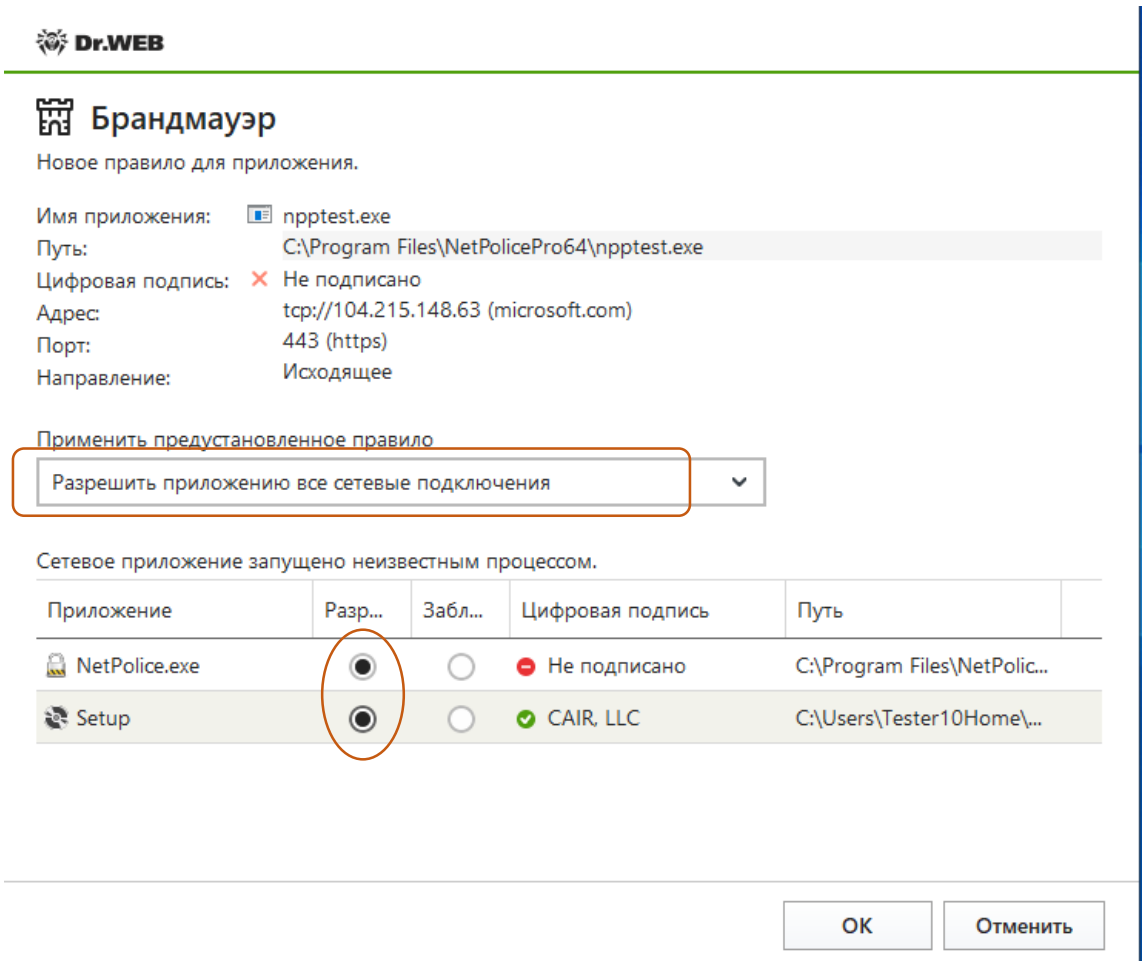
Если на компьютере установлен антивирус Dr.Web

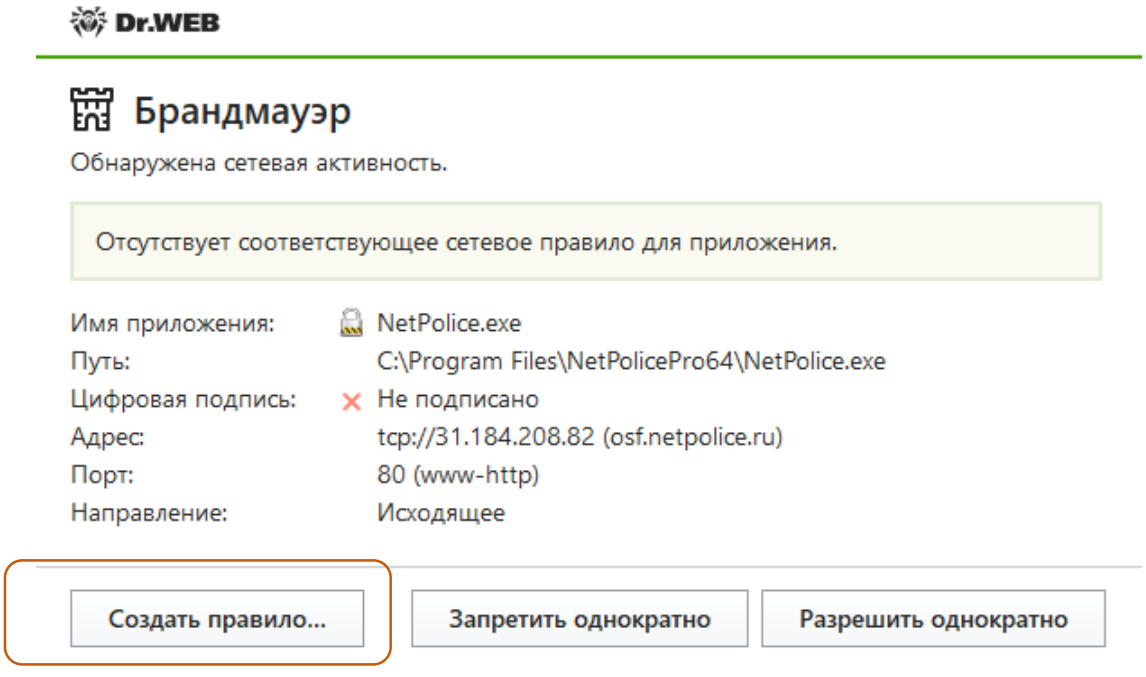
Во время установки NetPolice Pro, Dr.Web будет выдавать диалоговые окна. Выберите точно такие же настройки, как на приведенных ниже снимках экранов.

