Symantec Endpoint Protection - оптимальная настройка

★★★★★ 31 32 450 Автор: Tunecom Опубликовано: 2023-11-29

Сегодня мы рассмотрим параметры неуправляемого клиента комплексного антивируса Symantec Endpoint Protection и настроим оптимально. Антивирусный продукт Symantec Endpoint Protection довольно удачное решение, сочетает в себе хорошие показатели защиты компьютера и высокое быстродействие.

Наше руководство вам покажет как настроить оптимально комплексный антивирусный пакет Symantec Endpoint Protection для лучшей безопасности компьютера. Давайте посмотрим на параметры и настроим **антивирус**, чтобы улучшить защитные свойства и повысить удобство использования.

Полезные ссылки

> ***Как запретить программе доступ в Интернет используя Symantec Endpoint Protection***
>
> ***Как добавить файл или папку в исключения Symantec Endpoint Protection***
>
> ***Скачать неуправляемый клиент Symantec Endpoint Protection***

Устанавливать Symantec Endpoint Protection лучше всего стандартным клиентом.

ПОПУЛЯРНЫЕ СТАТЬИ

Как запретить программе доступ в Интернет с помощью ESET

Kaspersky Standard для Windows - бесплатная лицензия

Как скачать Windows 10 версия 22H2

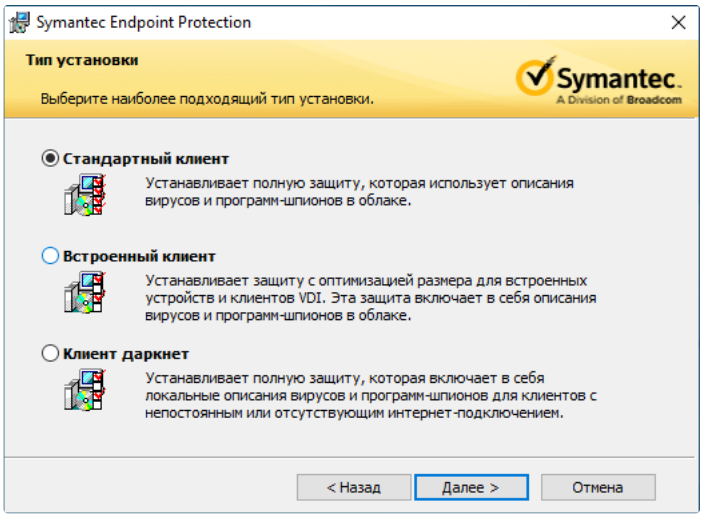
Бесплатное обновление Windows 7 до Windows 10

Скачать Windows 11 версии 23H2

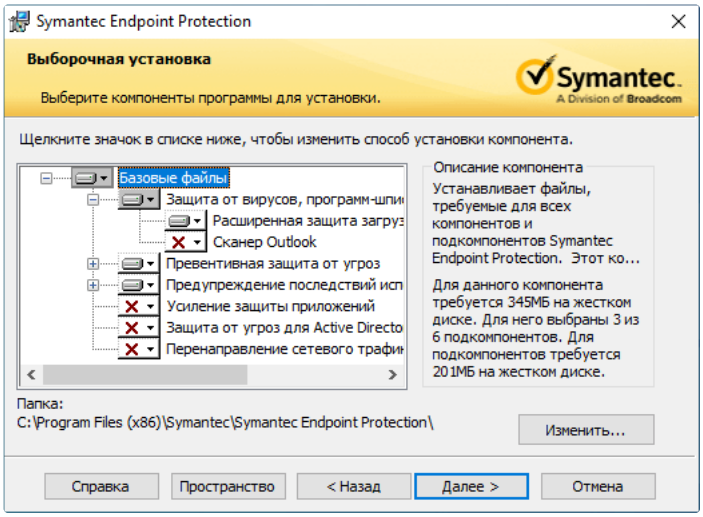
ОБСУЖДАЕМЫЕ СТАТЬИ

Kaspersky Plus для Android - бесплатная лицензия на 3 месяца

2024-02-04

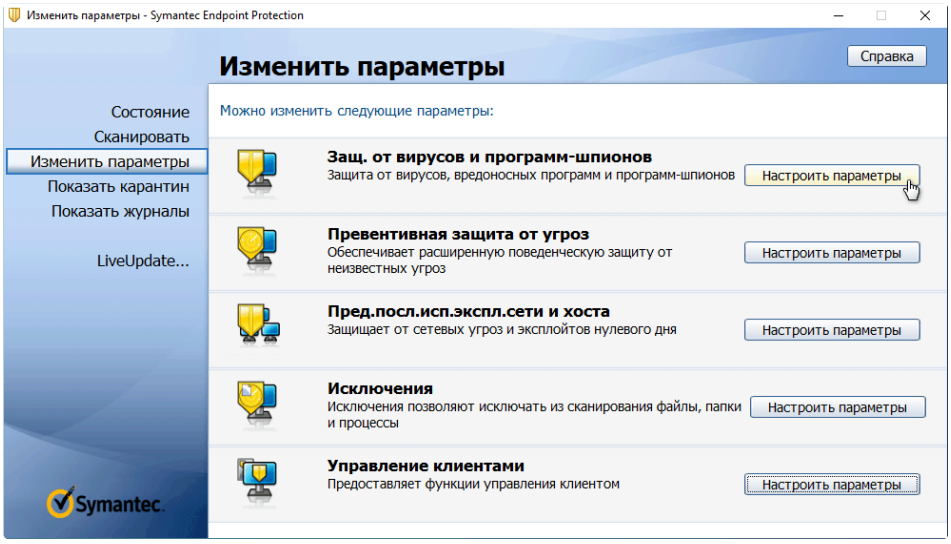


Компонентов которые выбраны на скриншоте для надежной защиты достаточно:



Оптимальная настройка Symantec Endpoint Protection

Запустите антивирус и перейдите в меню "**Изменить параметры**". Откройте настройки параметров "**Защиты от вирусов и программ-шпионов**".



