COMODO
Internet Security PREMIUM

МОИ НАСТРОЙКИ

АВТОР

Maverick Forever

ОГЛАВЛЕНИЕ

ОГЛАВЛЕНИЕ (продолжение)

ВВЕДЕНИЕ

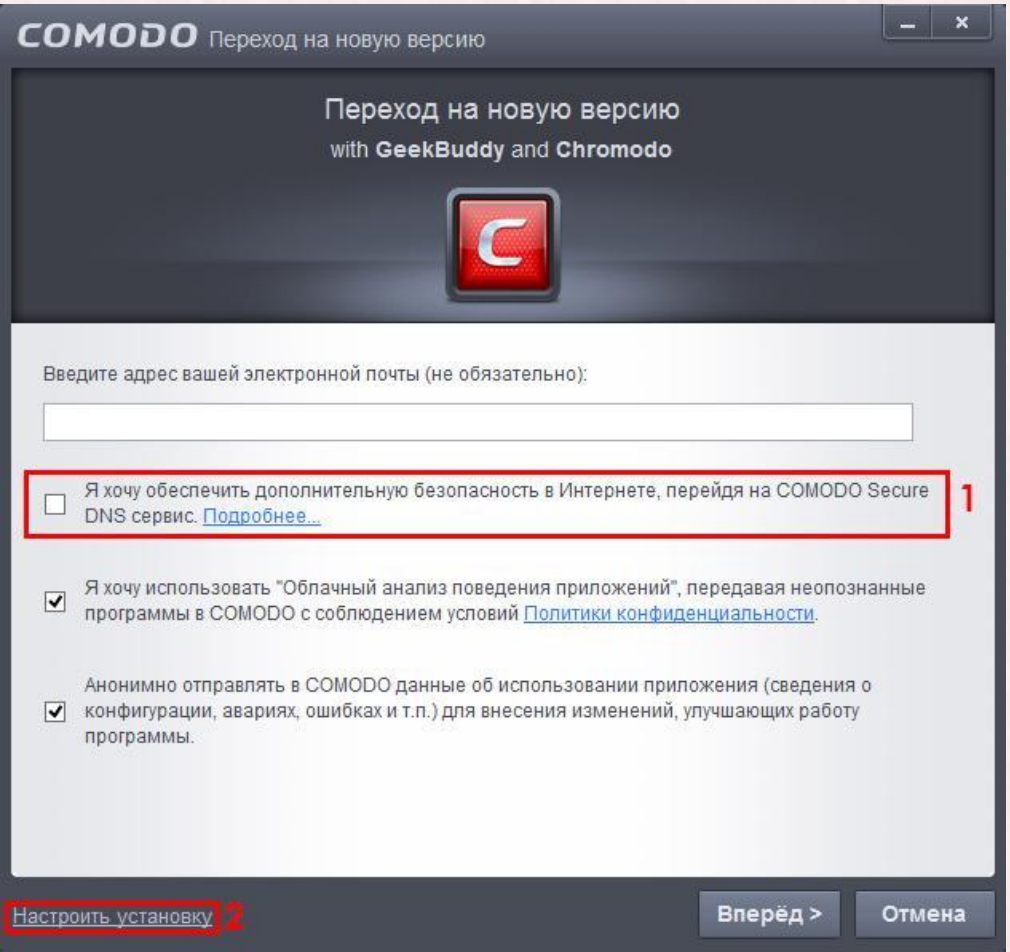
Мой выбор – COMODO Internet Security PREMIUM. Это целиком и полностью бесплатный антивирусный комплекс, сильными сторонами которого являются проактивная защита (HIPS) и брандмауэр (он же фаервол). Кроме того у него есть изолированная среда, т.н. «песочница» (SandBox), изолирующая подозрительные (неизвестные)/вредоносные объекты и не позволяющая им вести свою разрушительную деятельность (возможную и явную).
Он не прожорлив и при должной настройке весьма надежен и не донимает пользователя оповещениями. Я пользуюсь им около 6-7 лет и он меня НИ РАЗУ не подвел (т.е. не пропустил заразу), но справедливости ради хотелось бы еще уточнить что я более-менее опытный пользователь.
Хочется еще сказать несколько слов тем кто боится ставить COMODO, считая (порой по чужим отзывам) его чересчур сложным, параноидальным, забагованным, требовательным к ресурсам и т.д. и т.п. Это не так. Поверьте. Не намного он сложнее чем любой другой антивирус класса Internet Security. Параноидальность есть результат настроек, которые делал ПОЛЬЗОВАТЕЛЬ, т.е. те кто, не разобравшись в тонкостях, стал закручивать гайки сами виноваты в первую очередь. Все в нем весьма гибко настраивается под любого и каждого, нужно лишь немного разобраться. Багов в нем не так уж и много, а те что есть (я не специалист и не стану углубляться), уверен исправят разработчики. Он не требователен к системным ресурсам. А еще он целиком и полностью БЕСПЛАТНЫЙ для всех и каждого. **Зачем платить?**

ВВЕДЕНИЕ (продолжение)

Наверное многие со мной не согласятся, но я считаю что его первоочередная задача ПРЕДОТВРАЩАТЬ заражение, а не бороться с ним, т.е. его желательно ставить на свежеустановленную систему (или хотя бы гарантированно чистую).
Для очистки зараженных машин есть отдельный продукт от этой же компании – COMODO Cleaning Essentials и много других продуктов от других компаний.
Повторюсь: мне еще не приходилось после COMODO чистить систему. Я периодически проверяю ее сторонними сканерами и они неизменно отвечают что заразы нет. Это ли не показатель? У меня два компьютера: ноутбук (i7, 8Гб ОЗУ, 7200 rpm HDD, ОС Windows 8.1 x64) и стационарный компьютер (Intel Core 2Duo, 2 Гб ОЗУ, 7200 rpm HDD, ОС Windows XP SP3 x32) и на них он работает исправно и быстро.
Я покажу вам какие у меня настройки и начну с установки этого комплекса, потому что уже на данном этапе пользователю предлагается внести кое-какие изменения…

ОСНОВНЫЕ НАСТРОЙКИ (установка)

1. Я отказался от DNS сервиса COMODO, потому что он не очень эффективен, по крайней мере в RU-регионе, и может создать некоторые проблемы при использовании сети ИНТЕРНЕТ (например он может заблокировать безопасный сайт).



Я оставил включенными «облачный анализ» и «отправку данных о работе программы». Не вижу в этом никаких проблем.
Рекомендую оставить их включенными.

2. ОБЯЗАТЕЛЬНО перейдите к дополнительным настройкам. Сделать это можно нажав кнопку «настроить установку».

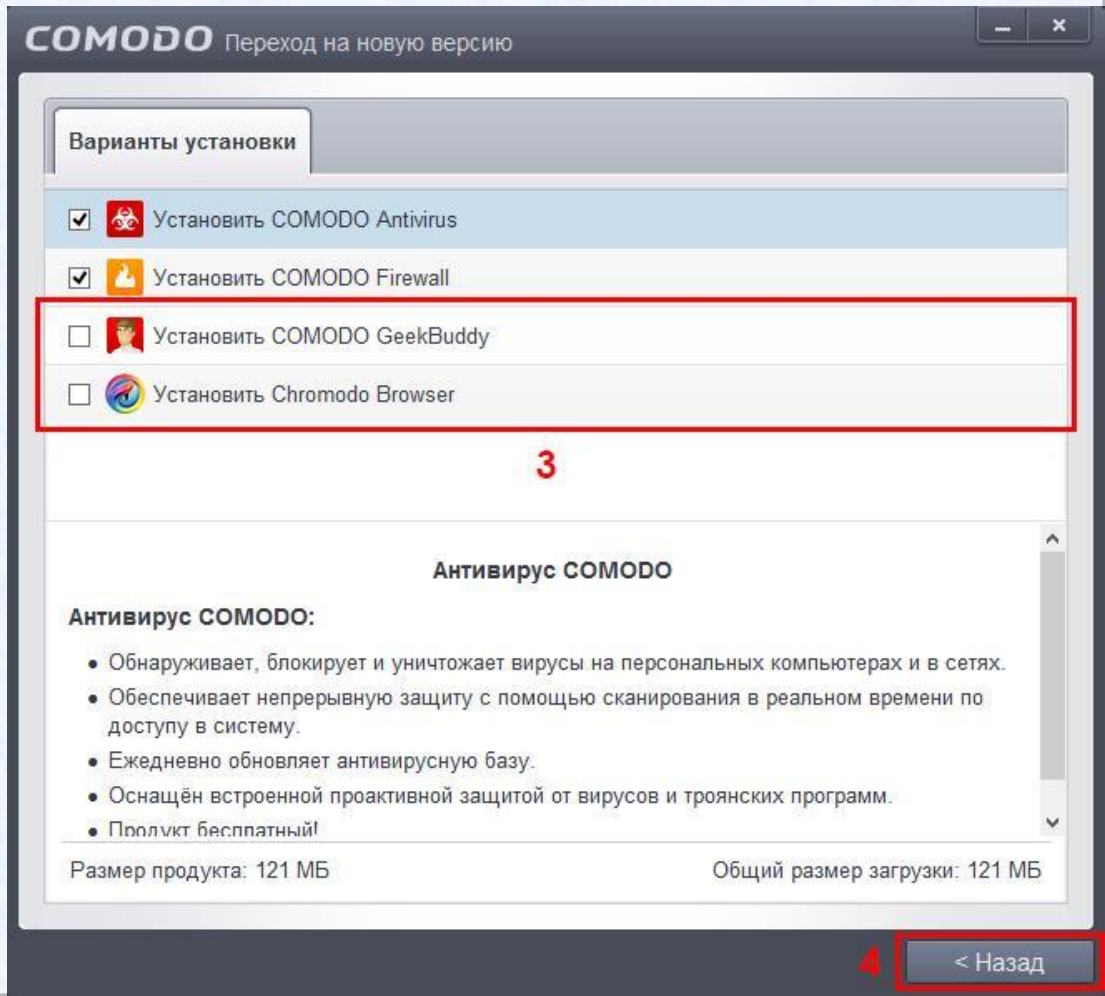
НАСТРОЙКА УСТАНОВКИ (установка)

3. Здесь можно выбрать необходимые для установки компоненты. Я выбрал COMODO Antivirus и COMODO Firewall. Это основные компоненты и они по сути определяют комплекс Internet Security.