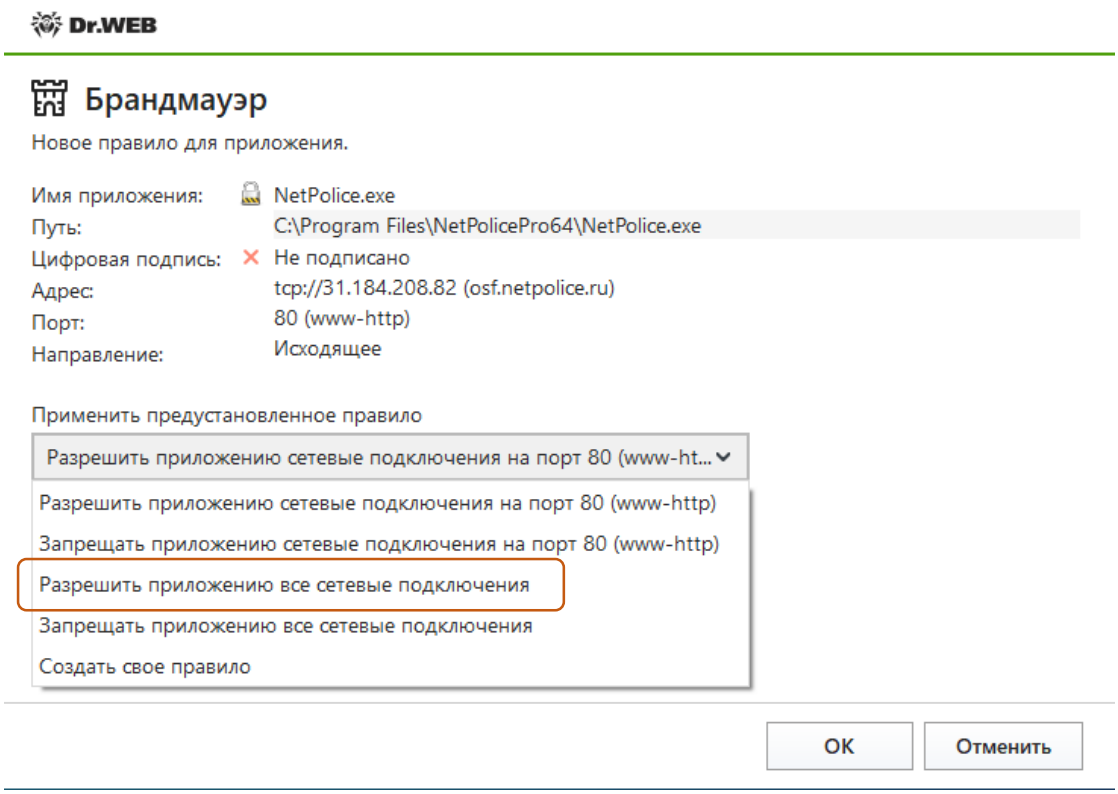



Dr.WEB
Брандмауэр
Новое правило для приложения.
Имя приложения: gaptdb.exe
Путь: C:\Program Files\NetPolicePro64\gaptdb.exe
Цифровая подпись: Не подписано
Адрес: tcp://31.184.208.82 (dnsc1.netpolice.ru)
Порт: 80 (www-http)
Направление: Исходящее
Применить предустановленное правило
Разрешить приложению сетевые подключения на порт 80 (www-ht...
Разрешить приложению сетевые подключения на порт 80 (www-http)
Запрещать приложению сетевые подключения на порт 80 (www-http)
Разрешить приложению все сетевые подключения
Запрещать приложению все сетевые подключения
Создать свое правило
OK
Отменить


Dr.WEB
Брандмауэр
Обнаружена сетевая активность.
Отсутствует соответствующее сетевое правило для приложения.
Сетевое приложение запущено неизвестным процессом.
Имя приложения: npptest.exe
Путь: C:\Program Files\NetPolicePro64\npptest.exe
Цифровая подпись: Не подписано
Адрес: tcp://104.215.148.63 (microsoft.com)
Порт: 443 (https)
Направление: Исходящее
Создать правило...
Запретить однократно
Разрешить однократно


Dr.WEB
Брандмауэр
Новое правило для приложения.
Имя приложения: nptest.exe
Путь: C:\Program Files\NetPolicePro64\nptest.exe
Цифровая подпись: Не подписано
Адрес: tcp://104.215.148.63 (microsoft.com)
Порт: 443 (https)
Направление: Исходящее
Применить предустановленное правило
Разрешить приложению все сетевые подключения
Сетевое приложение запущено неизвестным процессом.
Приложение
Разр...
Забл...
Цифровая подпись
Путь
NetPolice.exe
Не подписано
C:\Program Files\NetPolic...
Setup
CAIR, LLC
C:\Users\Tester10Home\...
OK
Отменить


