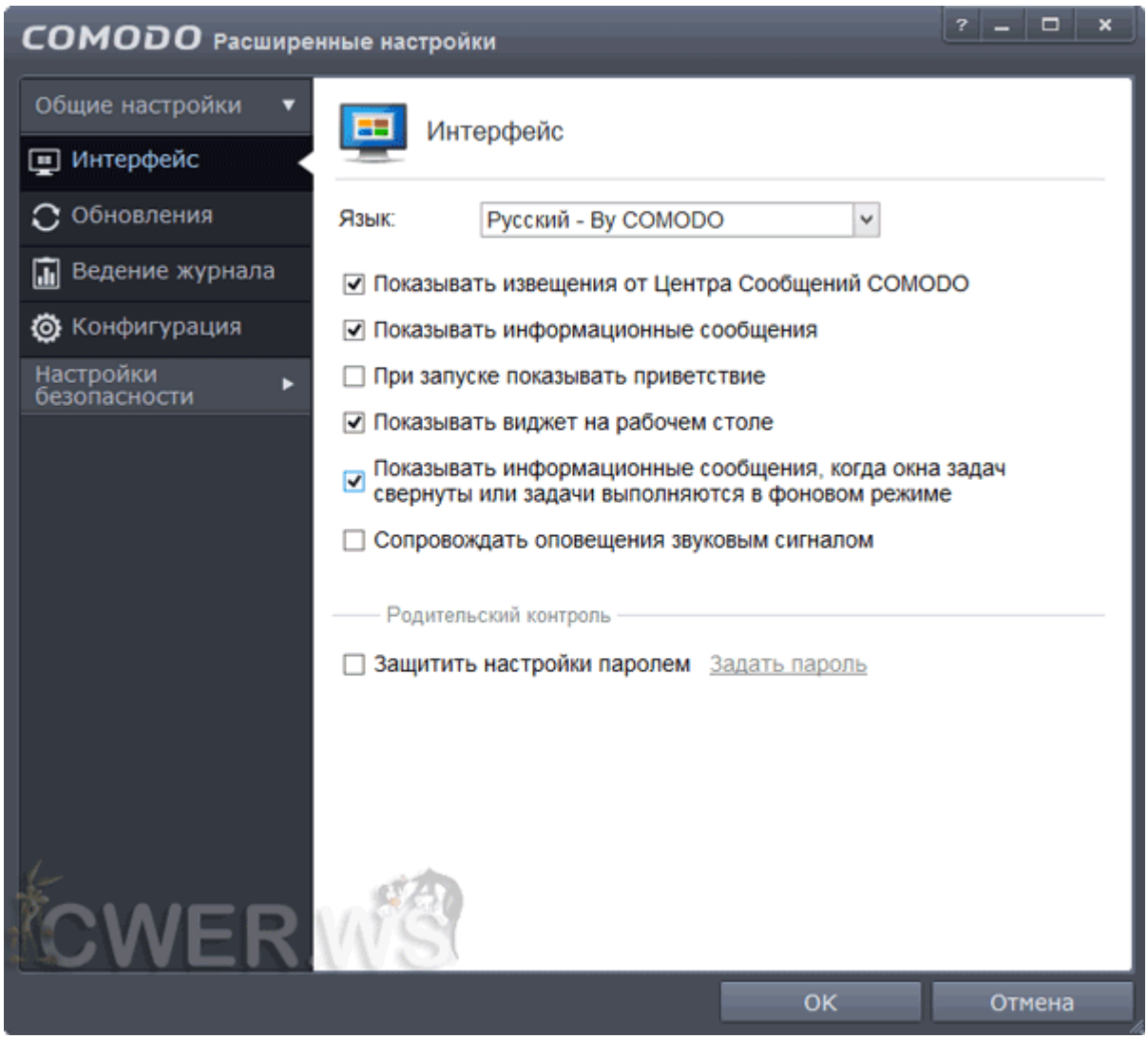
Как настроить COMODO Internet Security 6

В связи с тем, что интерфейс шестой версии COMODO Internet Security сильно отличается от пятой, мы подготовили для всех посетителей http://cwer.ws/ отдельную инструкцию по COMODO IS 6. Это, возможно, не лучшая и не единственно правильная настройка, но она позволит новичку, только что установившему этот программный комплекс, быстро настроить все его компоненты.

В 6-й версии добраться до настроек не так просто, как в 5-й, но это скорее с непривычки. В главном окне программы нажимаем на круговую стрелку, чтобы перейти в окно "**Задачи**". Затем нужно отобразить выпадающий список задач одного из компонентов и выбрать в нем заветный пункт "**Расширенные настройки**".



В разделе "**Интерфейс**" категории "**Общие настройки**" расположились привычные пункты, отвечающие за "поведение" программы. Советуем активировать пункты:

- Показывать извещения от Центра Сообщений COMODO
- Показывать информационные сообщения
- Показывать информационные сообщения, когда окна задач свернуты или задачи выполняются в фоновом режиме

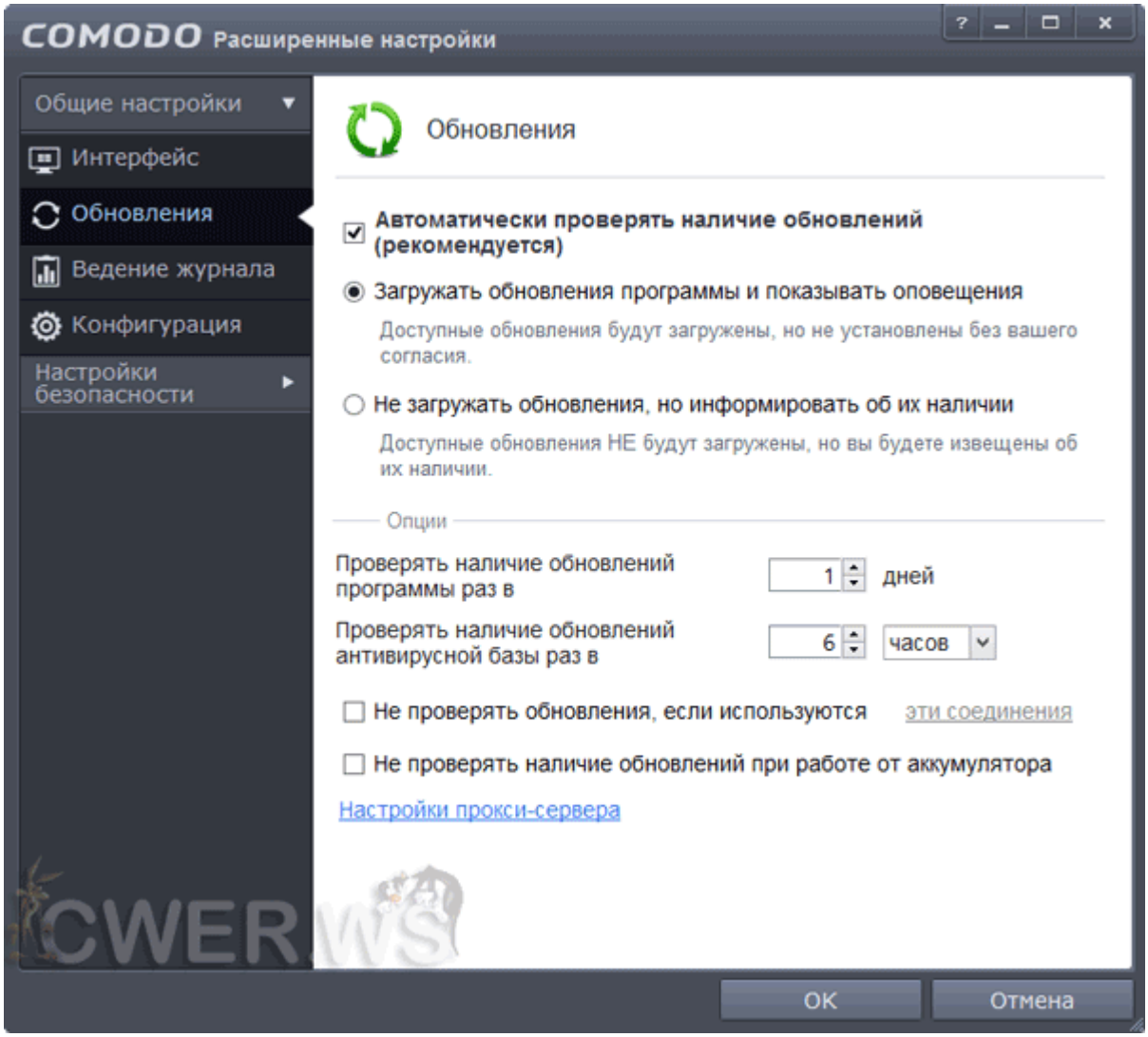
Это позволит вам быть в курсе, какие файлы были удалены программой, какие процессы были заблокированы, какие программы были изолированы и по каким причинам. Кроме того, вы будете уведомляться о всевозможных новинках и акциях от COMODO. Впрочем, если вам будут надоедать эти рекламные сообщения, их можно отключить.
Мы не видим смысла в следующих пунктах:

- При запуске показывать приветствие
- Сопровождать оповещения звуковым сигналом

Если же вам нравится, когда программа светится и "пиликает", можете оставить их включенными, на безопасность вашего компьютера это никак не повлияет.

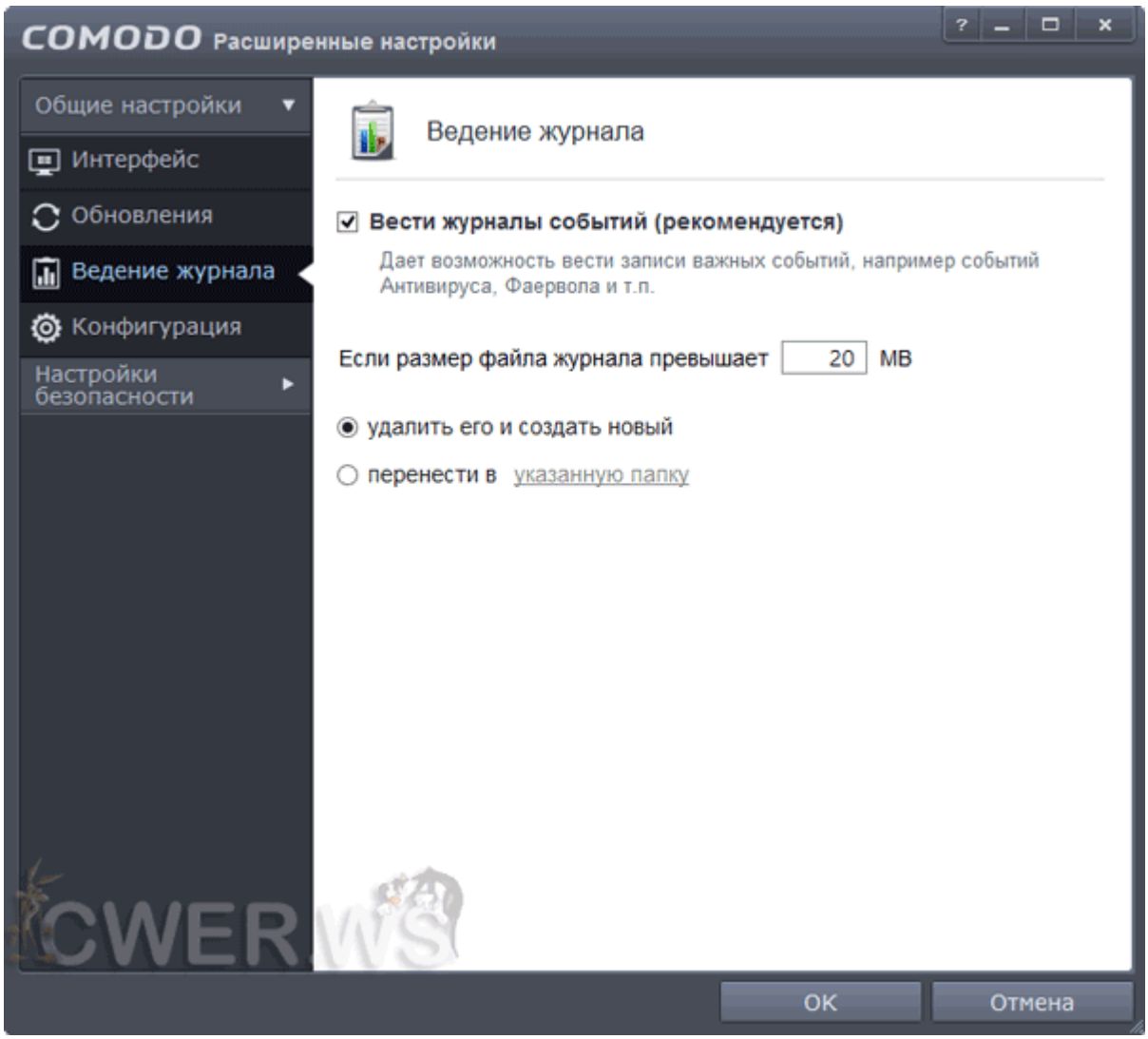
Показывать ли *виджет на рабочем столе*, личное дело каждого. Если вы не пользуетесь боковой панелью Windows, то вам и виджет COMODO скорее всего не будет нужен.

Следующий раздел категории "**Общие настройки**" - **Обновление**.