COMODO GeekBuddy – это сервис, позволяющий получить онлайн-поддержку. Общение осуществляется в ЧАТе. Сервис платный с пробным периодом. Рекомендую отказаться.

Также я отказался от браузера Chromodo, потому что в нем нет возможности проводить синхронизацию закладок, паролей и прочих данных с серверами Google, а для владельцев смартфонов с ОС Android это не удобно.

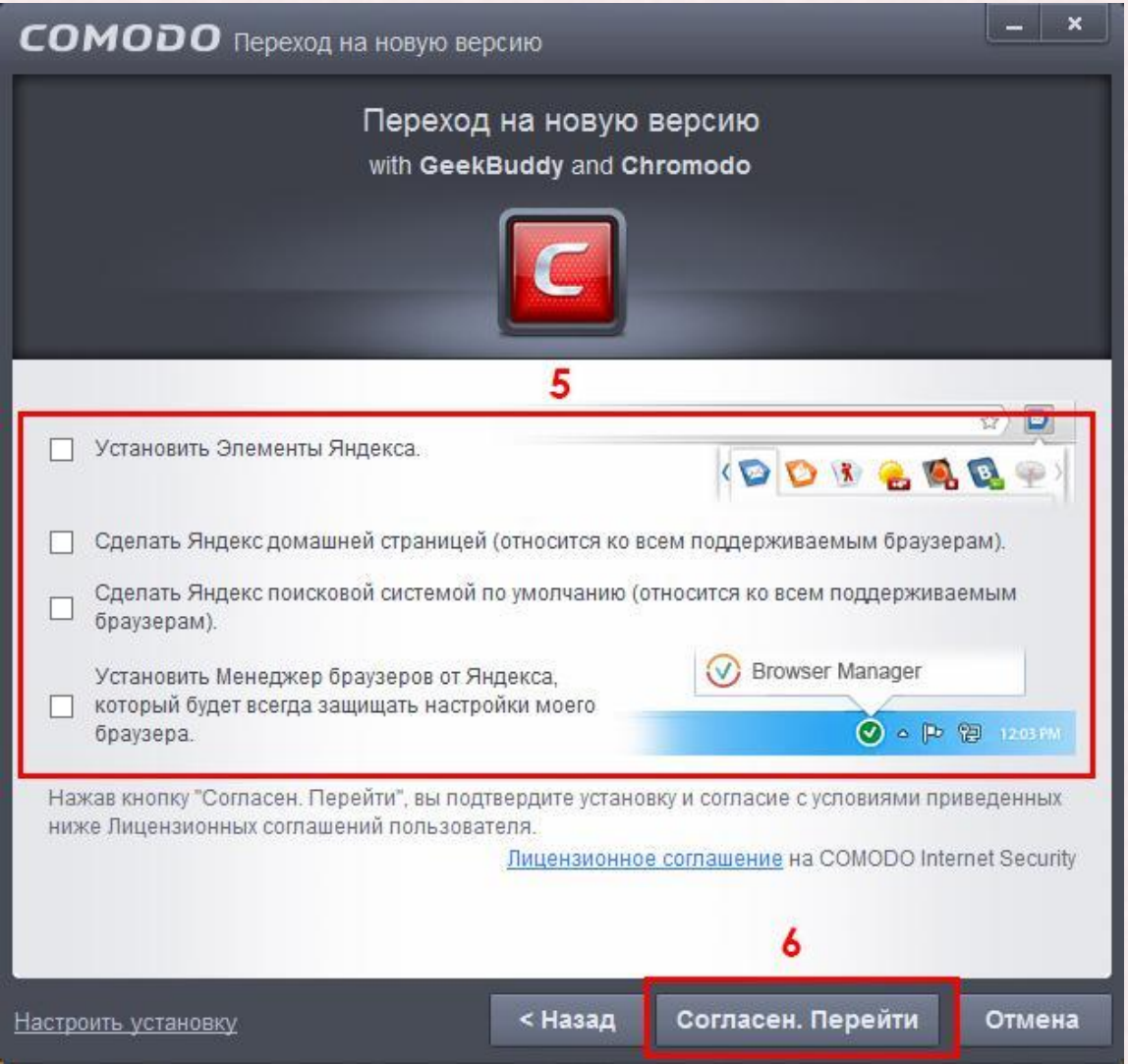
4. Вернемся к предыдущему меню.



НАСТРОЙКА СЕРВИСОВ ЯНДЕКСА

(установка)

5. Выбор необходимых сервисов от компании-партнера «Яндекс». Рекомендую отказаться, чтобы не захламлять систему.

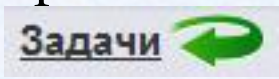


Хотя ярым фанатам сервисов Яндекса это все может пригодится.

6. Для начала установки с выбранными параметрами нажмите кнопку «Согласен. Перейти».
Начнется установка COMODO Internet Security.

РАСШИРЕННЫЕ НАСТРОЙКИ

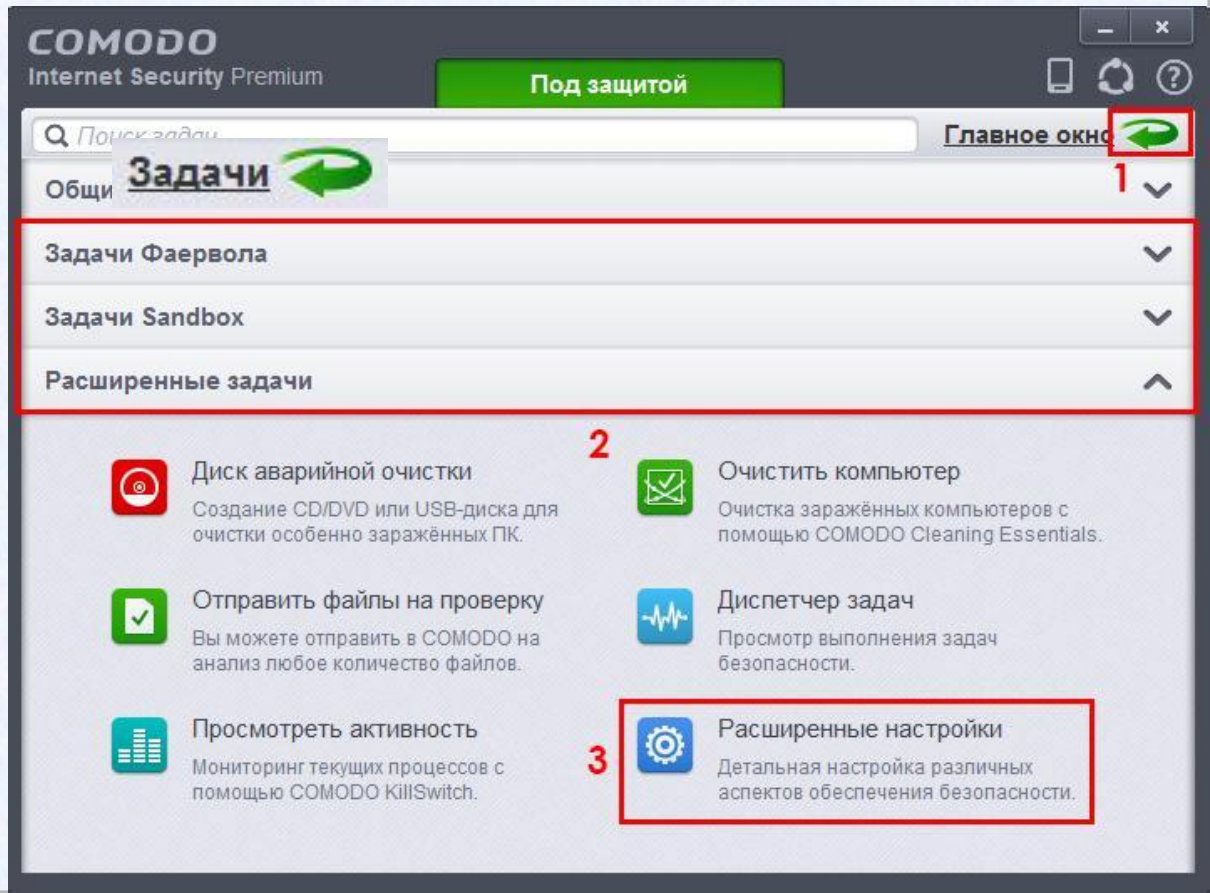
1. Итак мы переходим к более детальным настройкам COMODO Internet Security. Для этого открываем главное окно программы, разворачиваем главное меню через кнопку «задачи» (зеленая стрелочка).