Dr.WEB
Брандмауэр
Обнаружена сетевая активность.
Отсутствует соответствующее сетевое правило для приложения.
Имя приложения: NetPolice.exe
Путь: C:\Program Files\NetPolicePro64\NetPolice.exe
Цифровая подпись: Не подписано
Адрес: tcp://31.184.208.82 (osf.netpolice.ru)
Порт: 80 (www-http)
Направление: Исходящее
Создать правило...
Запретить однократно
Разрешить однократно



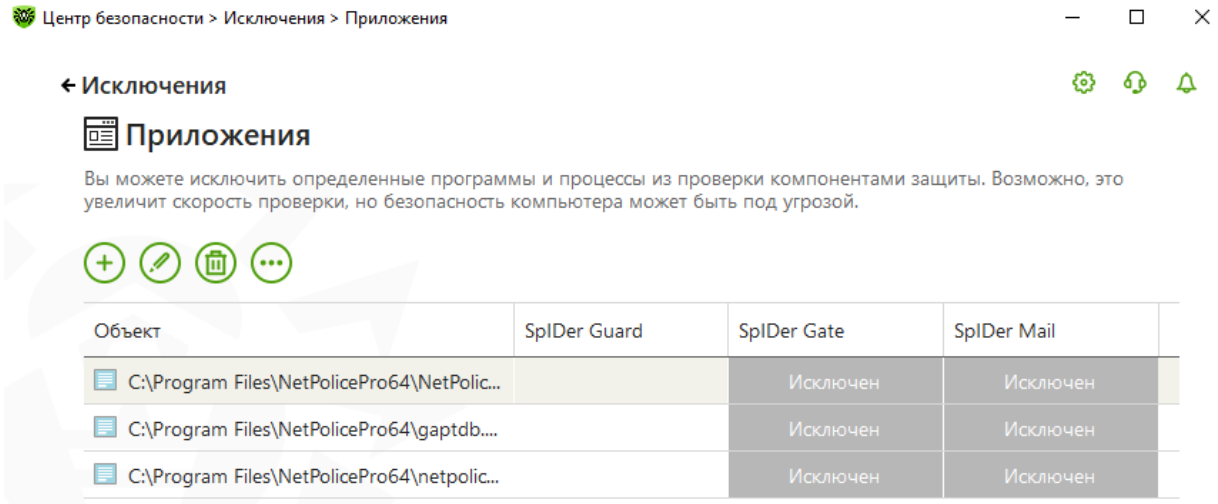
После установки NetPolice, зайдите в настройки антивируса и выставите правило, как на приведенном ниже снимке экрана:

Необходимо добавить следующие процессы NetPolice:

C:\Program Files\NetPolicePro64\gaptdb.exe

C:\Program Files\NetPolicePro64\NetPolice.exe

C:\Program Files\NetPolicePro64\netpolice_s.exe



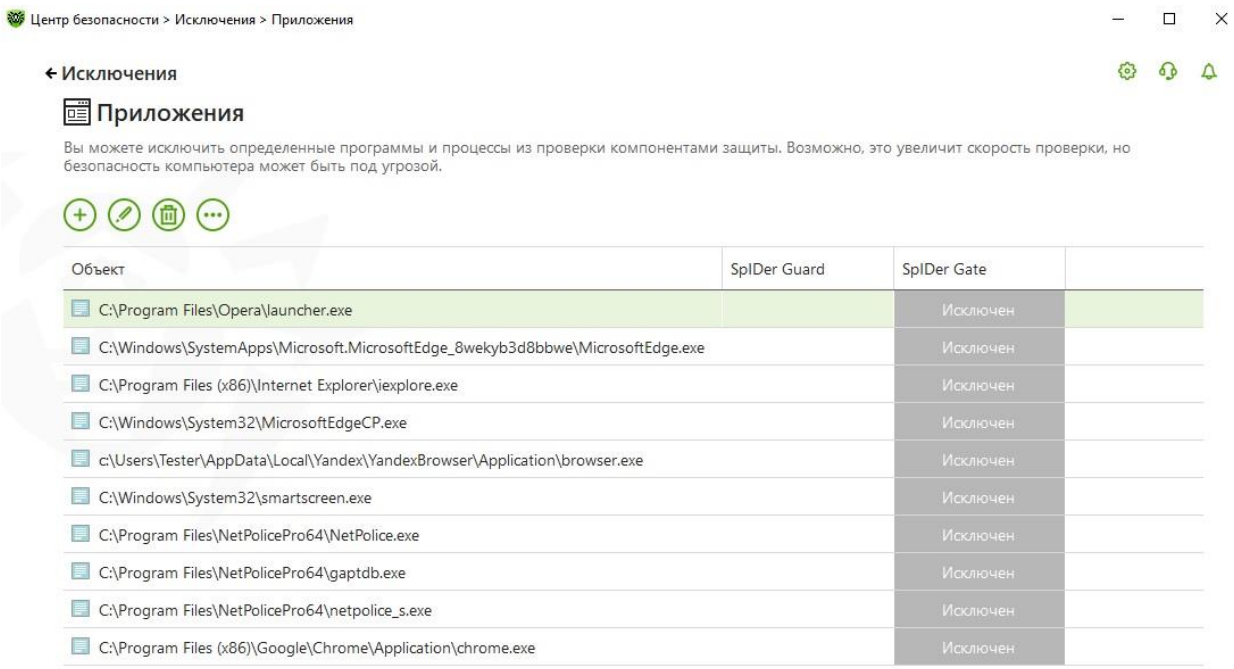
После этого необходимо аналогичным образом добавить в исключения исполняемые файлы браузеров Opera, Yandex, Chrome и т.д.