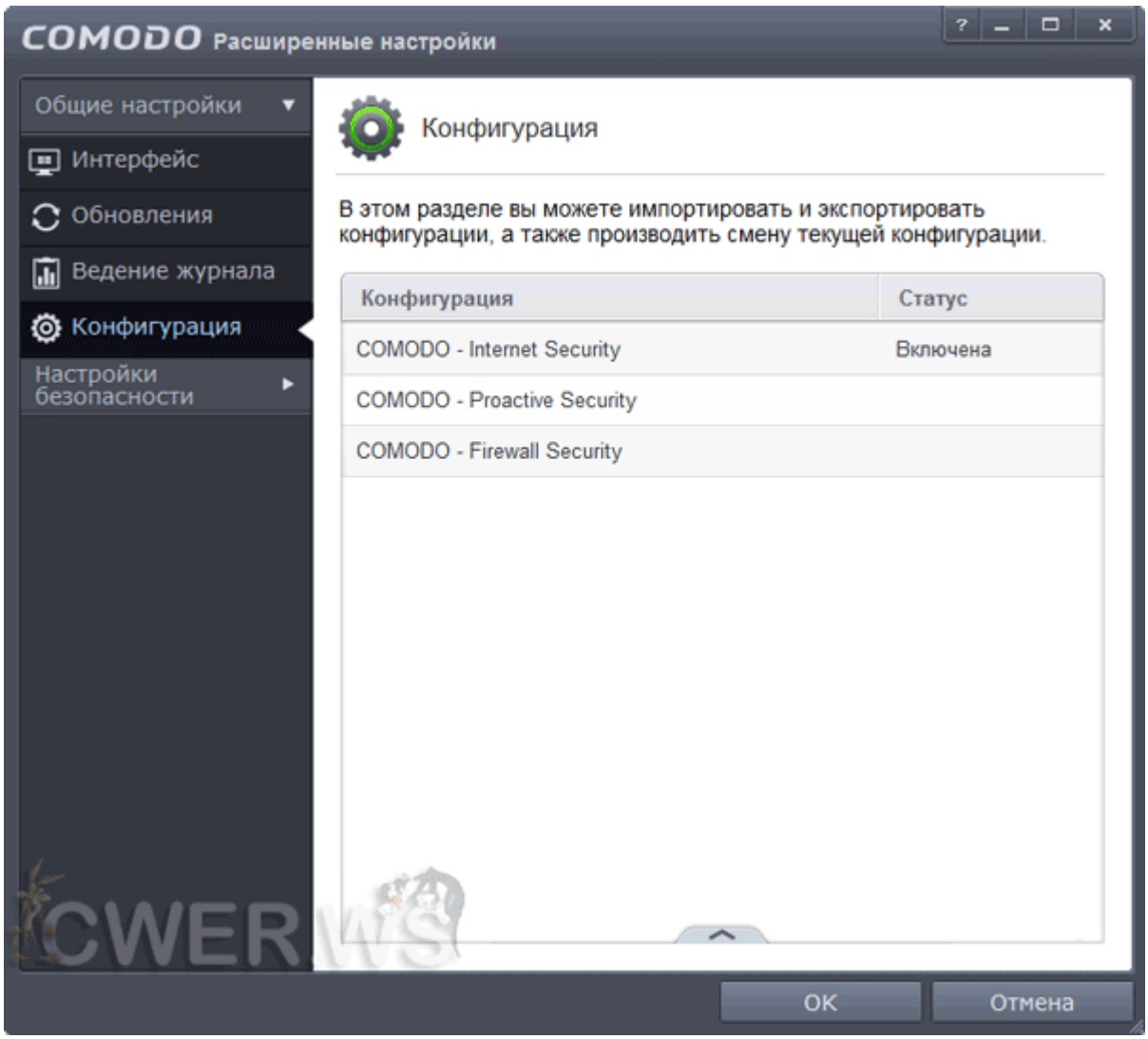
Думаю, наши советы здесь ни к чему. Регулярные обновление крайне желательны, но автоматические они будут или ручные, не имеет значения. О новых версиях программы COMODO Internet Security вы всегда сможете узнать на нашем сайте http://cwer.ws/. Если у вас портативный компьютер, нелишним может стать пункт "*Не проверять наличие обновлений при работе от аккумулятора*".

"Едем" дальше по списку.



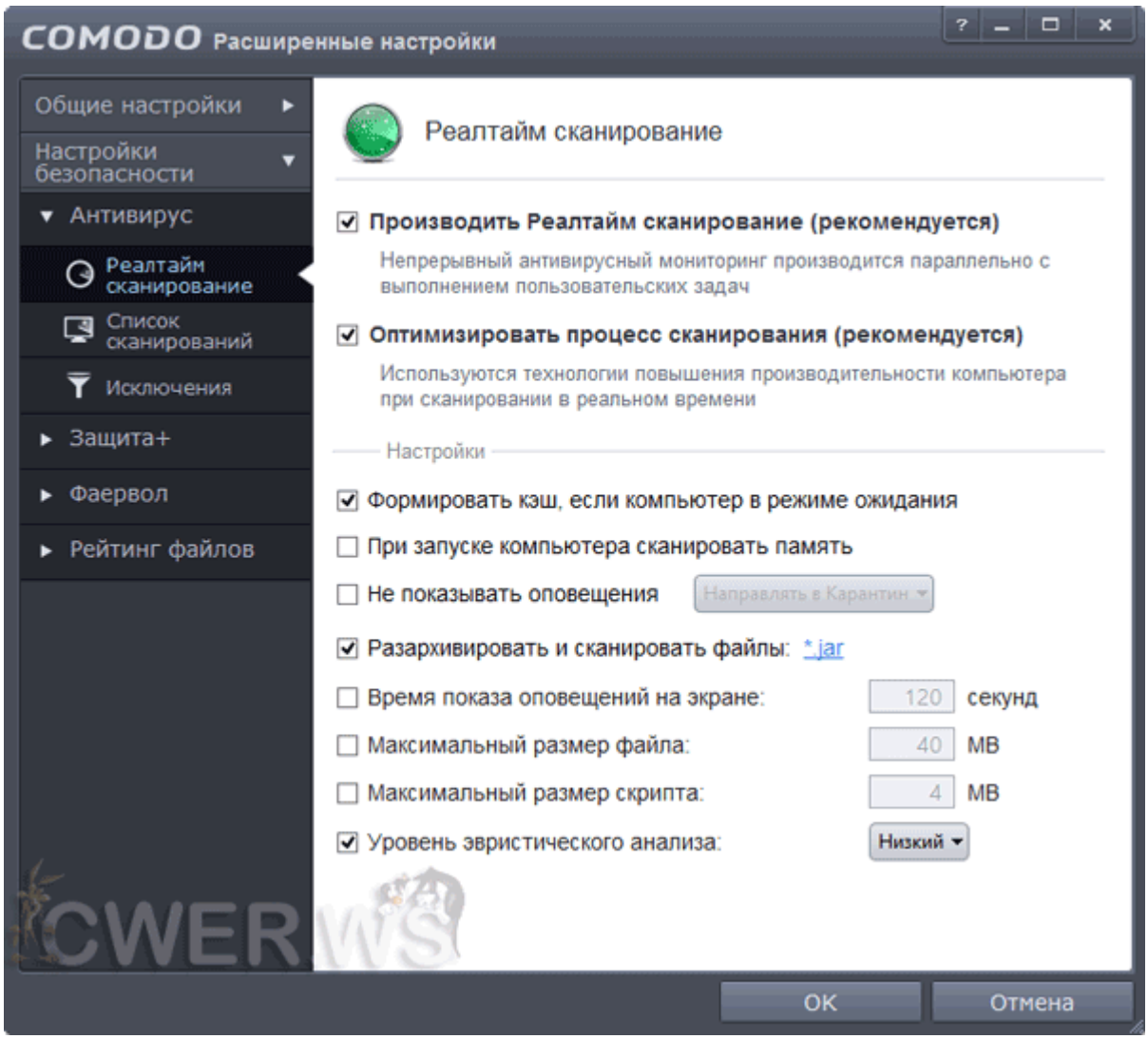
Ведение журнала дает возможность вести записи важных событий, например событий Антивируса, Фаервола и т.д. Даже если вы ограничены в дисковом пространстве, не отключайте журналирование, а лучше уменьшите предельный раздел журнала.