2. Теперь откроем любое дополнительное меню из выделенного блока. В нем (в каждом) есть кнопка «расширенные настройки».

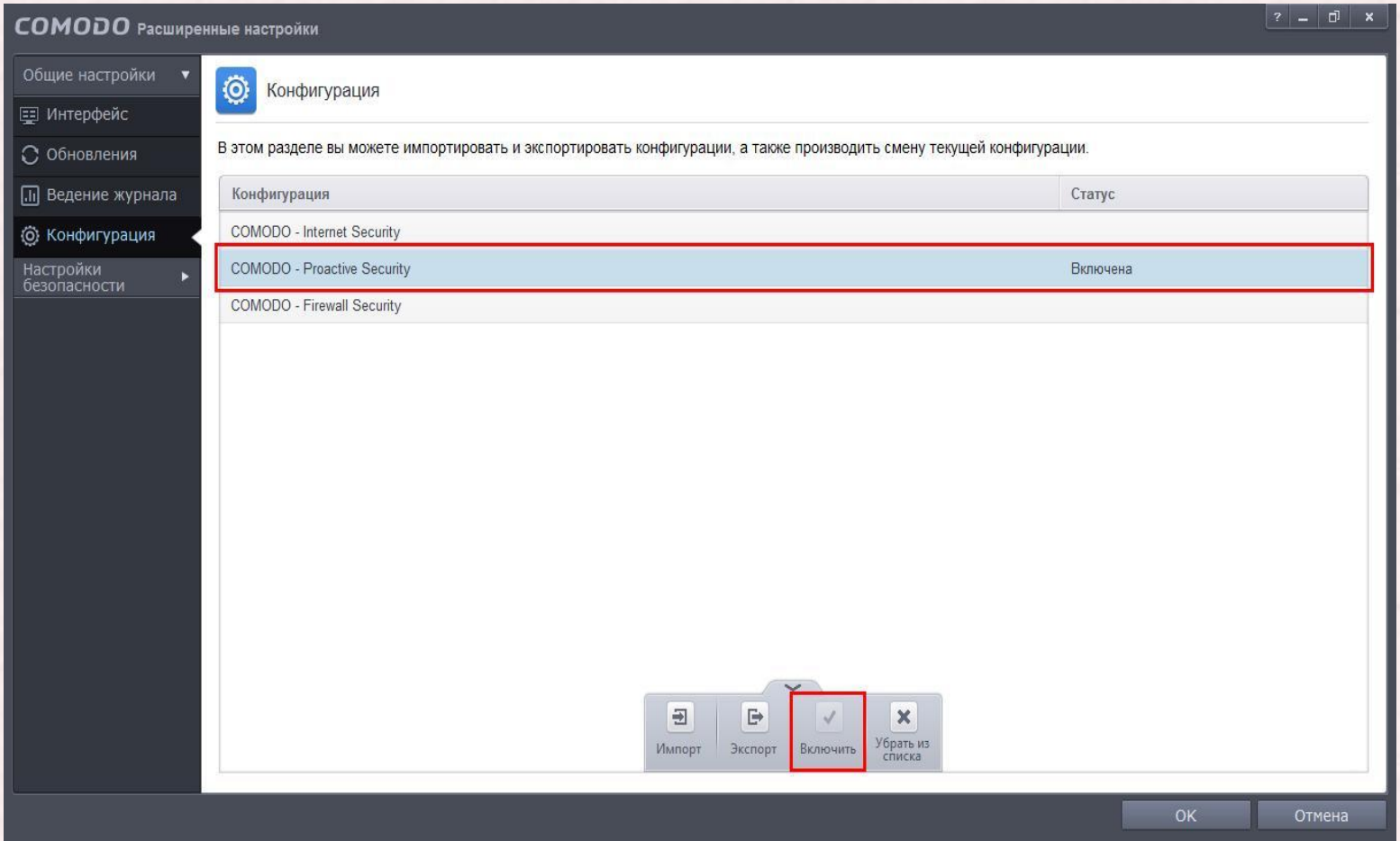
Каждому меню (2) соответствует свой набор дополнительных возможностей и настроек. Рекомендую ознакомится с ними.

3. Открыть «расширенные настройки» можно нажав соответствующую кнопку. Кроме того она есть и в виджете. 



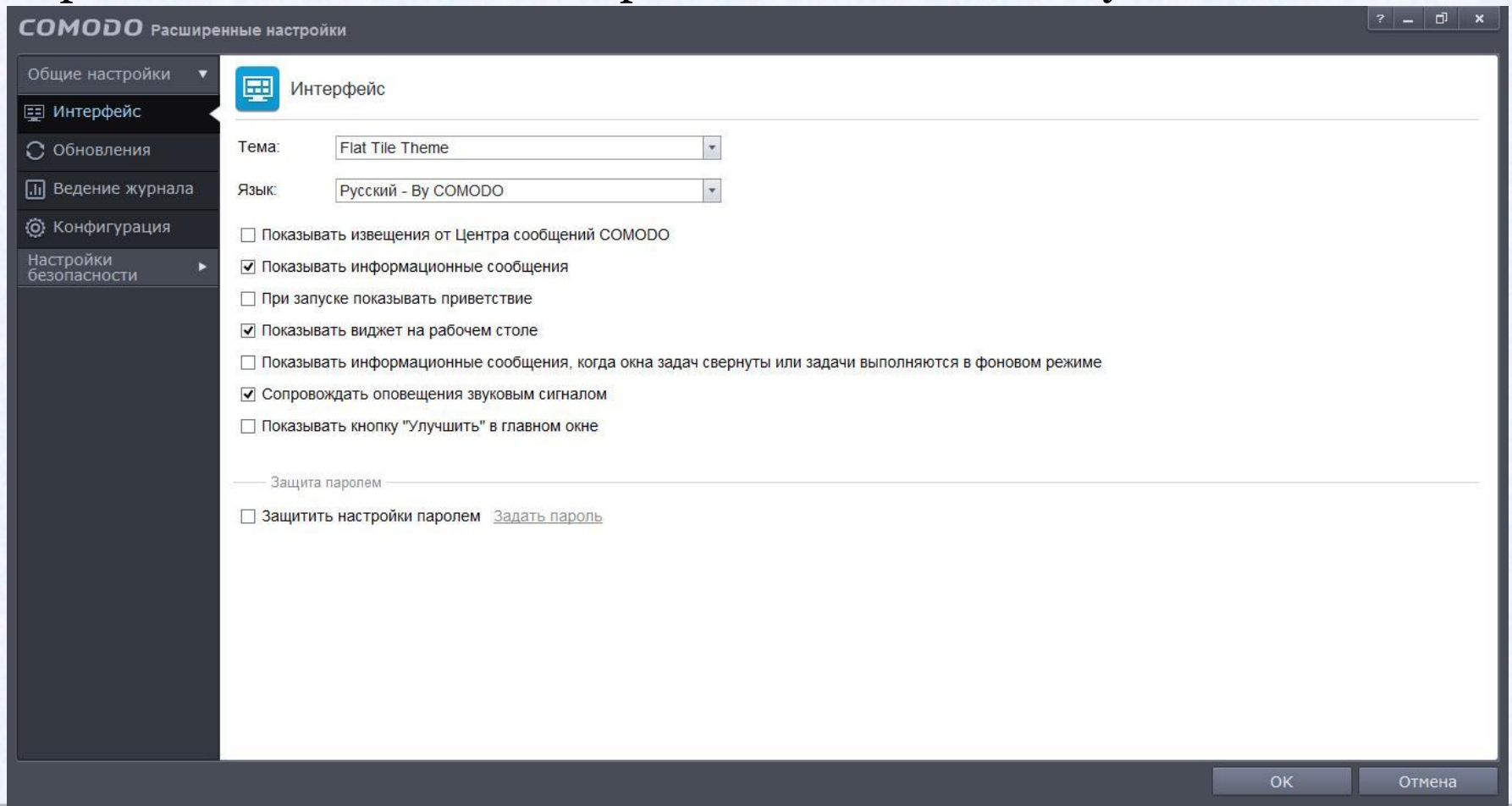
КОНФИГУРАЦИЯ

В расширенных настройках перейдите во вкладку «конфигурация».
Я выбрал конфигурацию Proactive Security, т.к. в данном режиме проактивная защита COMODO работает на все 100%. Конфигурацию желательно изменить в самом начале, сразу же после установки, ибо настройки меняются/сбрасываются. Проактивная защита COMODO одна из его сильнейших сторон, и было бы глупо пренебрегать ею. Рекомендую.