Для работы в браузере Edge также необходимо добавить процессы:

C:\Windows\System32\smartscreen.exe

C:\Windows\System32\MicrosoftEdgeCP.exe

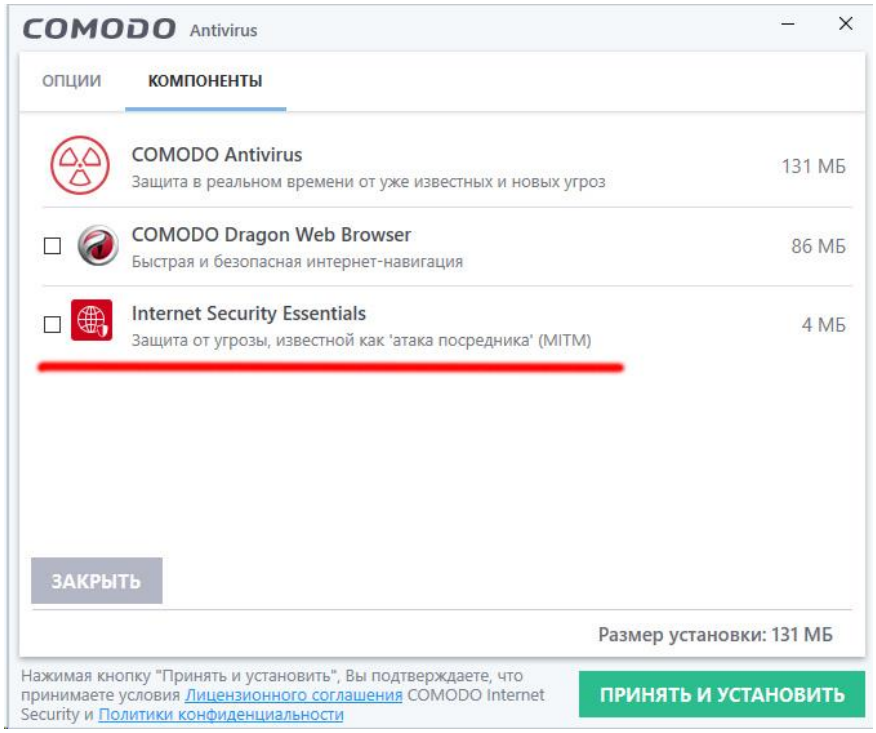
Как на снимке экрана, приведенном ниже:



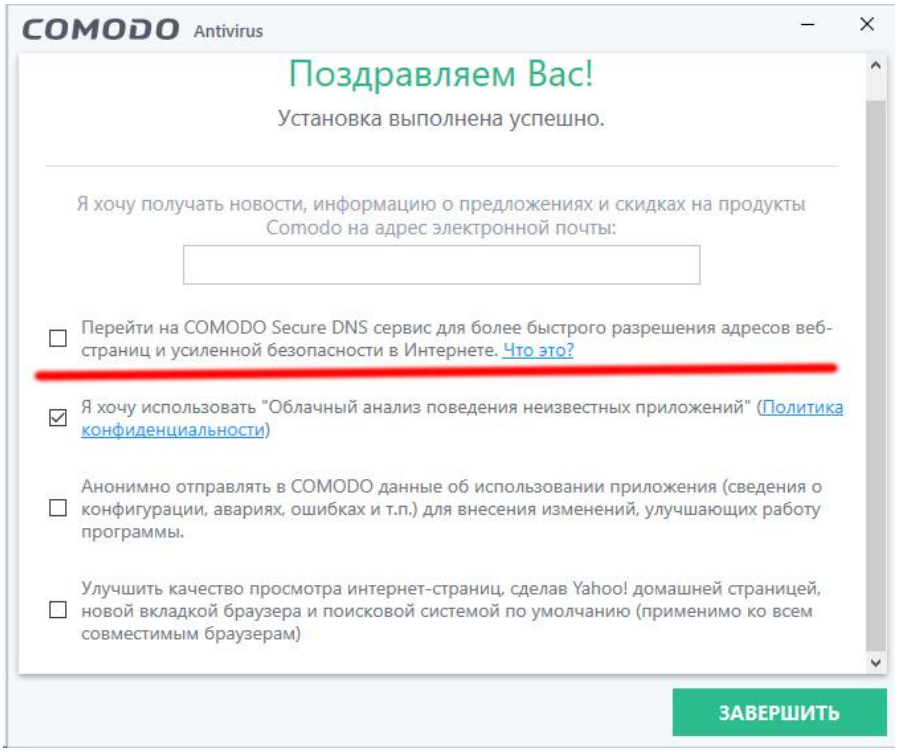
После внесения изменений перезагрузите операционную систему.