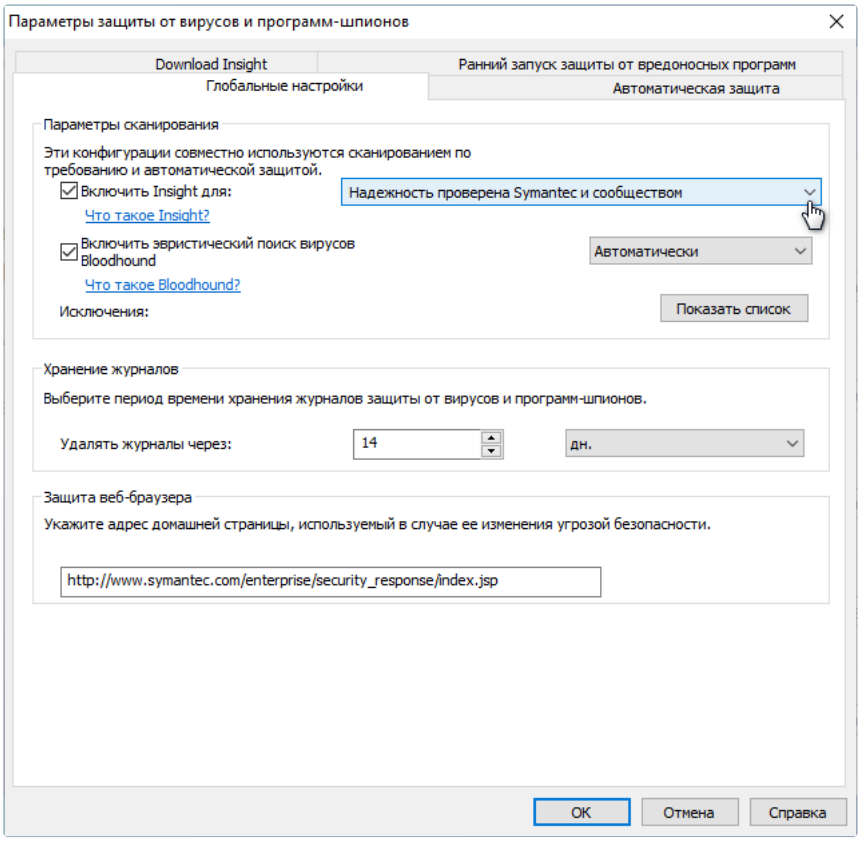
В глобальных настройках задайте компоненту **Insight** - "**Надежность проверена Symantec и сообществом**", это уменьшит количество ложных срабатываний и немного компенсирует следующую настройку. (не забывайте нажимать кнопку "**OK**" для применения изменений).

Kaspersky Standard для Windows - бесплатная лицензия
2024-02-04

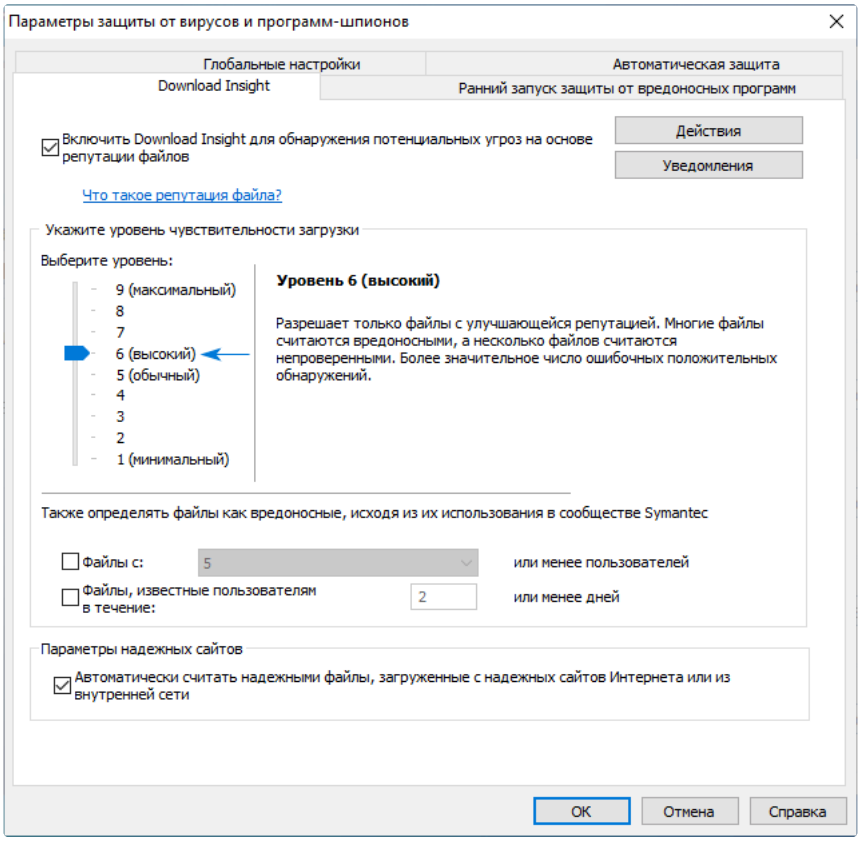
Realtek ALC1200 - подробности и отличия от более качественного аудиокодека ALC1220-VB
2021-02-09

Как включить русский язык в Microsoft Edge на основе Chromium
2019-07-11

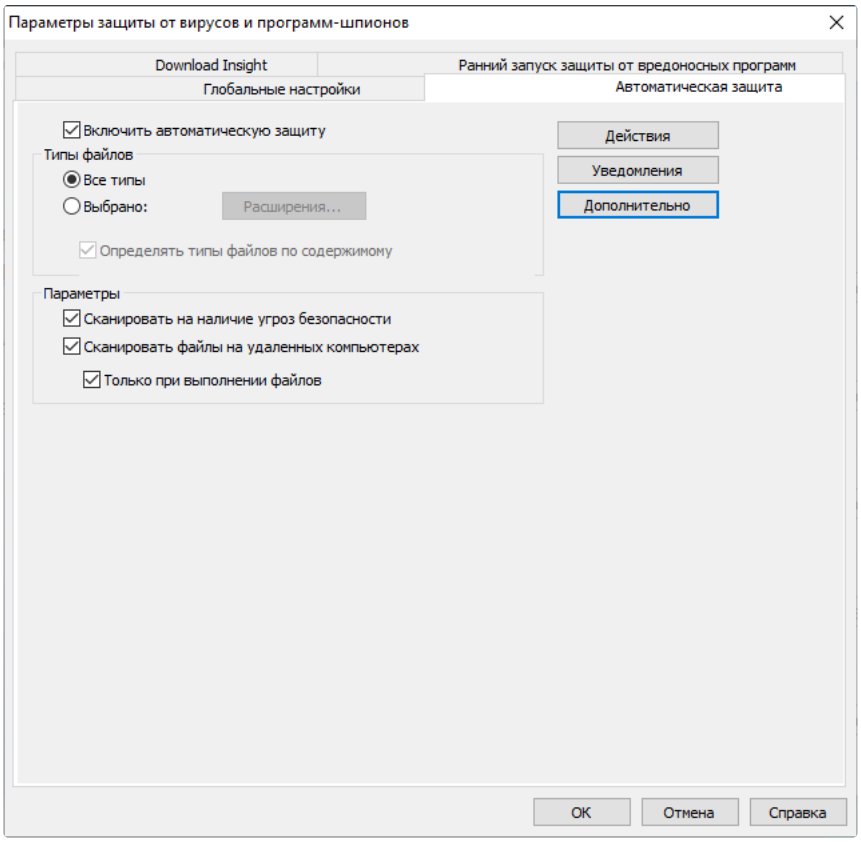
Kerish PC Doctor - бесплатная лицензия на 1 год
2024-02-19



Для начинающих пользователей компьютера, чтобы снизить риск заражения вирусами, рекомендуется на вкладке "**Download Instinct**" немного повысить уровень чувствительности — до высокого "**6**" и улучшить безопасность. (Если будет много неприемлемых обнаружений и удалений важных файлов, можно занести детектируемые объекты в **исключения**, либо вернутся на обычную "**Пятую**" ступень).