Ниже по списку раздел "**Конфигурация**".



За этим многообещающим название скрывается переключение конфигураций COMODO Internet Security. Очень полезными также будут функции импорта/экспорта настроек, например, при переустановке системы или для обмена с товарищами.

Наконец-то мы можем перейти в категорию "**Настройки безопасности**".



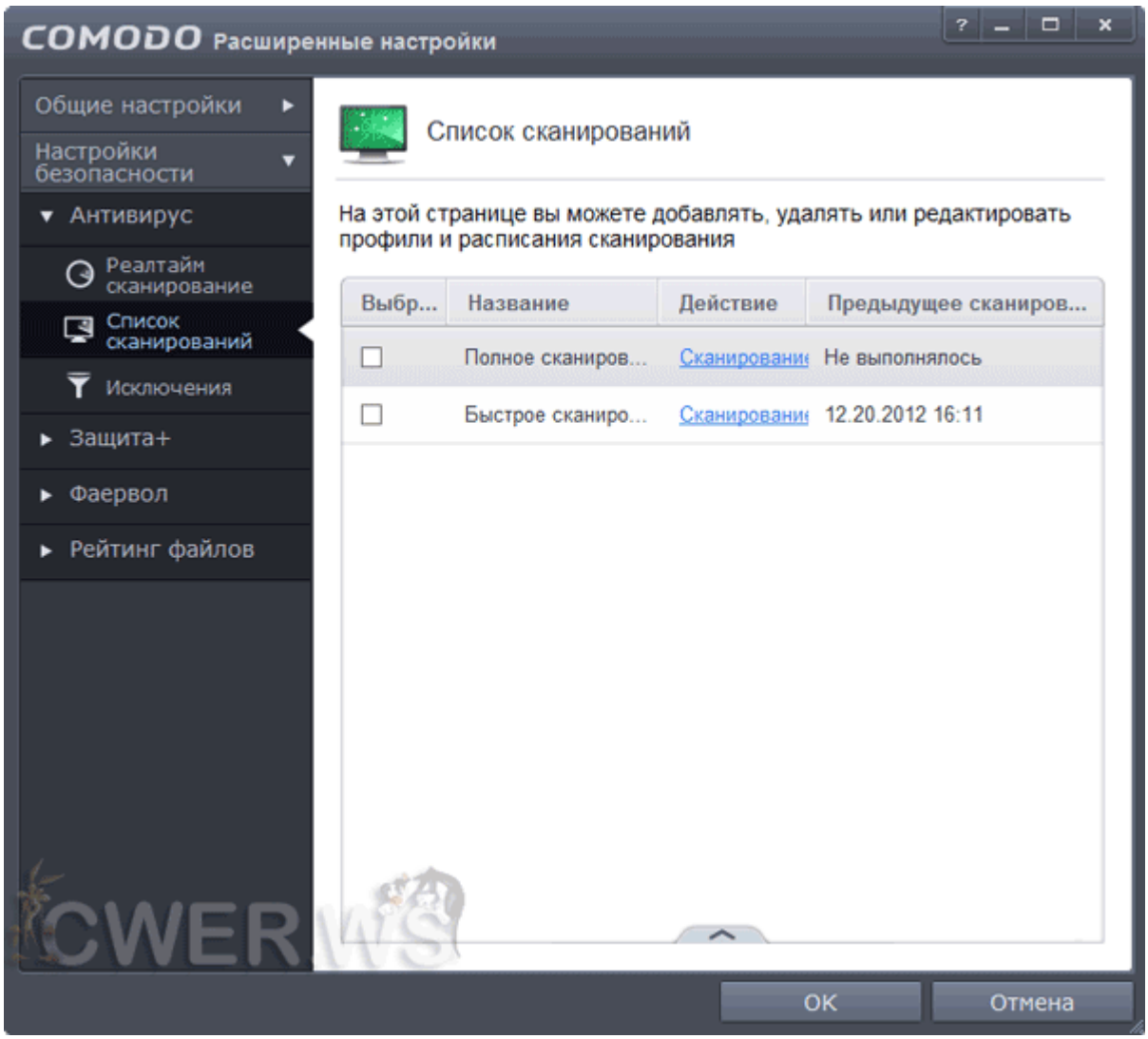
В разделе "**Реалтайм сканирование**" категории "**Антивирус**" более чем логичным будет наличие галочек напротив пунктов "*Производить Реалтайм сканирование*" и "*Оптимизировать процесс сканирования*". Первый обеспечивает антивирусный мониторинг параллельно с выполнением пользовательских задач, а второй использует технологии повышения производительности компьютера при сканировании в реальном времени. Кроме того, указываем программе формировать кэш, если компьютер в режиме ожидания, а также разархивировать и сканировать файлы .jar, что как минимум позволит вам не подцепить Винлокер.

Отключаем пункты "При запуске компьютера сканировать память" и "Не показывать оповещения", если они включены.

Вы также можете настроить сканирование больших файлов и время показа оповещений по своему вкусу, однако скорее в сторону уменьшения, нежели увеличения.

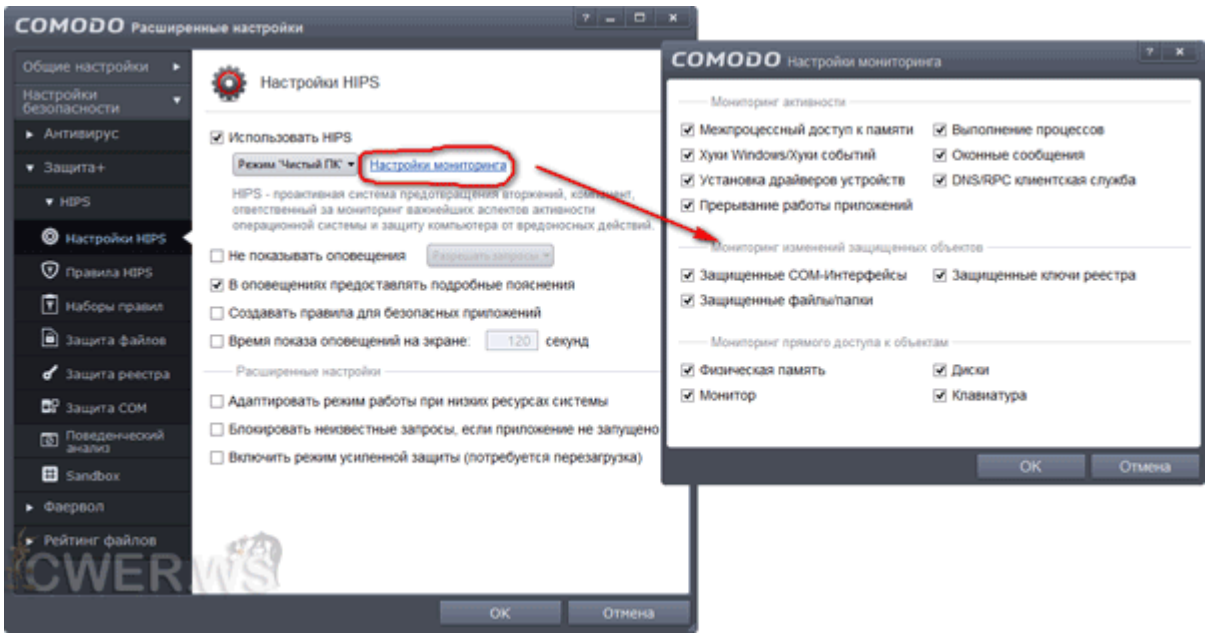
Уровень эвристического анализа можно повысить, если вы спокойно относитесь к антивирусной паранойе и более высокой нагрузке на процессор и память, создаваемой антивирусом.