Инструкция по настройке антивируса COMODO для совместного использования с NETPOLICE Pro/Child

1. При установке антивируса **необходимо отключить установку компонента «Защита от MITM»** ! (снять галочку)



2. На последнем окне установки, в конце, **отключить галочку "Использовать Comodo Secure DNS"**



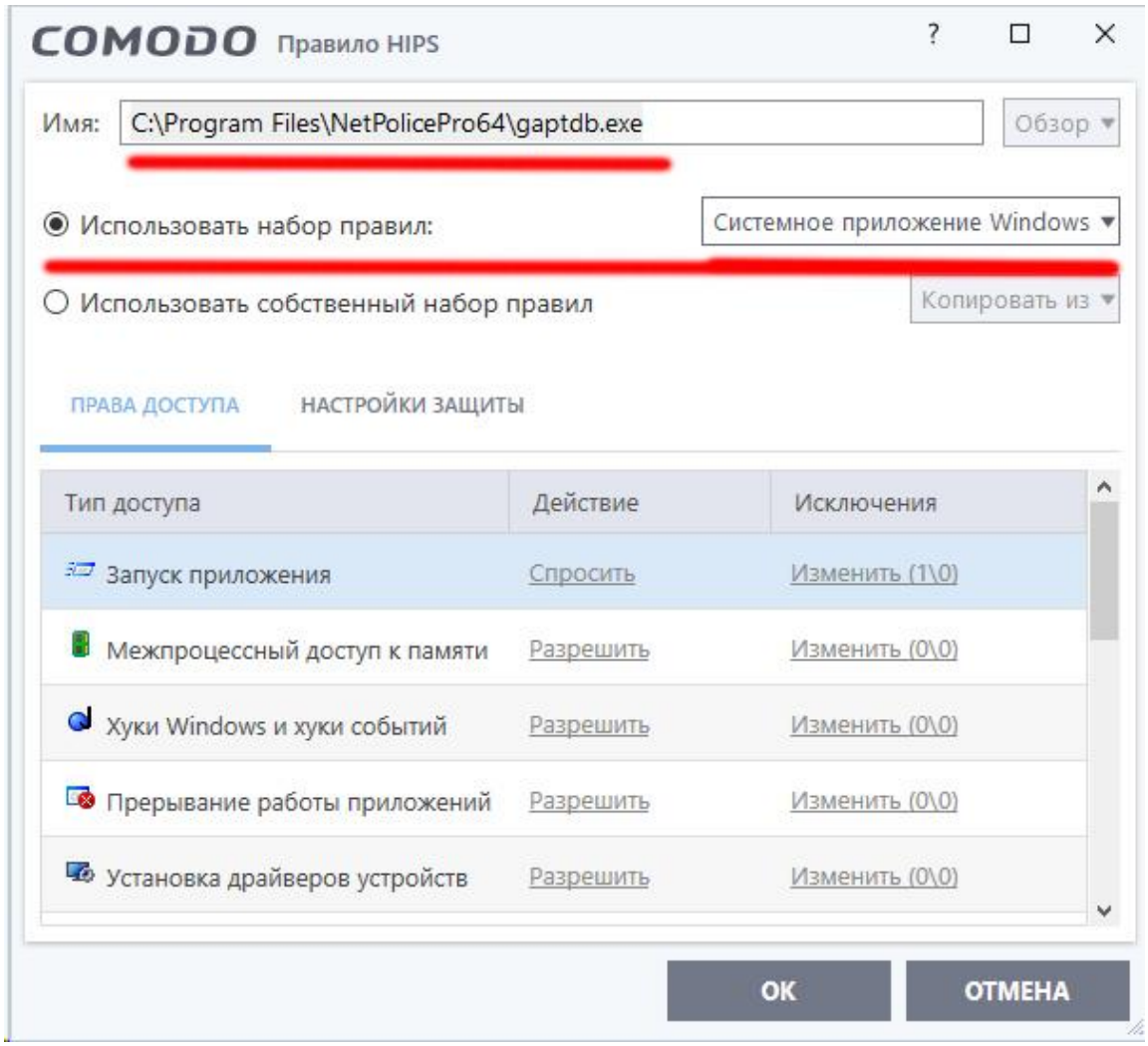
3. В настройках антивируса, если Вы используете компонент HIPS, необходимо добавить следующие строки (приложения):
   Настройки -> HIPS -> Правила HIPS -> Добавить

Обзор->Приложения:

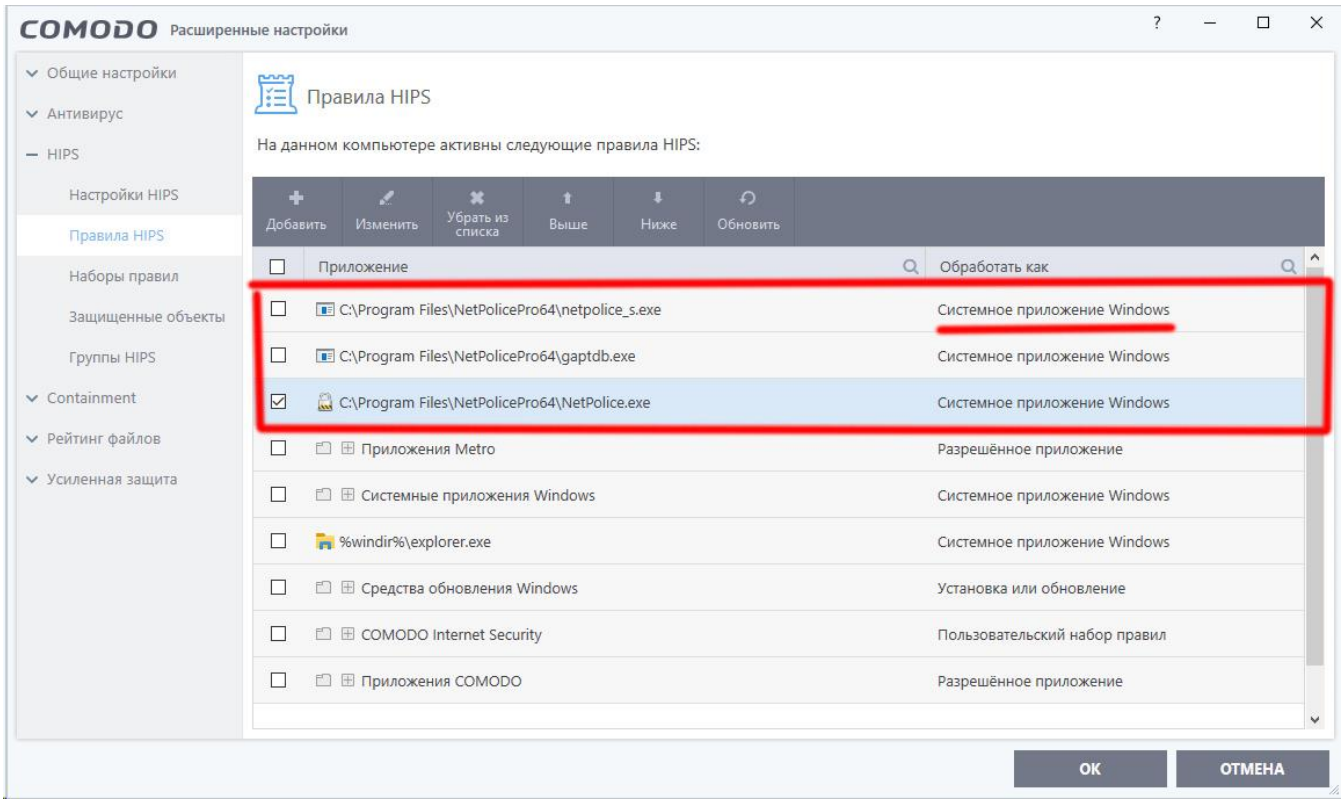
C:\Program Files\NetPolicePro64\NetPolice.exe
C:\Program Files\NetPolicePro64\gaptdb.exe
C:\Program Files\NetPolicePro64\netpolice_s.exe

Обратите внимание – путь к приложению может отличаться в зависимости от разрядности операционной системы и установленного продукта Netpolice.

Для каждого приложения установить набор правил **"Системное приложение Windows"**



В конце у Вас должен получиться вот такой список:



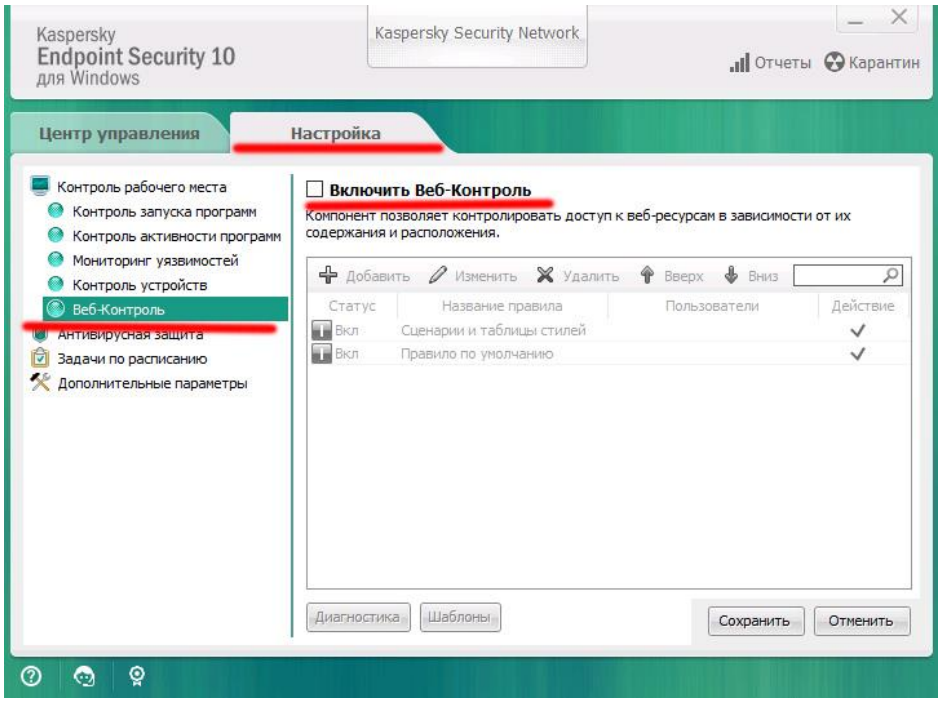
4. Сохраните все настройки и перезагрузите компьютер. В случае дополнительных запросов антивируса для вышеуказанных приложений, необходимо разрешить этим трём приложениям все действия.