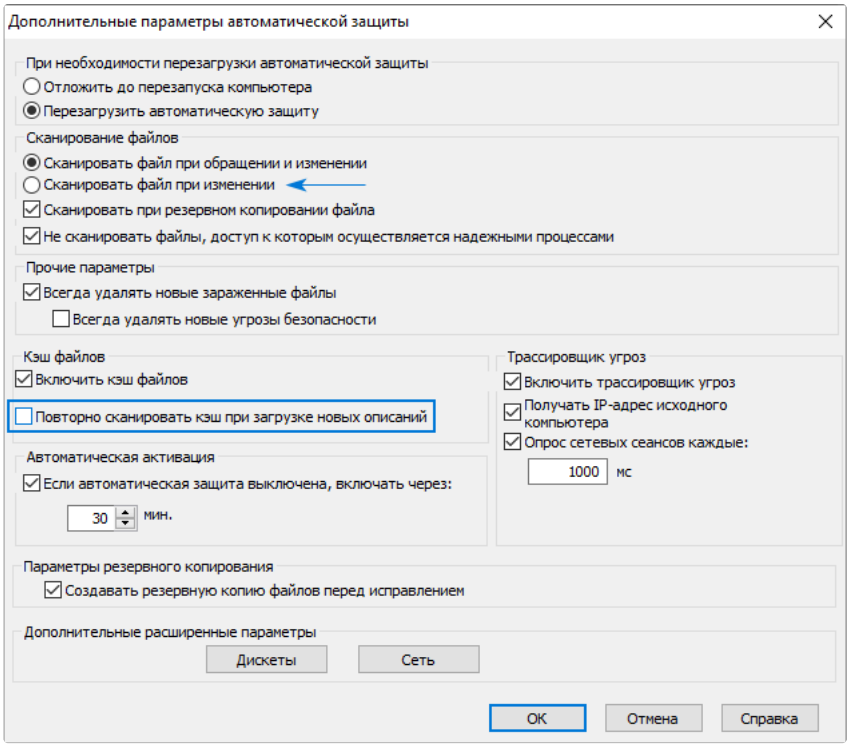


Зайдите в раздел "**Автоматическая защита**" и нажмите "**Дополнительно**".

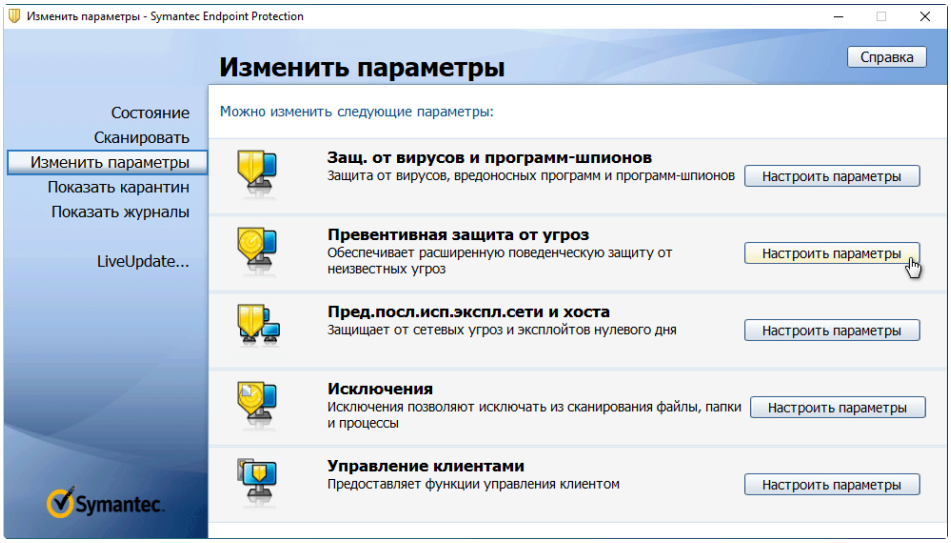


Активируйте пункт "**Сканировать файл при изменении**", если продукт сильно влияет на быстродействие при операциях с файлами и считается что допустимо ослабить защиту.

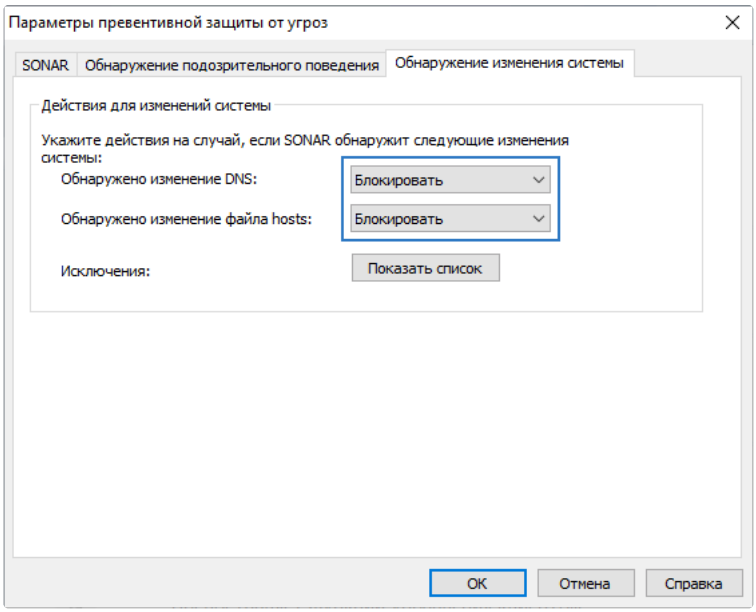
Снимите галочку с параметра "**Повторно сканировать кэш при загрузке новых описаний**" - это немного снизит нагрузку на **слабых компьютерах**.