ИНТЕРФЕЙС

Рекомендую поставить галочки как у меня. Рекламы нет, надоедливых приветствий тоже.
Кроме того здесь можно выбрать тему согласно вашему видению прекрасного.
Настройки можно защитить паролем. Но мне это не нужно.

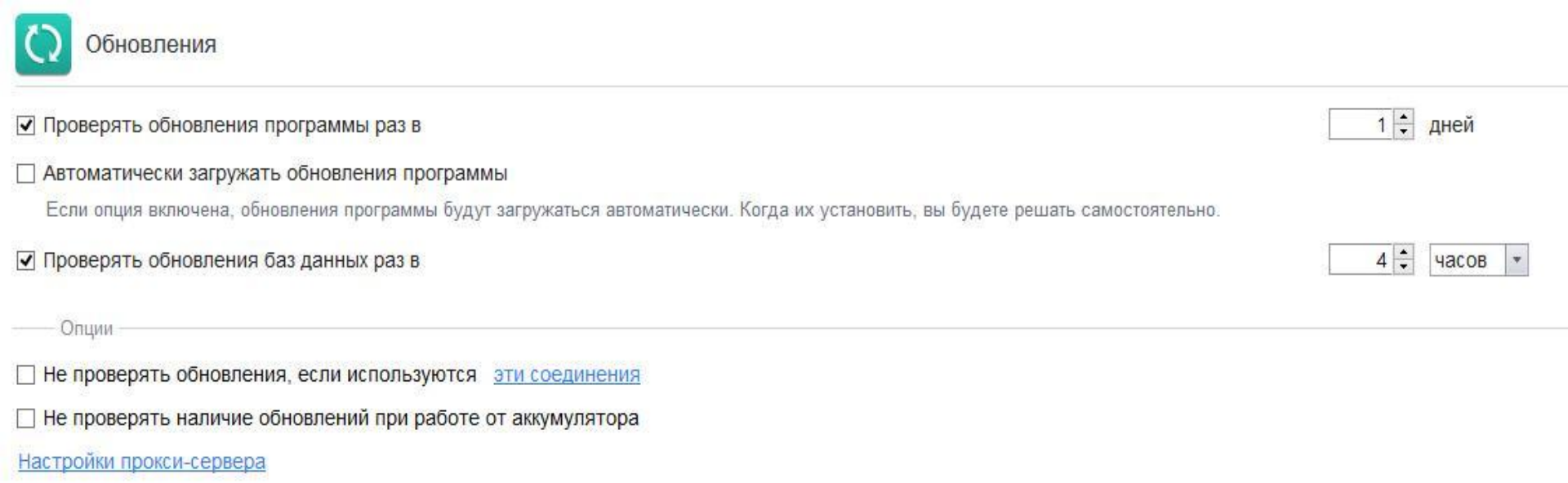


ОБНОВЛЕНИЯ

Такие настройки обновлений стоят у меня. Я отключил автоматическую загрузку обновлений программы, чтобы была возможность в удобное для меня время загрузить их и установить.

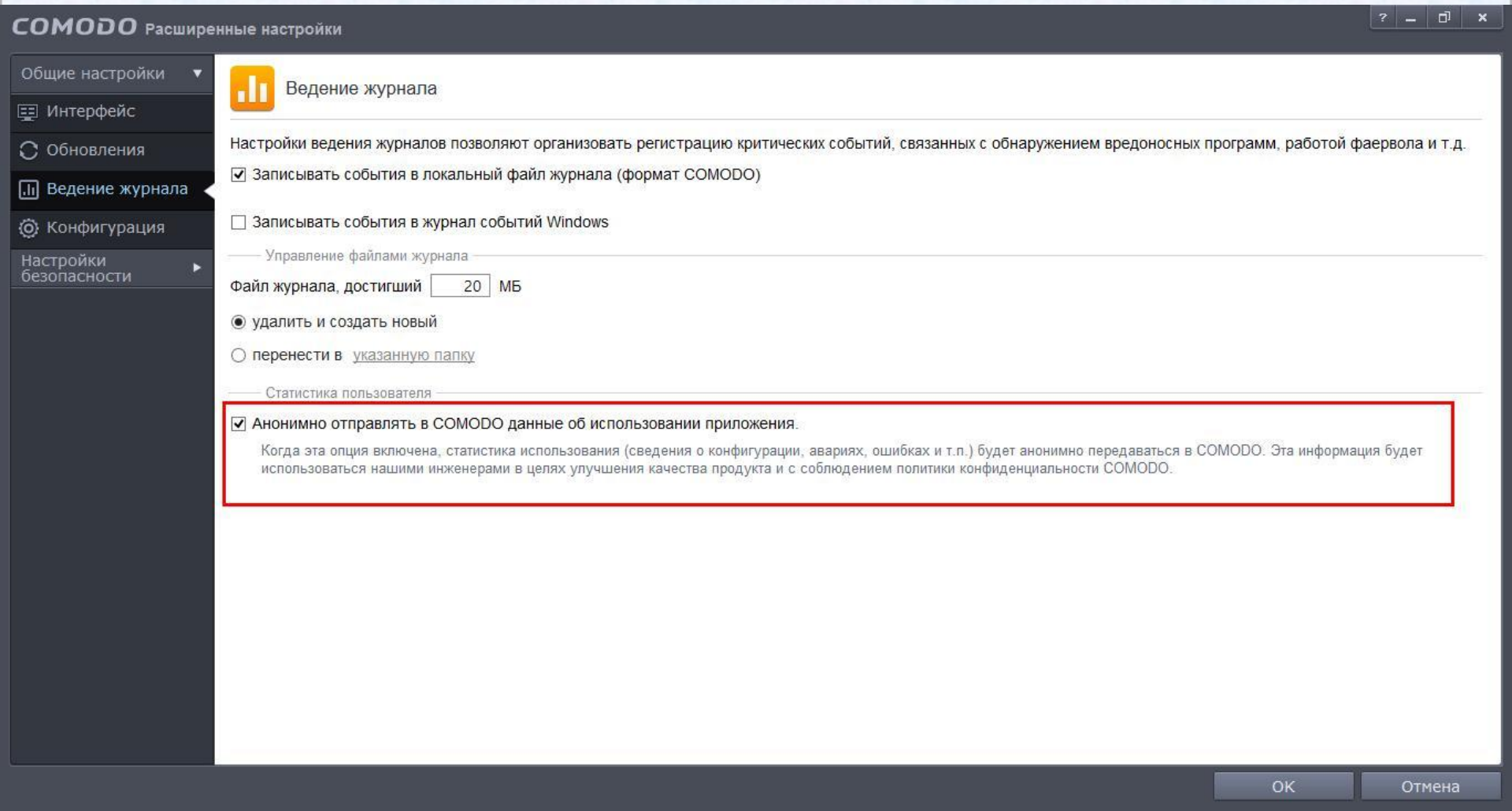
При переходе с одной версии на другу (например с 7 на 8) желательно удалить вручную данную версию, почистить ОС и затем установить новую. Так вы сможете избежать возможных багов (иногда они появляются).

Бывали случаи когда в результате «аварии» на серверах COMODO обновления не выпускались более 24 часов. Заражения системы не произошло. Я считаю что в наше время антивирусный модуль идет как дополнение и ставку нужно делать на проактивные технологии (HIPS) и изолированную среду (SandBox), благо у COMODO есть и то и другое.