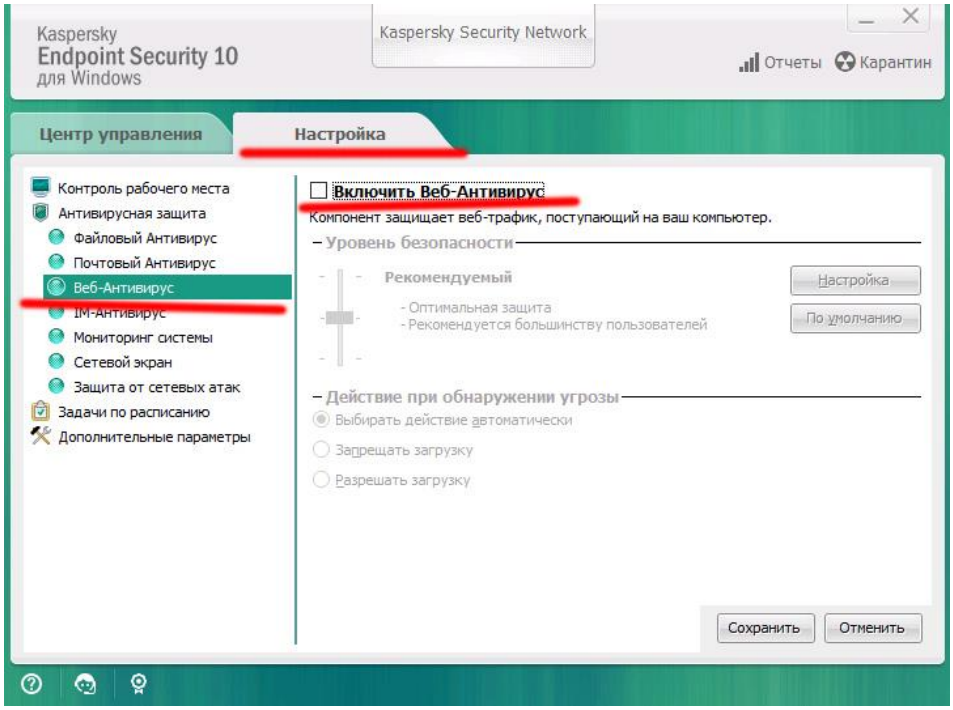
Инструкция по настройке Антивируса Касперского для совместного использования с программами Netpolice

- Kaspersky Endpoint Security

При установке антивируса, откажитесь от установки компонентов **«Веб-контроль»** и **«Веб-антивирус».**

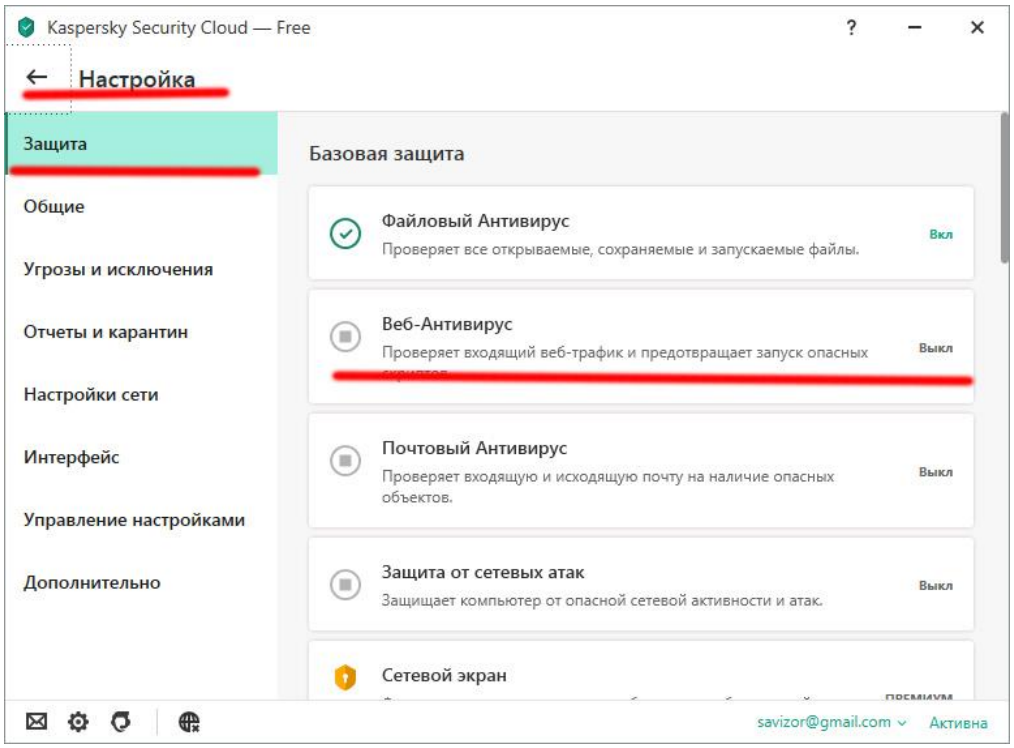
Если они уже установлены, необходимо отключить их в настройках антивируса, как показано на скриншотах.
Либо, если антивирус управляется централизовано, с консоли управления на сервере – отключить эти компоненты в политиках.