Переходим к следующему разделу.



На странице "**Список сканирований**" вы в дальнейшем сможете добавлять, удалять или редактировать профили и расписания сканирования.

Мы не станем в этой статье на http://cwer.ws/ уделять внимание разделу "**Исключения**", так как вы и сами знаете, для чего он предназначен. Переходим сразу к категории "**Защита+**". Начнем по порядку - с раздела **HIPS** (системы предотвращения вторжений).



Необходимость использования HIPS не должна вызывать у пользователей http://cwer.ws/ ни малейших сомнений. Выбираем режим "*Чистый ПК*" и открываем *Настройки мониторинга*. Проверяем, чтобы были установлены все галочки:

- Мониторинг активности
  - Межпроцессный доступ к памяти
  - Выполнение процессов
  - Хуки Windows/хуки событий
  - Оконные сообщения
  - Установка драйверов устройств
  - DNS/RPC клиентская служба
  - Прерывание работы приложений
- Мониторинг изменений защищенных объектов
  - Защищенные COM-интерфейсы
  - Защищенные ключи реестра
  - Защищенные файлы/папки
- Мониторинг прямого доступа к объектам
  - Физическая память
  - Диски
  - Монитор
  - Клавиатура

Сохраняем настройки нажатием кнопки "ОК".

Мы рекомендуем отключить все пункты:

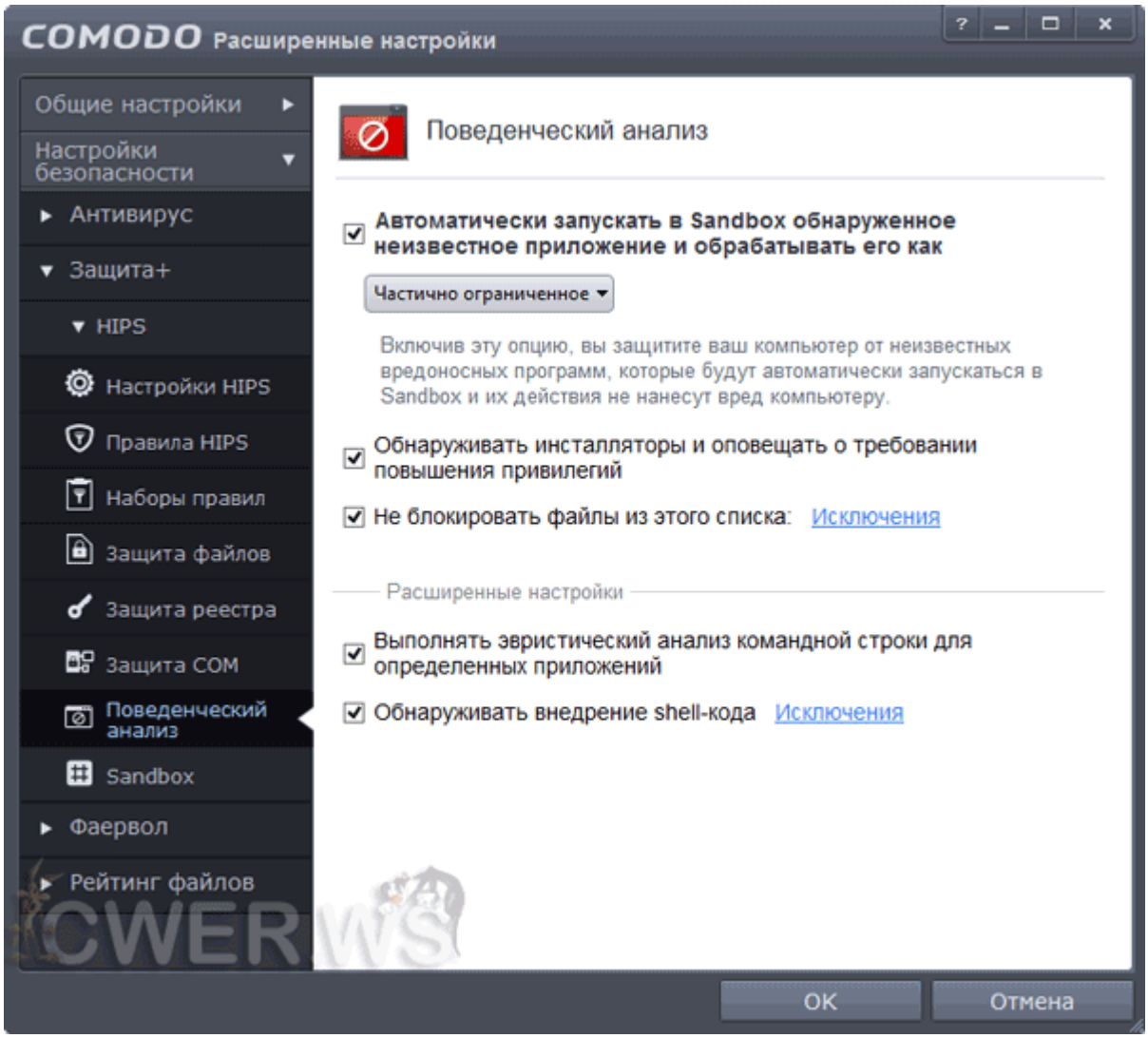
- Не показывать оповещения
- Создавать правила для безопасных приложений
- Адаптировать режим работы при низких ресурсах системы
- Блокировать все неизвестные запросы, если приложение закрыто
- Включить режим усиленной защиты

Однако, владельцы слабых компьютеров могут адаптировать режим работы модуля "**Защита+**". Приверженцы же максимально возможной защиты (параноидального режима) могут включить усиленный режим.

Думаю, всем захочется, чтобы в оповещениях были подробные пояснения, поэтому оставляем соответствующую галочку.

Обратите внимание, что для изменения некоторых параметров нужна перезагрузка системы.