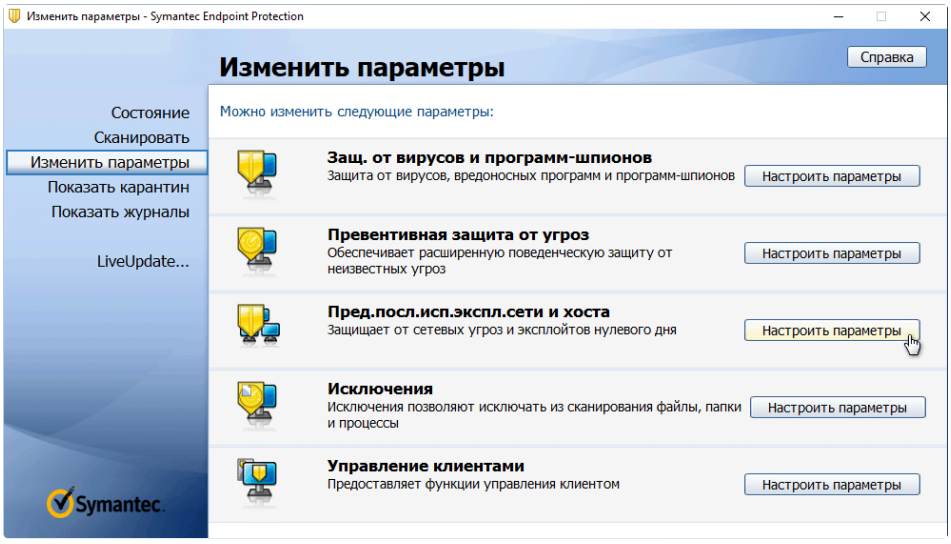
Откройте настройки "**Превентивной защиты от угроз**".



Перейдите на вкладку "**Обнаружение изменения системы**" и поставьте значение "**Блокировать**" для изменений "**DNS**" и файла "**Hosts**".



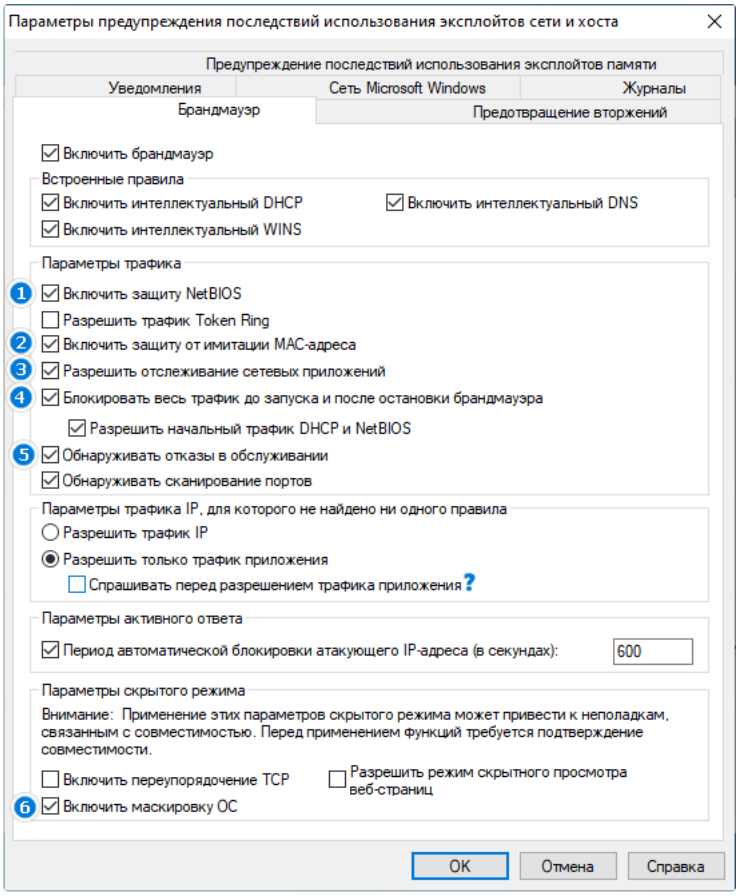
Зайдите в параметры "**Защиты от сетевых угроз и эксплойтов нулевого дня**".



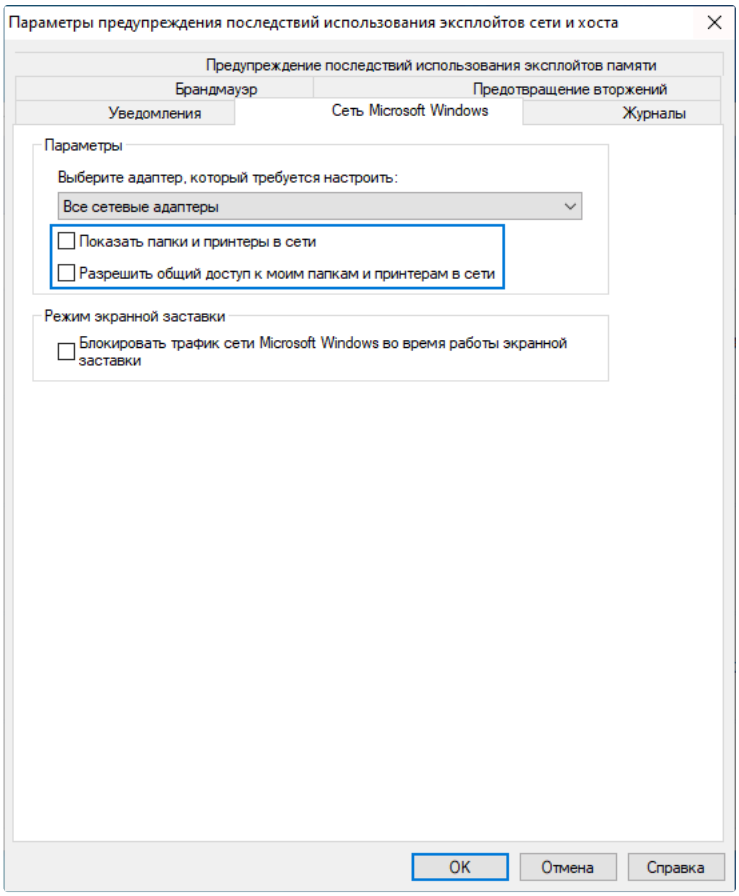
В настройках "**Брандмауэра**" можно включить:

1. Защиту NetBIOS.
2. Защиту от имитации MAC-адреса.
3. Разрешить отслеживание сетевых приложений (по желанию), проще заблокировать системному компоненту, (например SearchUI.exe) **доступ в интернет** и забыть о частых уведомлениях).
4. Блокировать весь трафик до запуска и после остановки брандмауэра.
5. Обнаруживать отказы в обслуживании.
6. Включить маскировку ОС.