ВЕДЕНИЕ ЖУРНАЛА

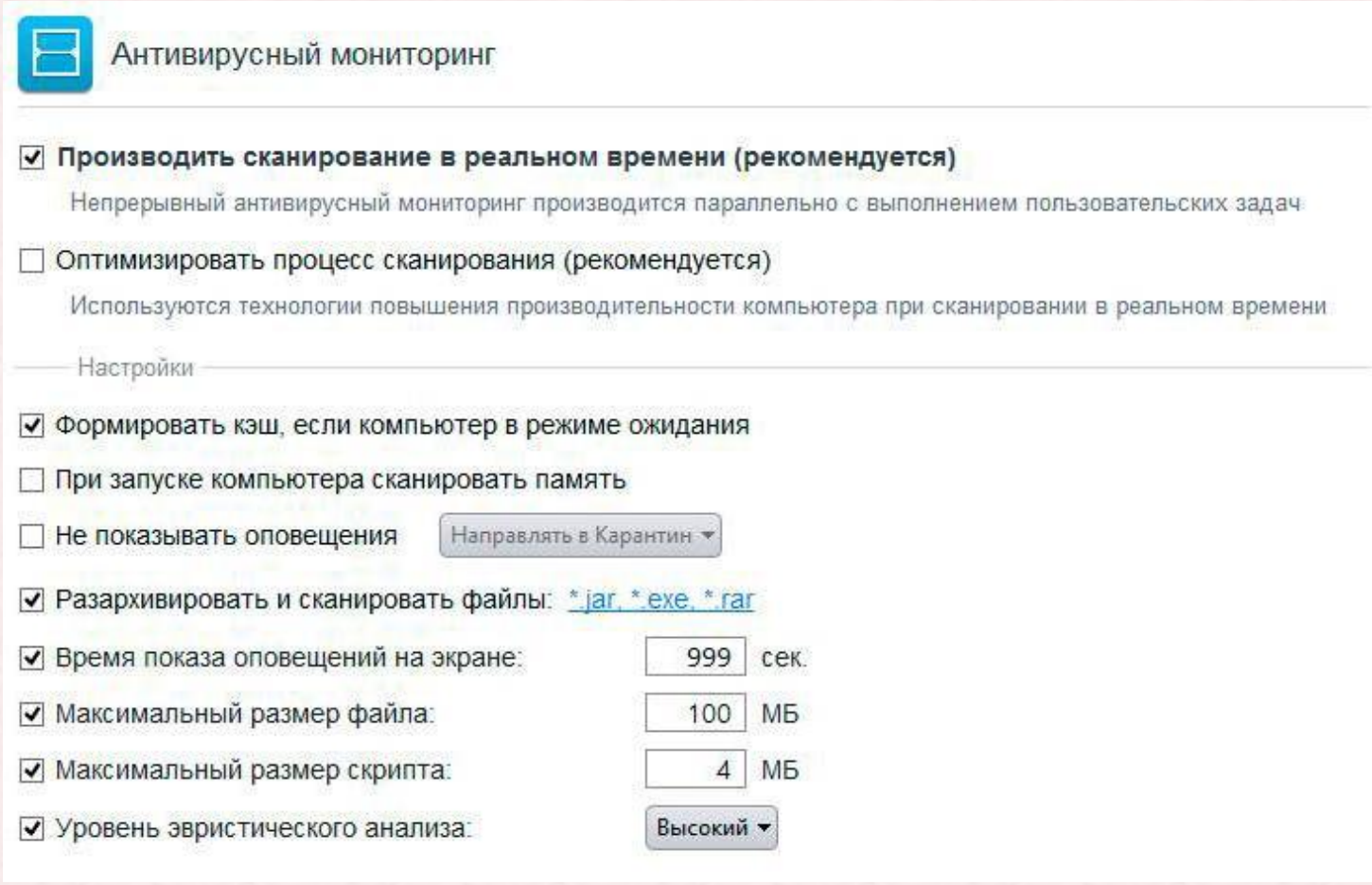
Здесь нет ничего интересного. Вроде даже не менял ничего.
Кстати, если вы вдруг захотите отключить передачу данных о работе программы, то сделать это можно здесь же.



НАСТРОЙКИ АНТИВИРУСА

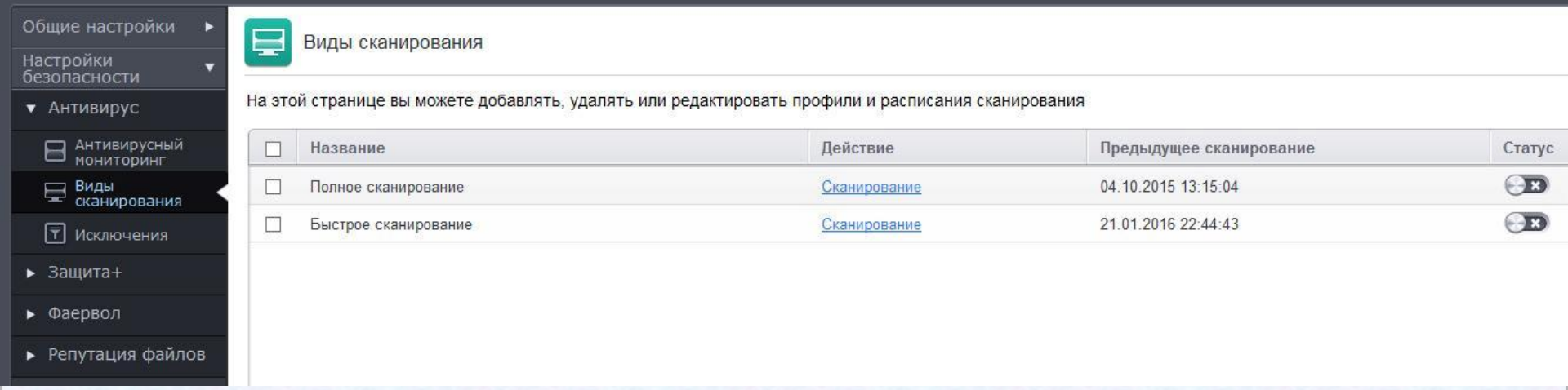
Настройки я «подтянул». Так они мне больше нравятся.
Оптимизацию процесса сканирования рекомендуется включать на слабых машинах. Мне это не нужно. «Максимальные размеры» можно оставить по умолчанию, но я немножко увеличил их, благо мощность ПК позволяет.

Кроме того есть возможность добавлять в исключения файлы, папки и приложения. Это делается через вкладку «исключения».



ЗАПЛАНИРОВАННОЕ СКАНИРОВАНИЕ

Здесь можно добавлять или удалять расписания сканирования. У меня все выключено, т.к. не вижу в этом смысла, но может быть кому-нибудь это пригодится. Сам по себе инструмент довольно таки полезный.
Следующую вкладку «исключения» я не стану рассматривать, потому что там все по умолчанию. Нет ничего интересного.



А мы переходим к...

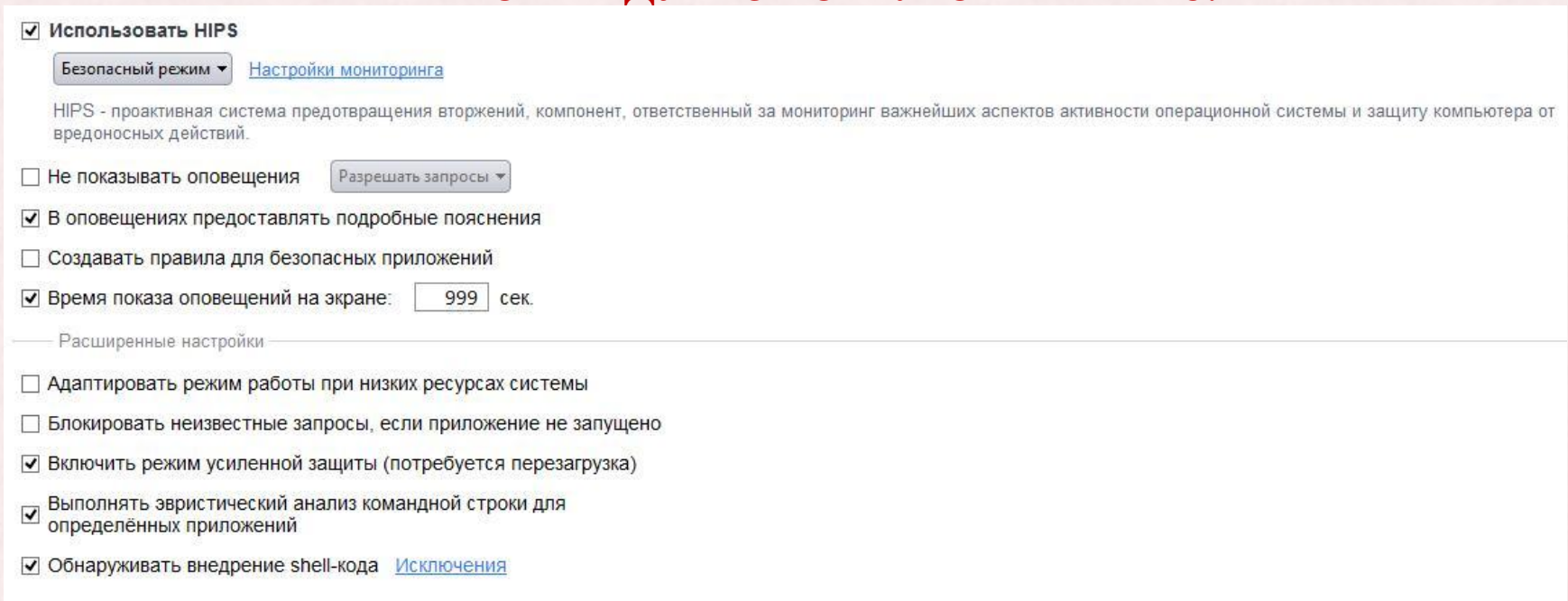
НАСТРОЙКИ HIPS

HIPS активен и настройки «подтянуты», ведь именно на него и опирается COMODO. Он один из лучших.

У меня включен «безопасный режим», как по мне самый оптимальный, НО, сразу же после установки CIS на чистую систему, т.е. не зараженную (Если только уверены!), рекомендую поставить «режим обучения», и позапускать различные программы, чтобы в дальнейшем можно было избежать массы всплывающих оповещений, которые неопытного пользователя могут напугать и запутать.

Если же система свежеустановленная, и предстоит установка массы новых программ (Если вы ставите то что знаете!), вполне подойдет и режим «чистый ПК». В дальнейшем, когда все утрясется, рекомендую поставить «безопасный режим».