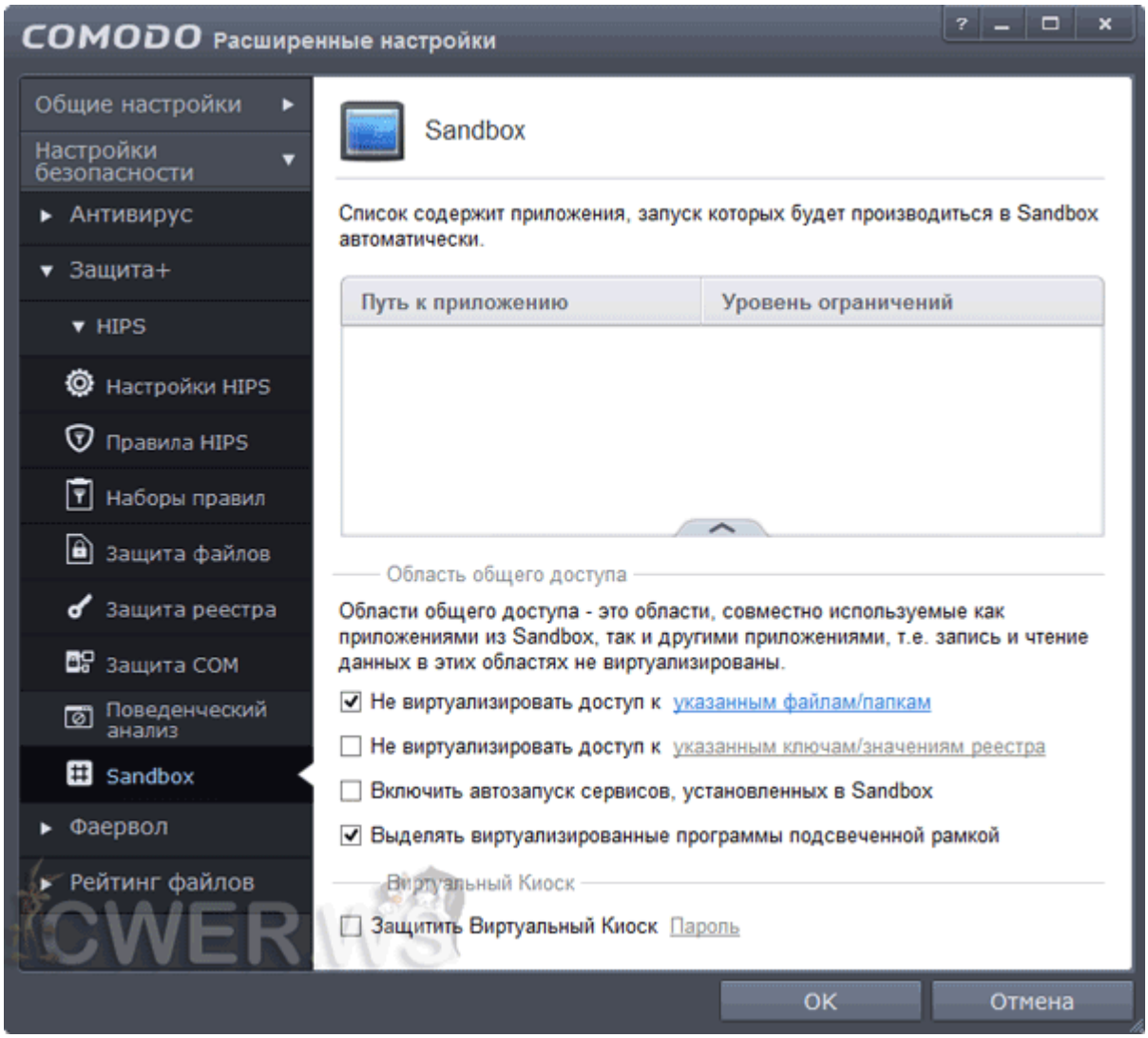
Нажимаем "ОК" и следуем к разделу "**Поведенческий анализ**".



Здесь должны быть активированы все пункты:

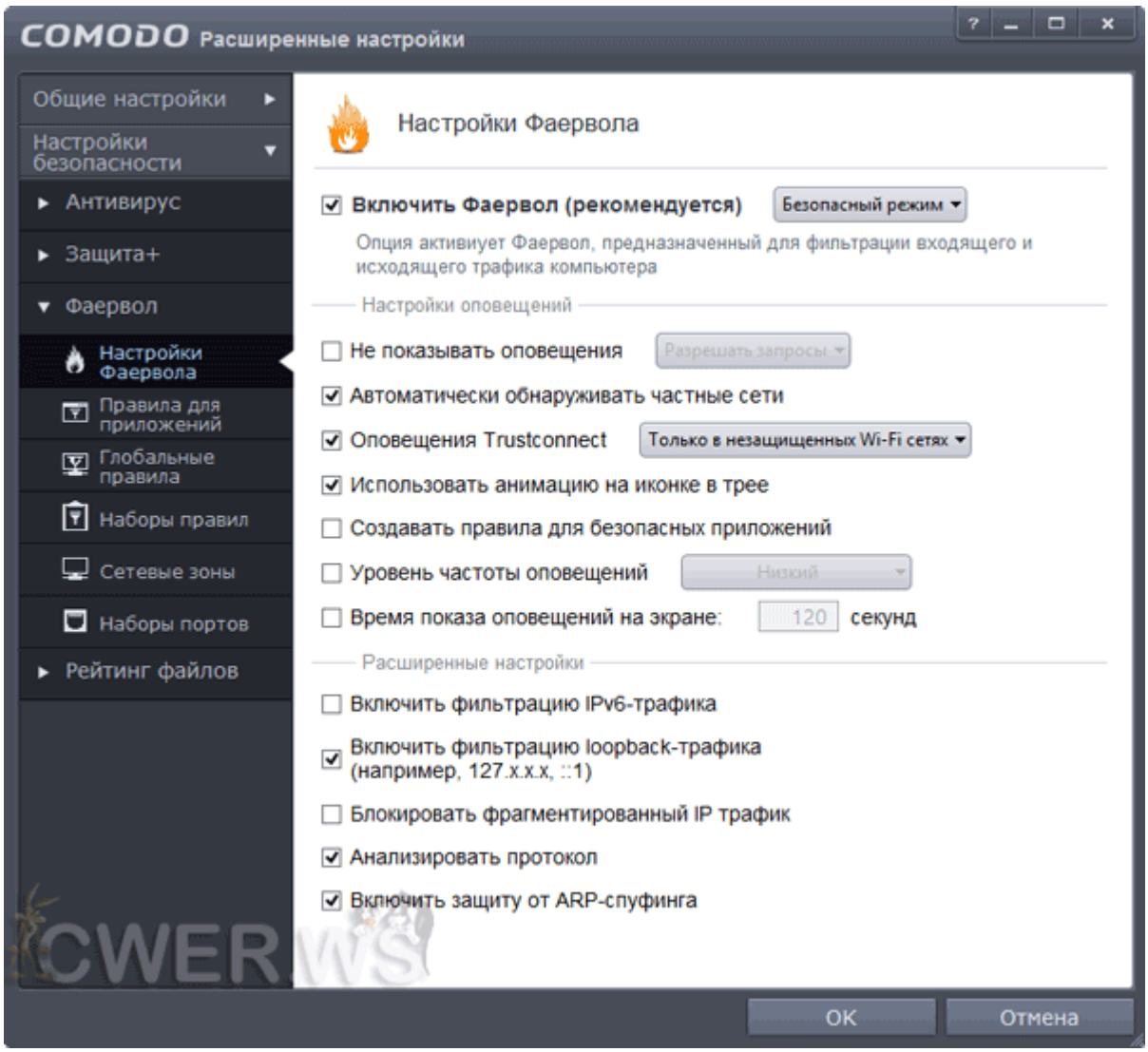
- Автоматически запускать в Sandbox обнаруженное неизвестное приложение и обрабатывать его как частично ограниченное (включив эту опцию, вы защитите ваш компьютер от неизвестных вредоносных программ, которые будут автоматически запускаться в Sandbox и их действия не нанесут вред компьютеру)
- Обнаруживать инсталляторы и оповещать о требовании повышения привилегий
- Выполнять эвристический анализ командной строки для определенных приложений
- Обнаруживать внедрение shell-кода