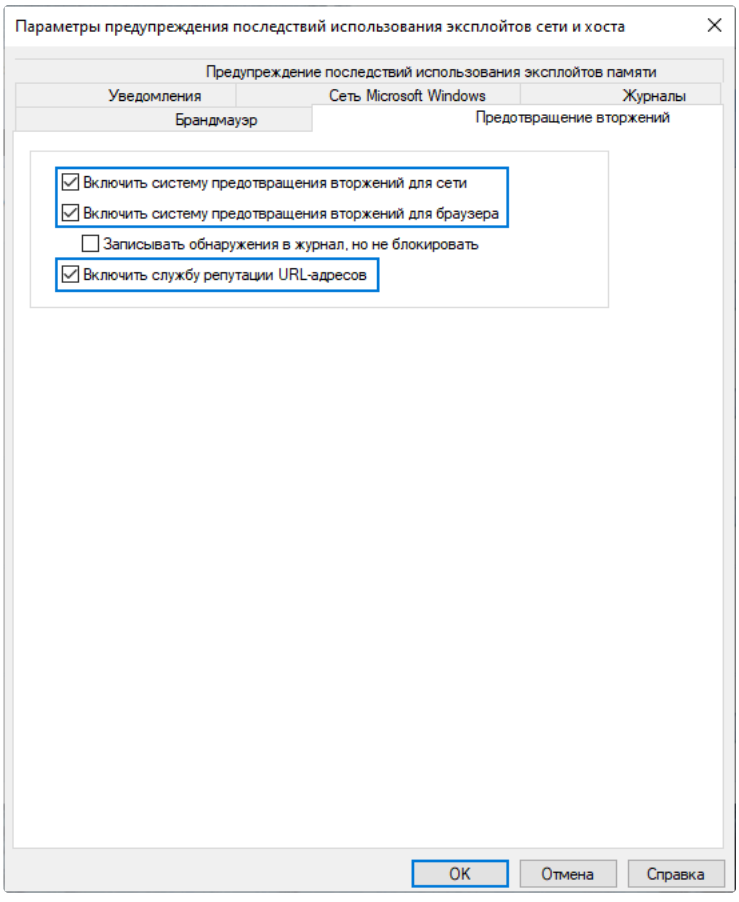
> ***Примечание**. Если вам необходимо контролировать доступ к Интернету для программ вручную, можно поставить галочку на пункт - "**Спрашивать перед разрешением трафика приложения**".*



Перейдите в "**Сеть Microsoft Windows**", снимите галочки с "**Показать папки и принтеры в сети**" и "**Разрешить общий доступ к моим папкам и принтерам в сети**". Это позволит скрыть ваш компьютер и убережет от хакерских атак.



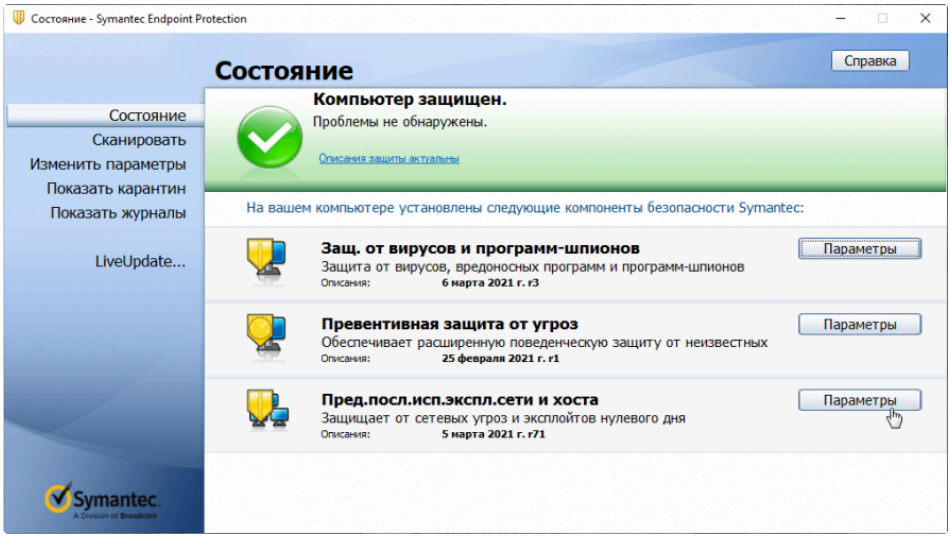
На вкладке "**Предотвращения вторжений**" проверьте активированные пункты "**Включить систему предотвращения вторжений для сети**", "**Включить систему предотвращения вторжений для браузера**" и "**Включить службу репутации URL-адресов**".



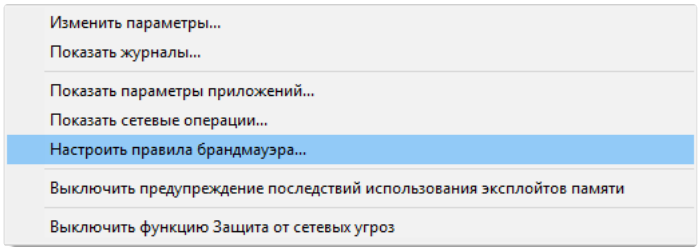
Отполировать настройки сети помогут правила брандмауэра, которые запретят возможное проникновение в компьютер по протоколу **ICMP Echo**, и всем портам **UDP** и **TCP**.

Для большего удобства мы создали и экспортировали три правила для вас, упаковали в zip-архив **BlockPort** который необходимо скачать и распаковать в удобное место.