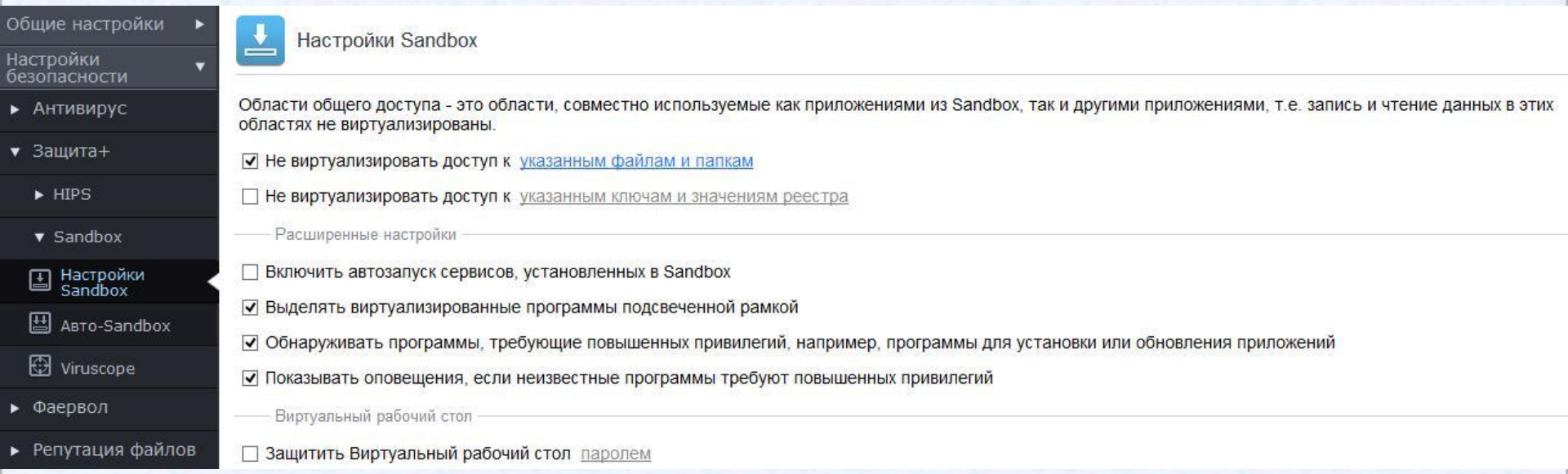
НЕ РЕКОМЕНДУЕТСЯ ОТКЛЮЧАТЬ HIPS!



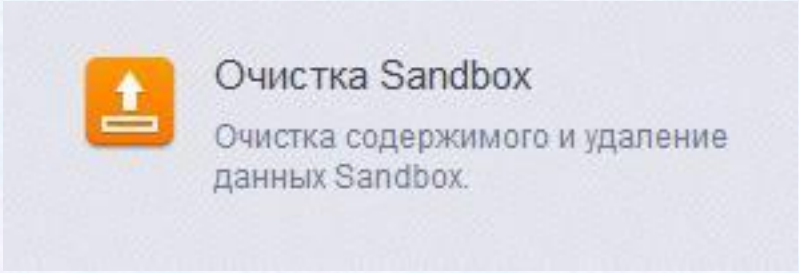
НАСТРОЙКИ SANDBOX

Остальные пункты, посвященные HIPS я пропущу, потому что там все по умолчанию и нет ничего интересного. Все правила «из коробки». Я доверяю COMODO, чего и вам советую. Перейду к изолированной среде.

Вот мои настройки изолированной среды. Неизвестные объекты COMODO автоматически кидает в нее, чтобы они не могли нанести вред. Даже если это ложное срабатывание, перестраховка не помешает.



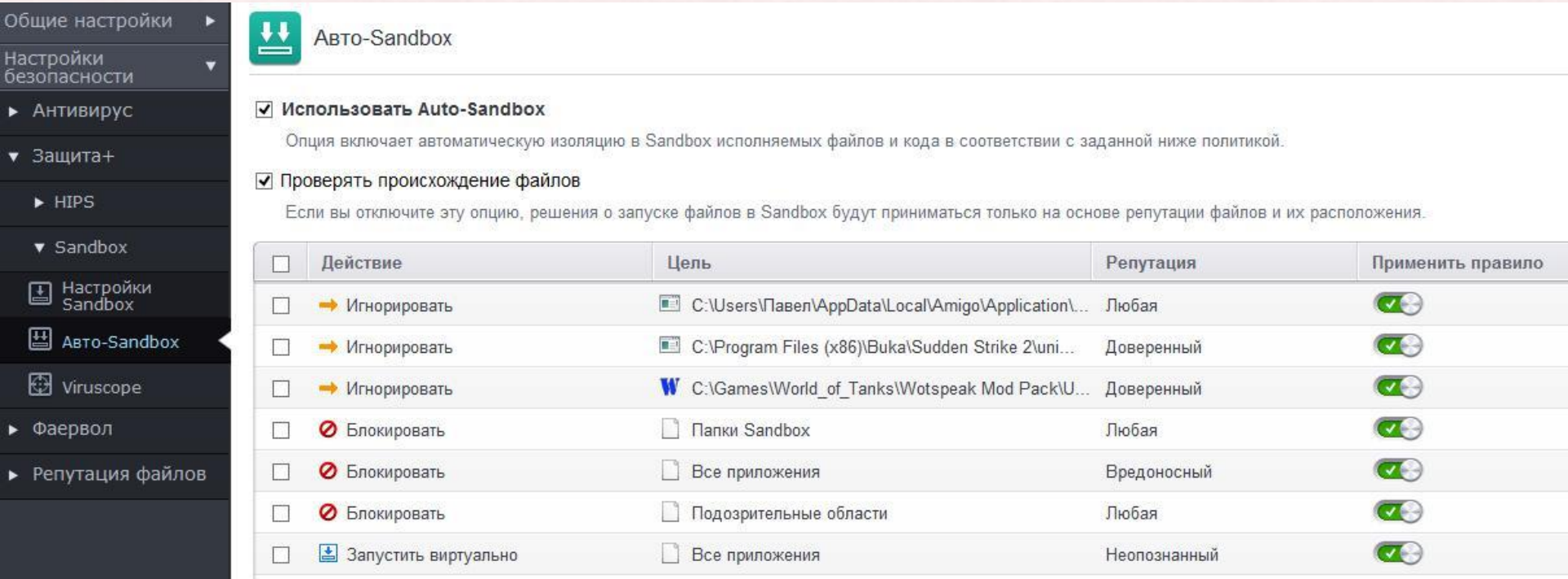
Кстати, очистить SandBox можно через главное меню программы. Вкладка «задачи sandbox».



АВТО-SANDBOX

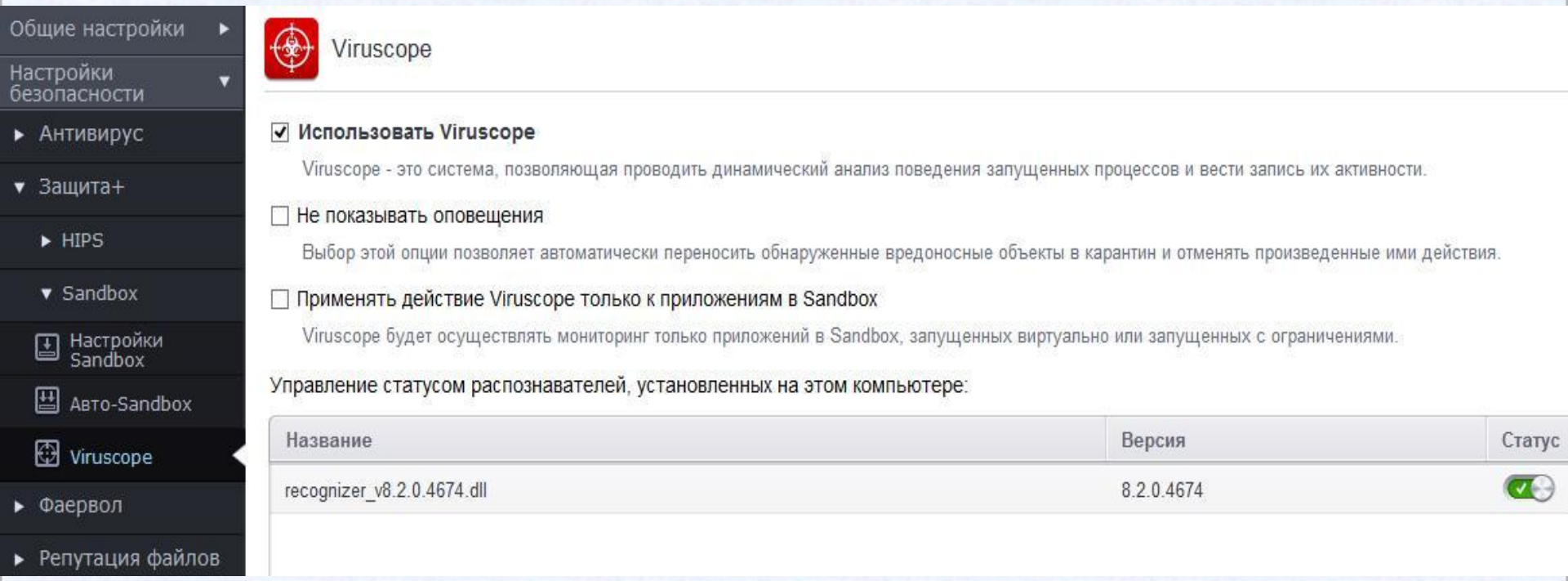
Здесь включается/отключается автоматическая изоляция в «песочнице». У меня она включена. Не беспокоит, ведь созданы правила для всех программ и в особенности тех, которые COMODO считает подозрительными (т.е. неизвестные). Для некоторых я создал исключения, т.к. уверен в их безопасности.