Крайним пунктом раздела HIPS является Sandbox (в простонародьи "песочница").



Мы не уверены, что большинству пользователей http://cwer.ws/ нужна "песочница". Если же вы все же включили режим Sandbox, советуем для начала настроить этот раздел так, как показано на скриншоте.

После произведения всех настроек нажимаем "ОК" и можем перейти к категории "**Фаервол**".



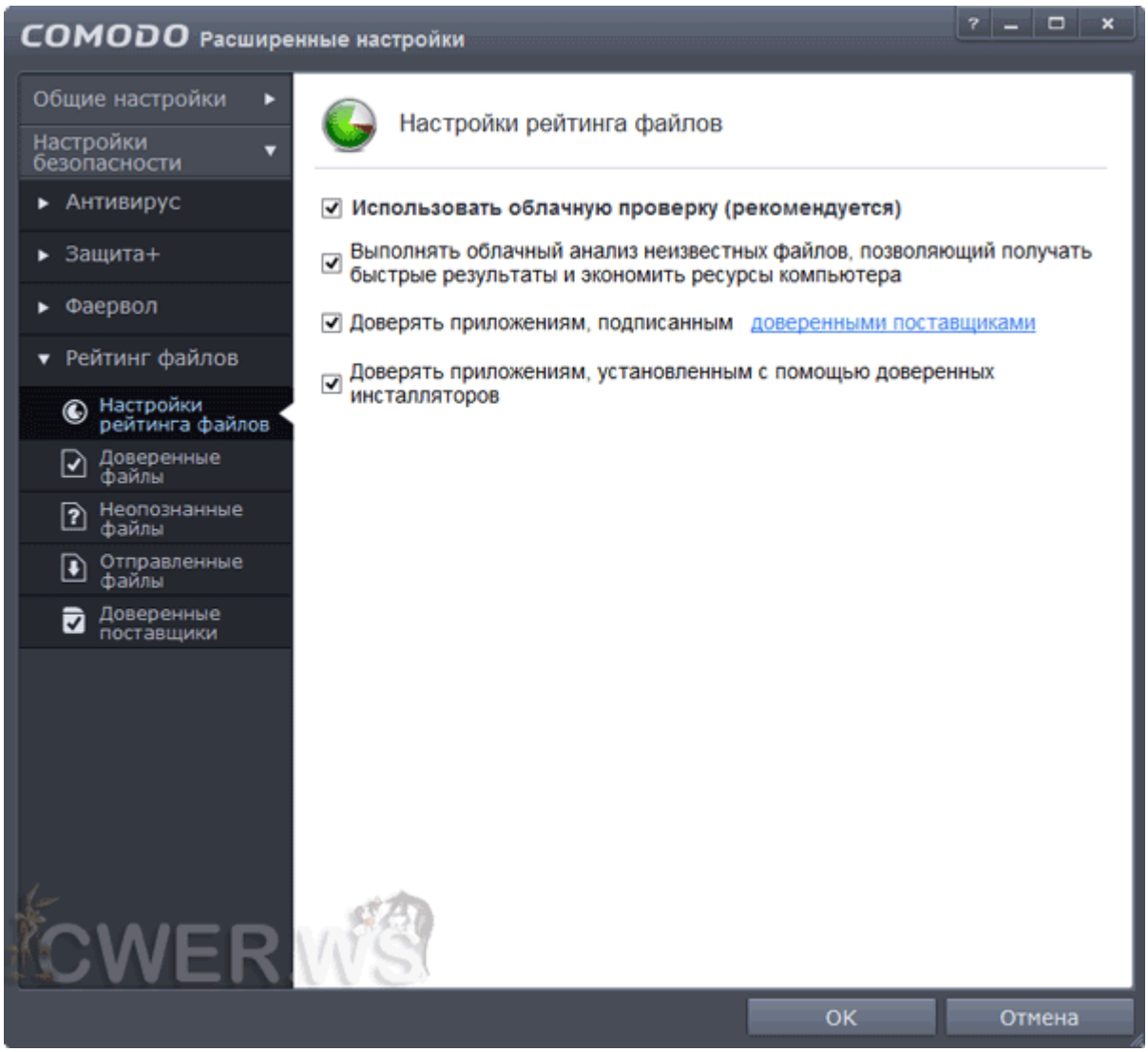
В разделе "**Настройки Фаервола**" мы, конечно, оставляем его включенным для фильтрации входящего и исходящего трафика компьютера.

Далее "просим" COMODO Internet Security автоматически обнаруживать частные сети и показывать оповещения TrustConnect. Нам не по душе автоматическое **создание правил для безопасных приложений**, так как к ним относятся всевозможные проверки обновлений, подлинности и т.п. Большинству пользователей также ни к чему **использовать фильтрацию IPv6**.

Показывать ли анимацию на иконке в трее, решайте сами. Уровень частоты оповещений рекомендуем ставить низкий, чтобы показывать оповещения для исходящих и входящих запросов TCP или UDP протоколов. Если вам хочется больше "общения" с фаерволом, можете повысить уровень.

Мы считаем нужным указать фаерволу включить защиту от ARP-спуфинга и анализировать протокол.