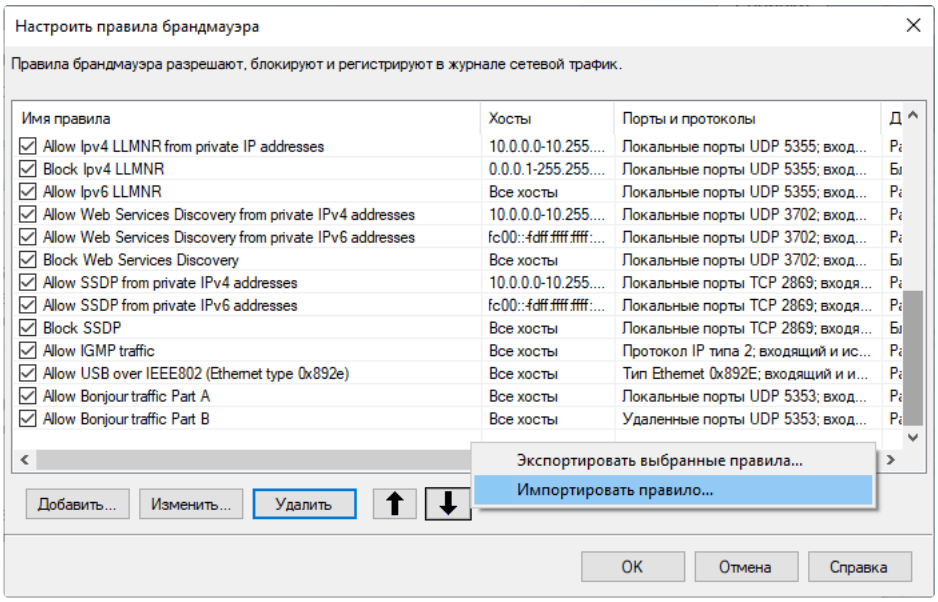
Открыть правила брандмауэра нажав параметры "**Предупреждение последствий использования эксплойтов сети и хоста**"



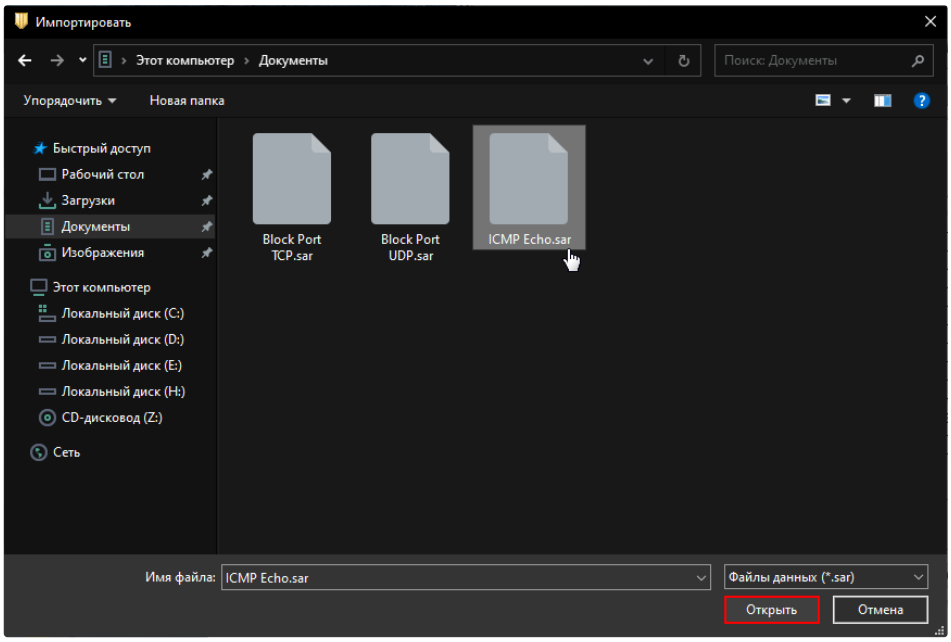
В появившемся окне нажать "**Настроить правила брандмауэра**".



Кликнуть правой кнопкой мыши на пустом месте окна и выбрать "**Импортировать правило**".



Добавить 3 правила по очереди:



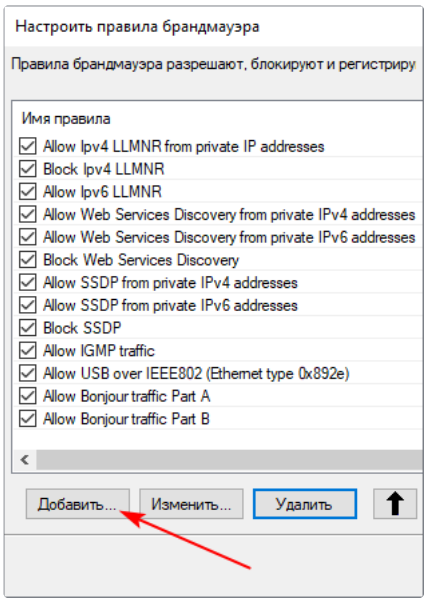
Выделить и поднять импортированные правила стрелочкой вверх. Теперь в компьютер вряд ли кто пробьется, программы, торрент клиенты, игры и мессенджеры будут работать в обычном режиме, брандмауэр интеллектуально распознает трафик официальных приложений и пропускает его.

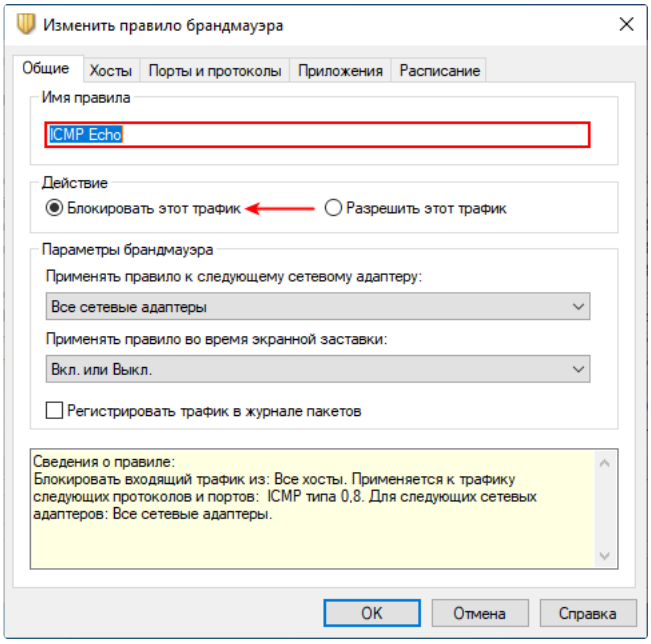
Проверено на собственном компьютере, qBittorrent качает, Forza Horizon играет по сети, Telegram переписывается, Mozilla Thunderbird отправляет и принимает письма, FileZilla передает файлы в обоих направлениях и остальной необходимый софт работает.

При возникновении проблем сетевого доступа с вашими программами, просто удалите добавленные правила. Но если важна капитальная сетевая безопасность, потратьте немного времени и подберите работающие альтернативы программного обеспечения с данными параметрами.