Если вы только установили систему и вам предстоит установка разных программ, то советую отключить авто-sandbox на некоторое время, ибо замучаетесь.



VIRUSCOPE

Viruscope активен. По умолчанию. Не отключал.
Я не стал включать опцию «не показывать оповещения», т.к. люблю сам все контролировать, но т.к. система кристально чистая, то оповещений нет.

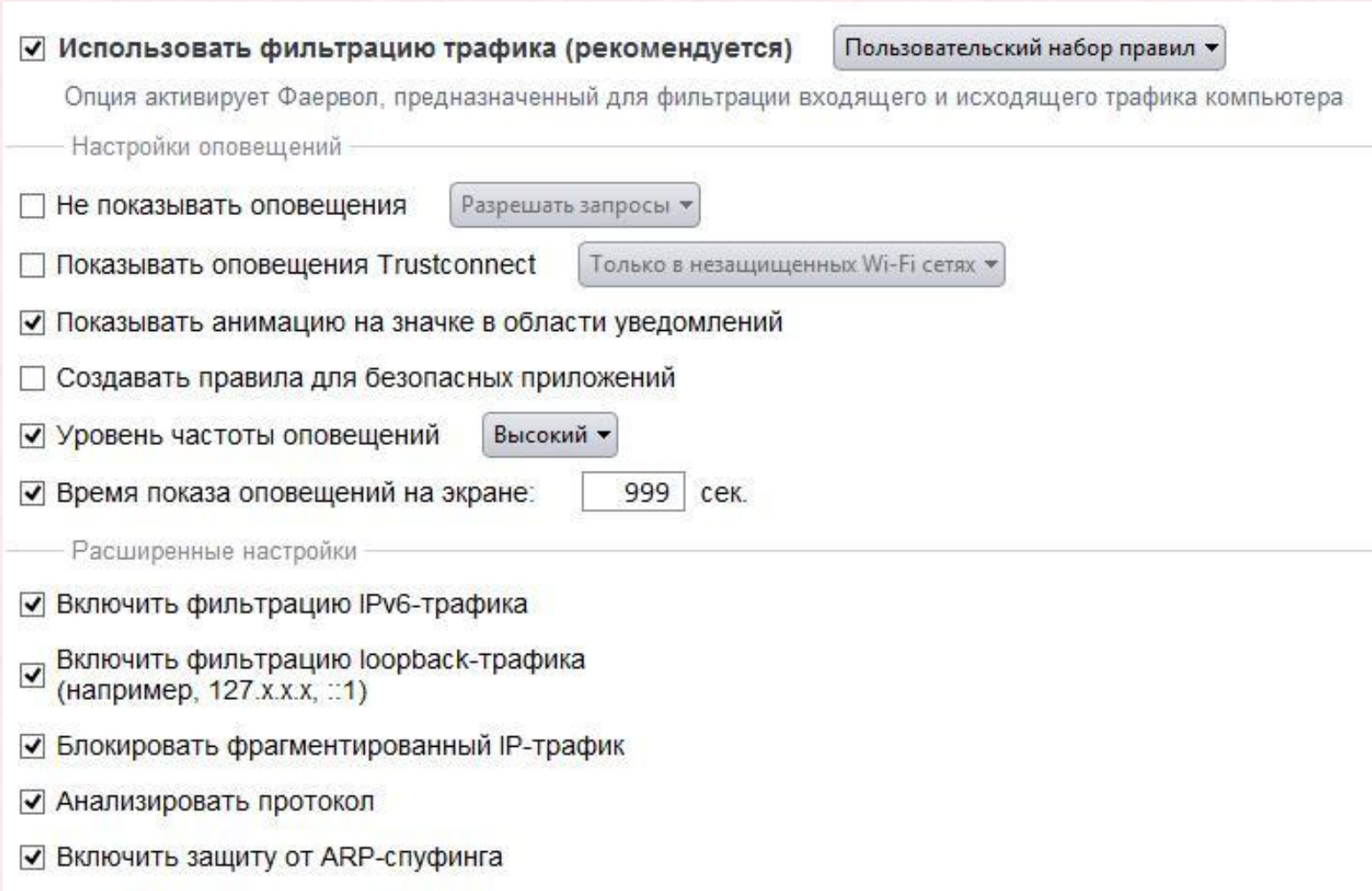


В целом все ясно. Переходим к фаерволу.

НАСТРОЙКИ ФАЕРВОЛА

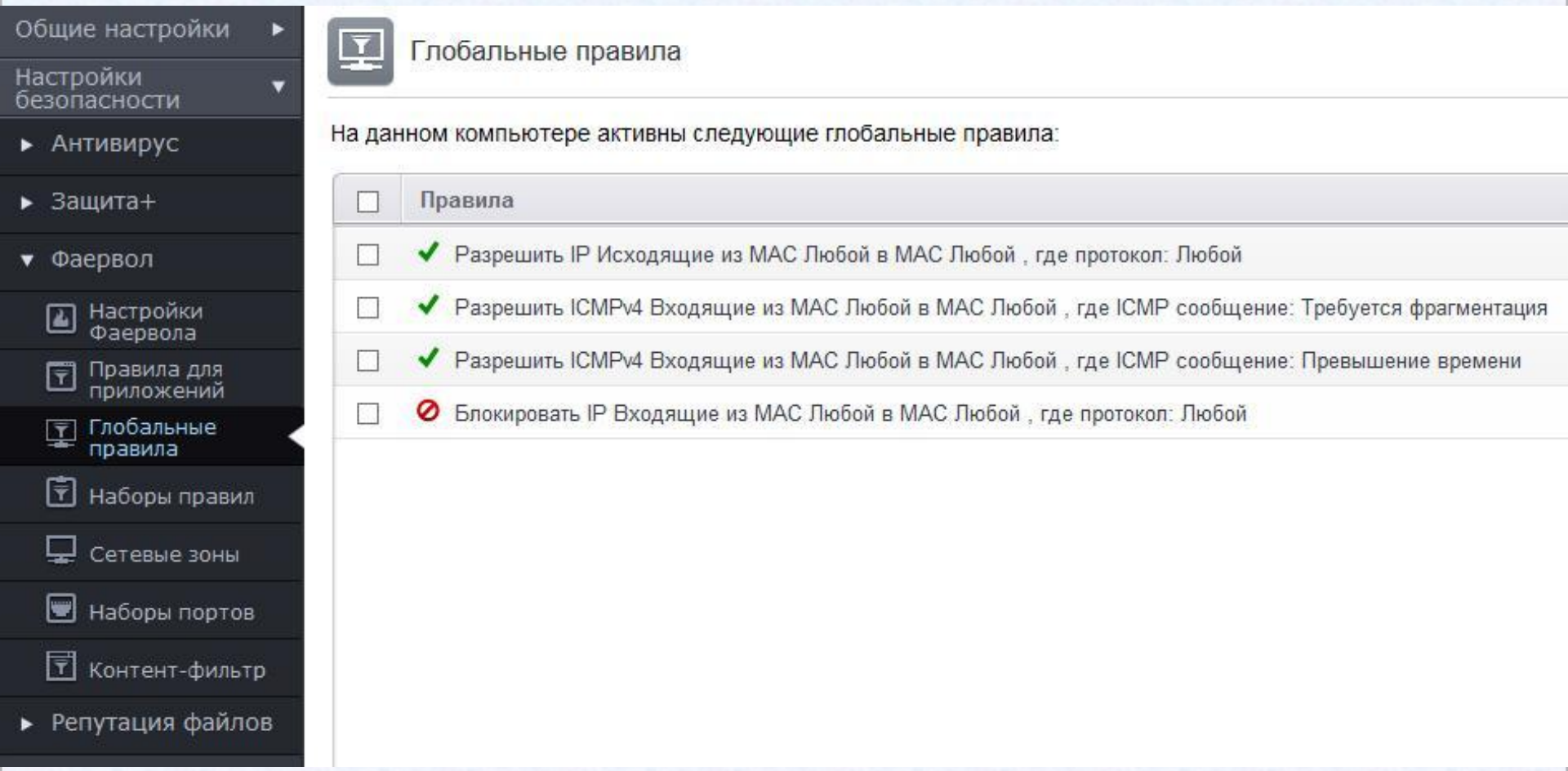
Стоит режим «пользовательский набор правил», потому что сам хочу решать чему нужно разрешить доступ к сети, а чему нет. В целом ничего особенного. Можно настроить его для работы без оповещений. Каждому свое.
Для всех новых программ он выдает оповещение с довольно обширными вариантами выбора правил.