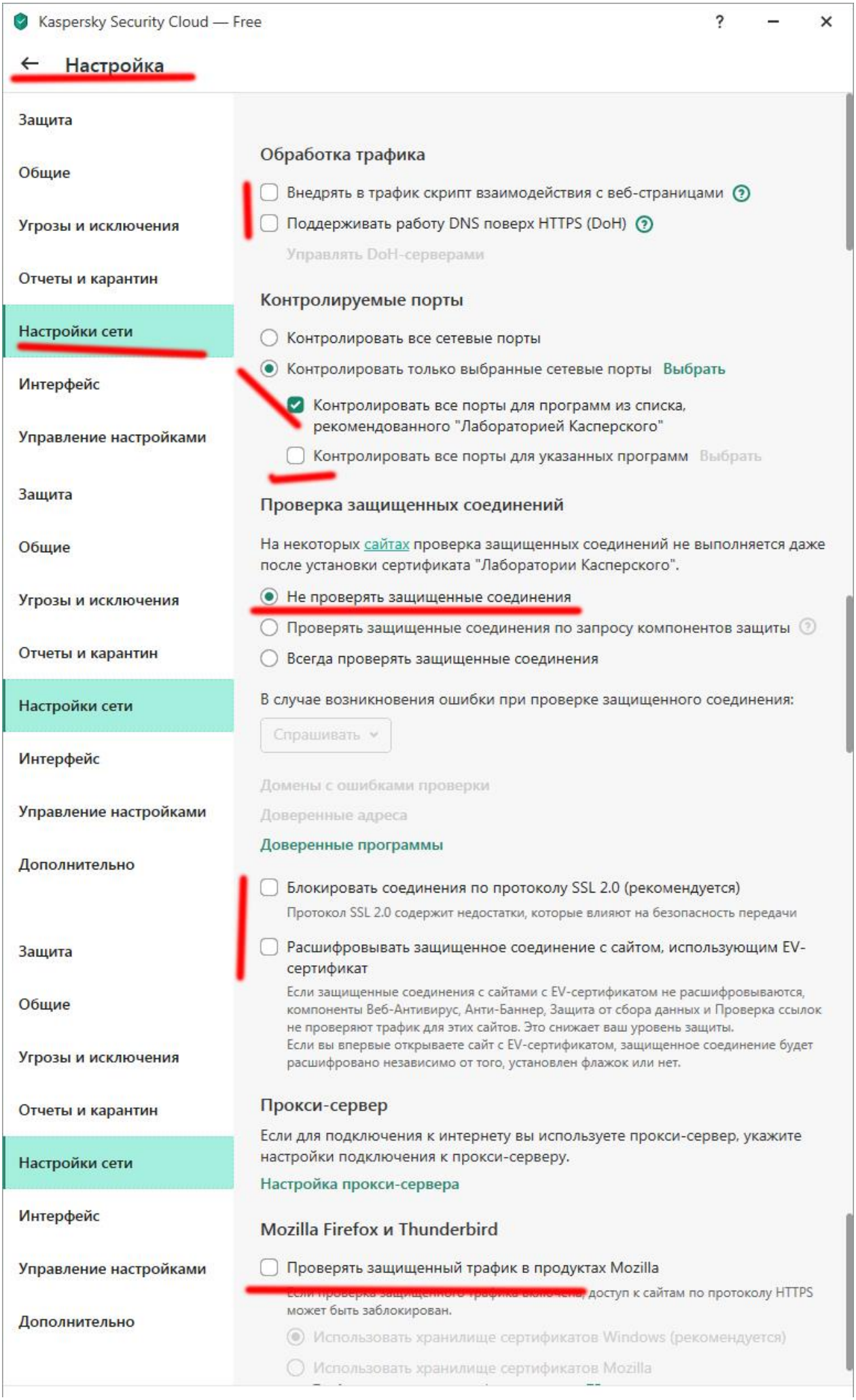


- Kaspersky Security Cloud

Отключить компонет **«веб-контроль»**



Так же в **настройках – настройка сети** снять галочки согласно приведенному далее скриншоту.


Kaspersky Security Cloud — Free
Настройка
Защита
Общие
Угрозы и исключения
Отчеты и карантин
Настройки сети
Интерфейс
Управление настройками
Защита
Общие
Угрозы и исключения
Отчеты и карантин
Настройки сети
Интерфейс
Управление настройками
Дополнительно
Защита
Общие
Угрозы и исключения
Отчеты и карантин
Настройки сети
Интерфейс
Управление настройками
Дополнительно
Обработка трафика
Внедрять в трафик скрипт взаимодействия с веб-страницами
Поддерживать работу DNS поверх HTTPS (DoH)
Управлять DoH-серверами
Контролируемые порты
Контролировать все сетевые порты
Контролировать только выбранные сетевые порты Выбрать
Контролировать все порты для программ из списка, рекомендованного "Лабораторией Касперского"
Контролировать все порты для указанных программ Выбрать
Проверка защищенных соединений
На некоторых сайтах проверка защищенных соединений не выполняется даже после установки сертификата "Лаборатории Касперского".
Не проверять защищенные соединения
Проверять защищенные соединения по запросу компонентов защиты
Всегда проверять защищенные соединения
В случае возникновения ошибки при проверке защищенного соединения:
Спрашивать
Домены с ошибками проверки
Доверенные адреса
Доверенные программы
Блокировать соединения по протоколу SSL 2.0 (рекомендуется)
Протокол SSL 2.0 содержит недостатки, которые влияют на безопасность передачи
Расшифровывать защищенное соединение с сайтом, использующим EV-сертификат
Если защищенные соединения с сайтами с EV-сертификатом не расшифровываются, компоненты Веб-Антивирус, Анти-Баннер, Защита от сбора данных и Проверка ссылок не проверяют трафик для этих сайтов. Это снижает ваш уровень защиты.
Если вы впервые открываете сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.
Прокси-сервер
Если для подключения к интернету вы используете прокси-сервер, укажите настройки подключения к прокси-серверу.
Настройка прокси-сервера
Mozilla Firefox и Thunderbird
Проверять защищенный трафик в продуктах Mozilla
доступ к сайтам по протоколу HTTPS может быть заблокирован.
Использовать хранилище сертификатов Windows (рекомендуется)
Использовать хранилище сертификатов Mozilla