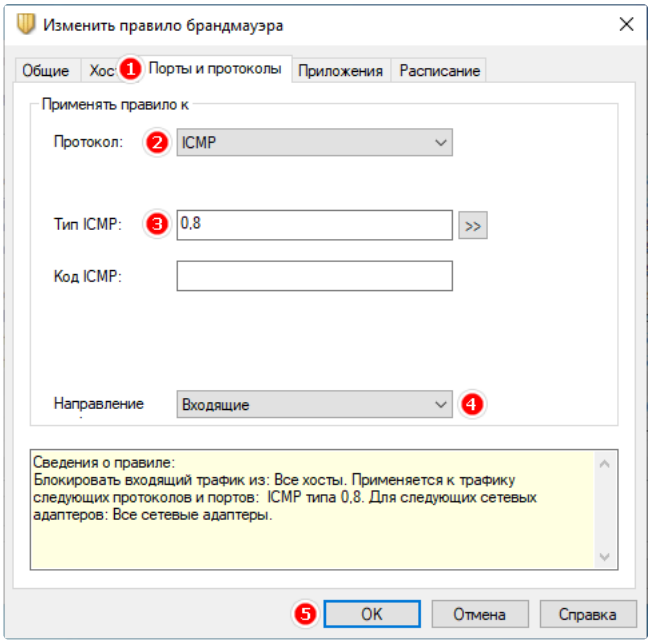
> *Дополнение. Если вы захотите самостоятельно настроить блокировку портов, воспользуйтесь наглядным руководством представленным ниже.*

1. Откройте настройки правил брандмауэра как показано выше, добавьте правило под названием "**ICMP Echo**" и отметьте "**Блокировать этот трафик**".

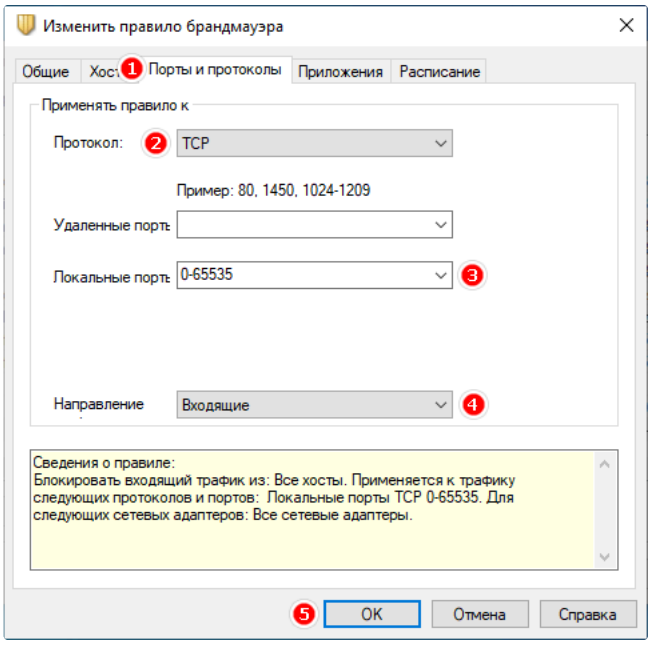




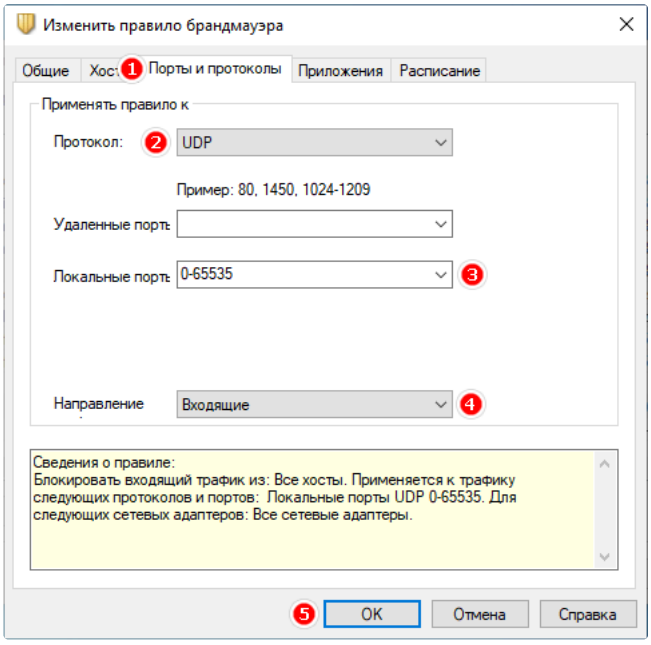
2. Перейдите на вкладку "**Порты и протоколы**", установите протокол "**ICMP**", пропишите тип значением "**0,8**", задайте направление "**Входящие**" и нажмите кнопку "**OK**".



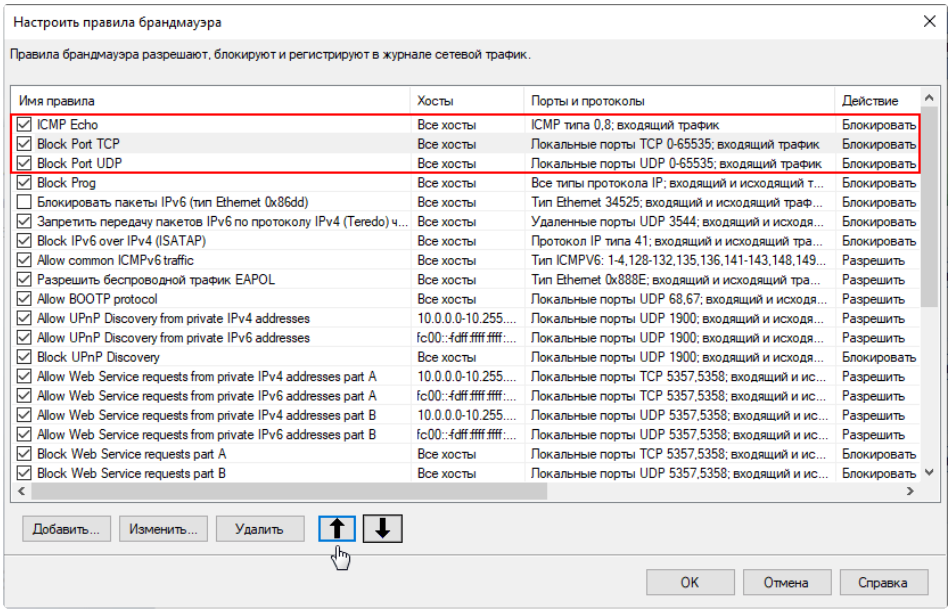
3. Создайте по аналогии блокирующее правило с именем "**Block Port TCP**", в разделе "**Порты и протоколы**" установите протокол "**TCP**", пропишите локальные порты "**0-65535**", выберите направление "**Входящие**" и нажмите "**OK**".