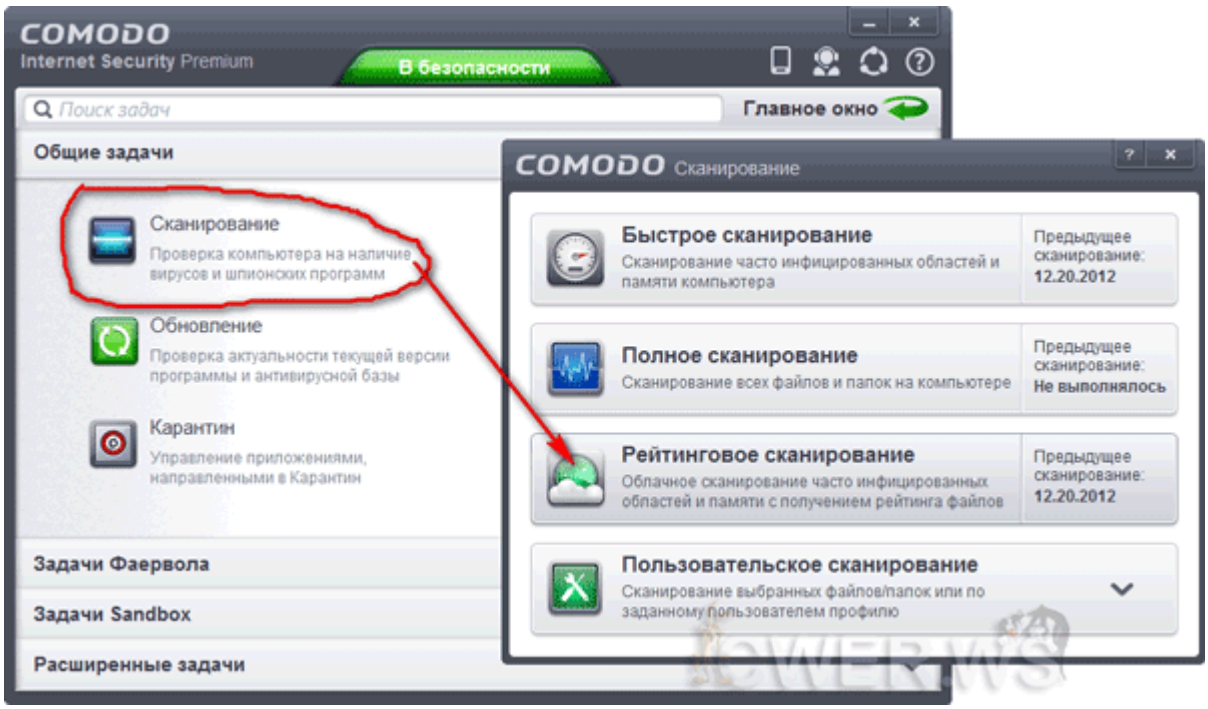
После этого можно перейти к категории "**Рейтинг файлов**".



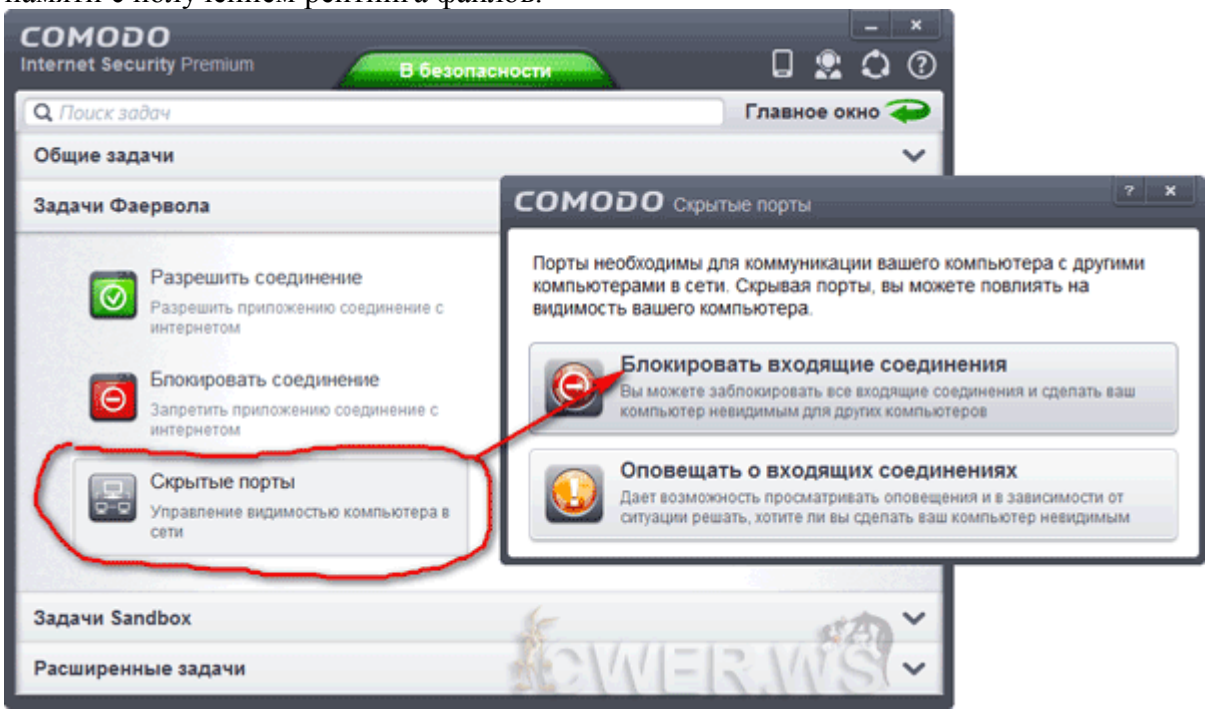
В настройках рейтинга файлов проверяем, что активированы все пункты:

- Использовать облачную проверку
- Выполнять облачный анализ неизвестных файлов, позволяющий получать быстрые результаты и экономить ресурсы компьютера
- Доверять приложениям, подписанным доверенными поставщиками
- Доверять приложениям, установленным с помощью доверенных инсталляторов

Кнопка "ОК" сохраняет установки. Далее следуют еще несколько советов.



Рекомендуется сделать **Рейтинговое сканирование** часто инфицированных областей и памяти с получением рейтинга файлов.



В разделе "**Задачи Фаервола**" выбираем "Скрытые порты", чтобы настроить видимость компьютера в сети.

Если вы планируете в будущем подключать компьютер к различным сетям, то вы можете "попросить" программу **оповещать о входящих соединениях**, и тогда вам придется **принимать отдельное решение для каждого порта**. Этот режим представляется полезным при работе в одноранговых сетях и при работе с приложениями на удаленном рабочем столе, когда необходима видимость вашего компьютера. Вы сможете создать набор глобальных правил, при котором вы будете получать запросы на разрешение любых входящих соединений.

Если же вы одиночка (в сетевом смысле), то укажите программе **блокировать входящие соединения** и скрыть ваши порты для всех входящих соединений. Тогда порты вашего компьютера будут невидимы для всех сетей и Фаервол будет блокировать все входящие соединения. Для большинства пользователей http://cwer.ws/ это самый удобный и безопасный вариант.

После выбора подходящего режима окно закроется.

В разделе "Расширенные задачи" есть пункт "Просмотреть активность". Он позволяет загрузить COMODO Killswitch, чтобы можно было следить за процессами, неизвестными и виртуализированными.

И наконец, если вы включили показ виджета на рабочем столе, то наверняка захотите узнать, что отображают три числовых параметра в центре него. В этом поможет последний скриншот.

На этом наш небольшой ликбез для посетителей http://cwer.ws/ окончен, можете переходить к использованию программного комплекса COMODO Internet Security.

Напомню, что эта статья для новичков, не желающих самостоятельно "копаться" в настройках и для простых пользователей, которые за услуги по "установке антивирусной защиты" привыкли платить "компьютерщикам".

Спасибо за внимание.