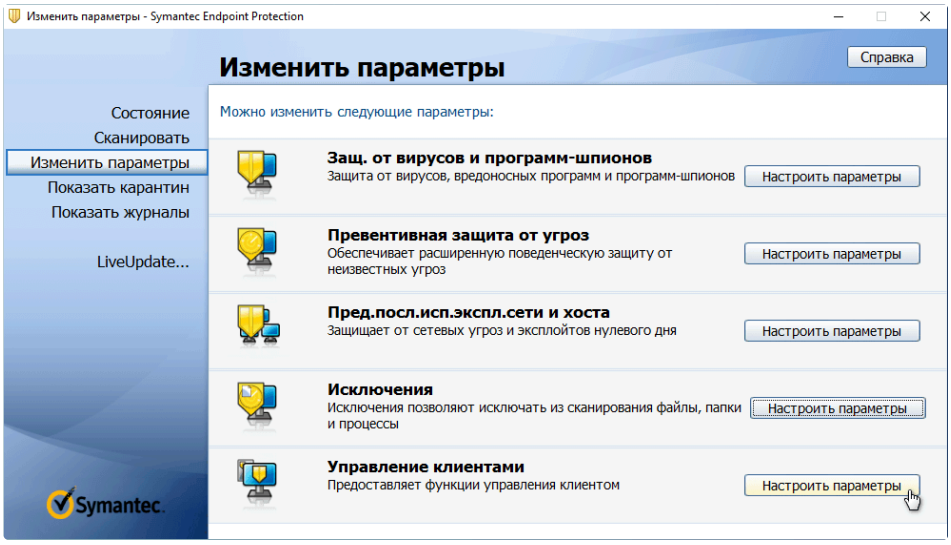
4. Теперь добавьте последнее правило блокировки трафика с названием "**Block Port UDP**", на вкладке "**Порты и протоколы**" поставьте протокол "**UDP**", задайте локальные порты "**0-65535**", укажите направление "**Входящие**" и кликните "**OK**".



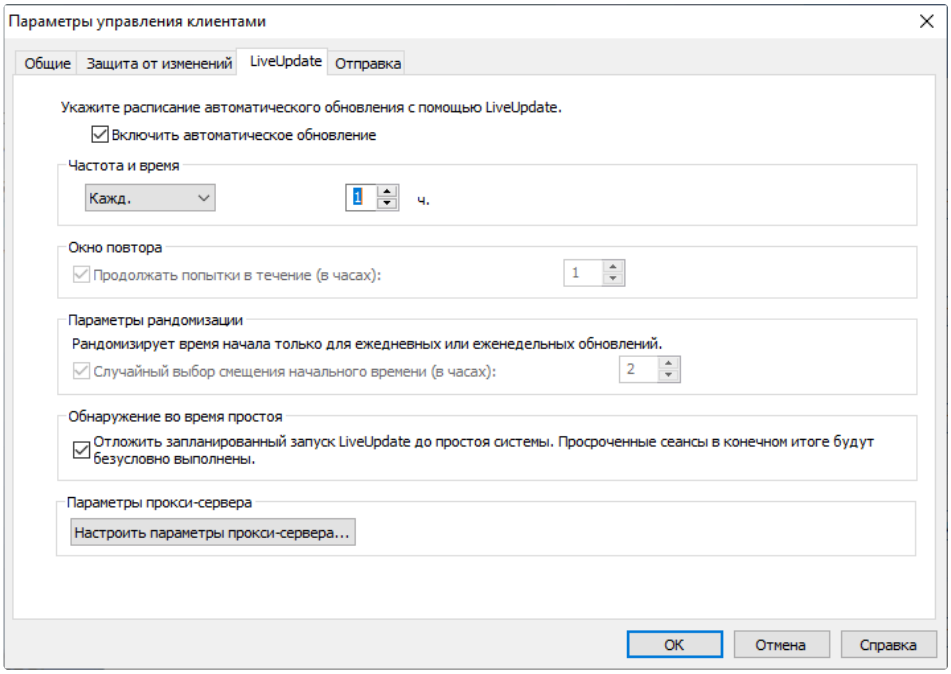
5. Поднимите все три созданных правила вверх.



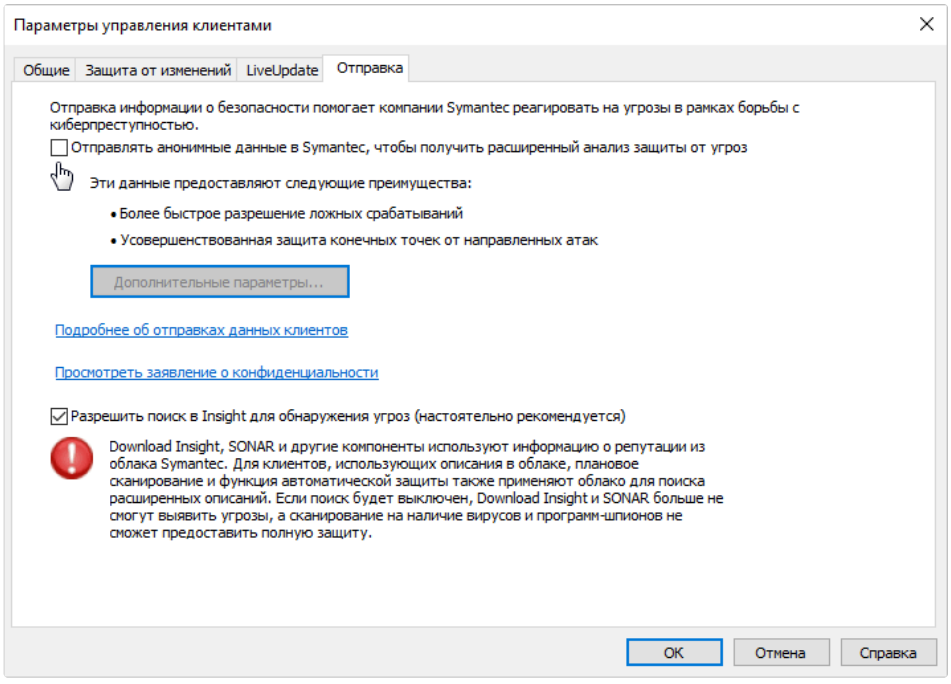
На завершающей стадии, пройдите в "**Параметры управления клиентами**".



Задайте получение автоматических обновлений "**LiveUpdate**" - каждый час.



Посетите раздел "**Отправка**" и отключите передачу анонимных данных не забыв проверить "**Дополнительные параметры**". Поиск в **Instinct** оставьте включенным, облако Symantec помогает лучше выявлять угрозы.



После выполнения всех мероприятий по **настройке**, неуправляемый клиент комплексного антивируса Symantec Endpoint Protection будет защищать ваш компьютер надежней и работать оптимально.

Рекомендуемый контент