Пункт «создавать правила для безопасных приложений» не нужен для данного режима работы. Для других он может быть полезен.



ГЛОБАЛЬНЫЕ ПРАВИЛА

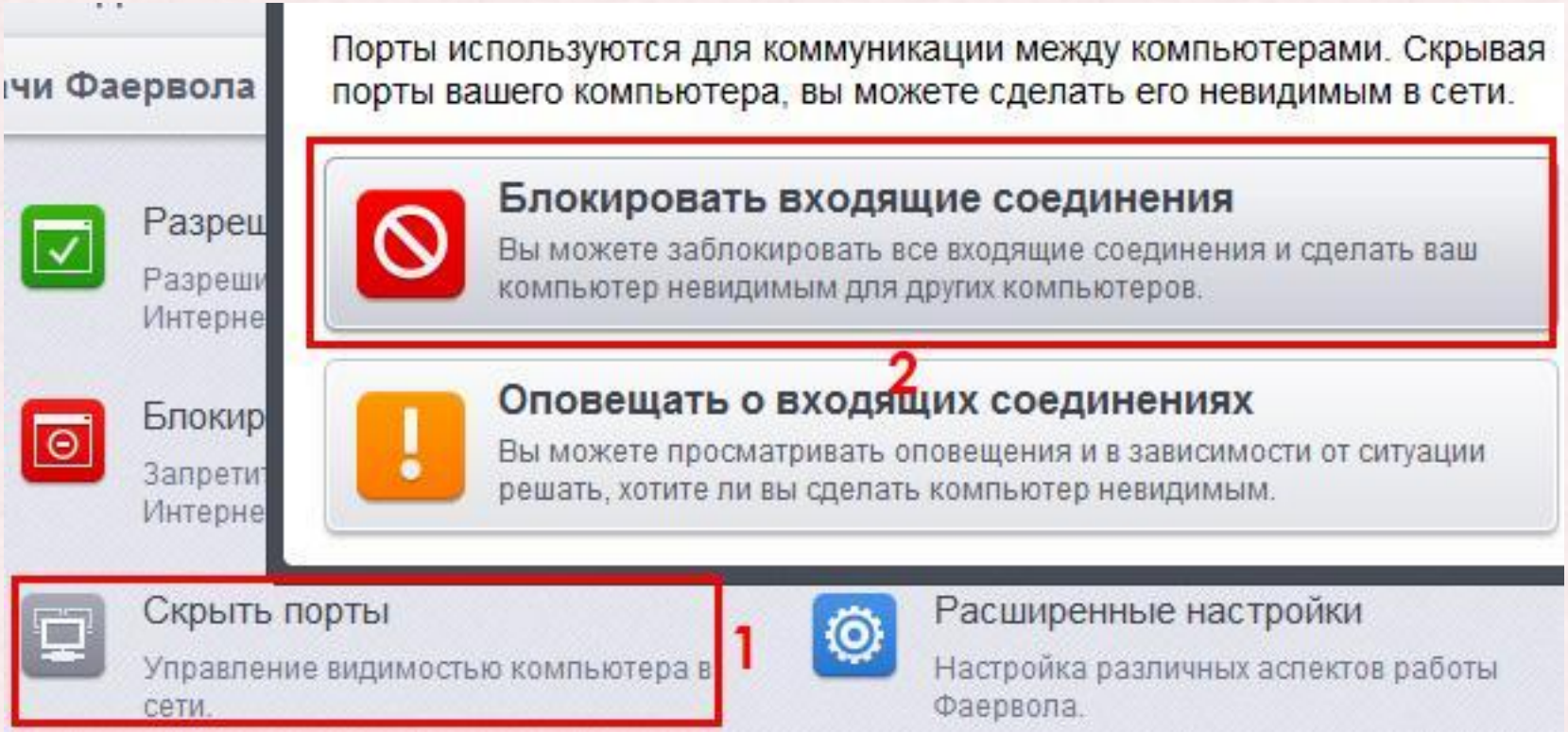
Правила для приложений я пропущу, т.к. они у каждого свои.
Глобальные правила стандартные. С ними проблем никогда не возникало.



Такие глобальные правила рекомендуется поставить через «скрытие портов».
Об этом ниже…

СКРЫТИЕ ПОРТОВ

Порты можно (и даже нужно) скрыть. Это можно сделать через главное меню программы.
Задачи Фаервола – Скрыть порты – Блокировать входящие соединения.



Могут быть проблемы со всевозможными DC++ клиентами!

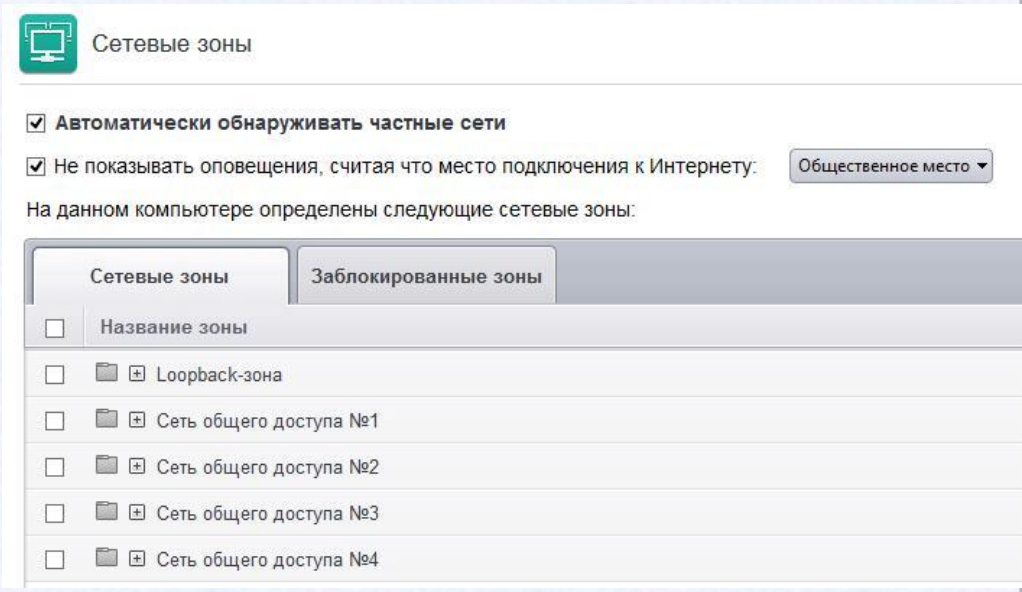
С программой uTorrent проблем нет, но возможно ВАША раздача не будет работать.

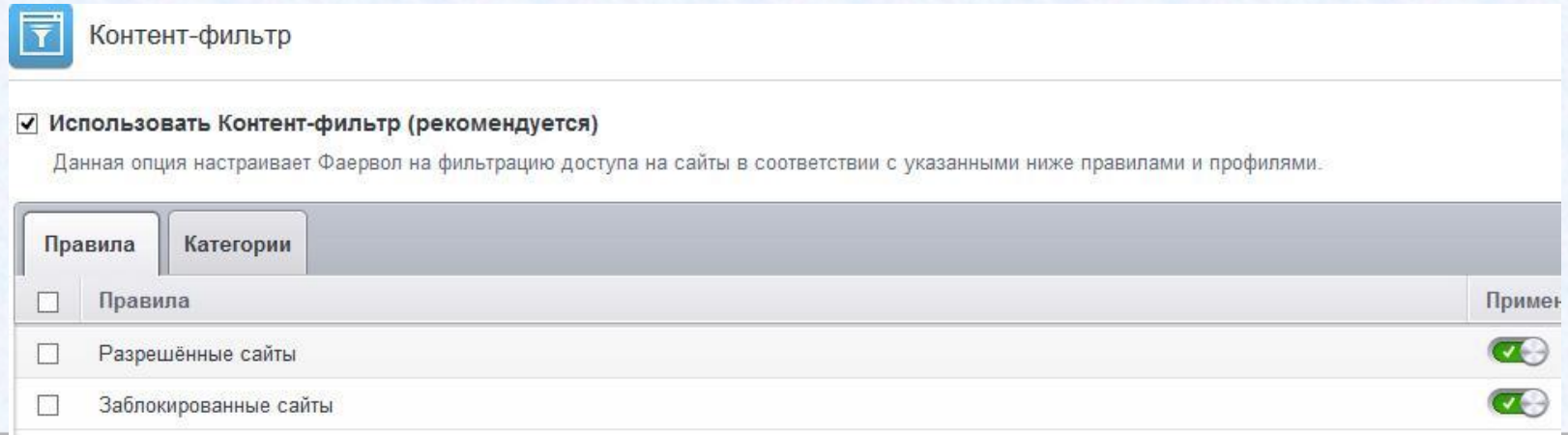
СЕТЕВЫЕ ЗОНЫ

В целях повышения безопасности рекомендую выставить режим для всех сетей «общественное место». Все по умолчанию. С этим проблем никогда не возникало, причем независимо от типа подключения.

КОНТЕНТ-ФИЛЬТР

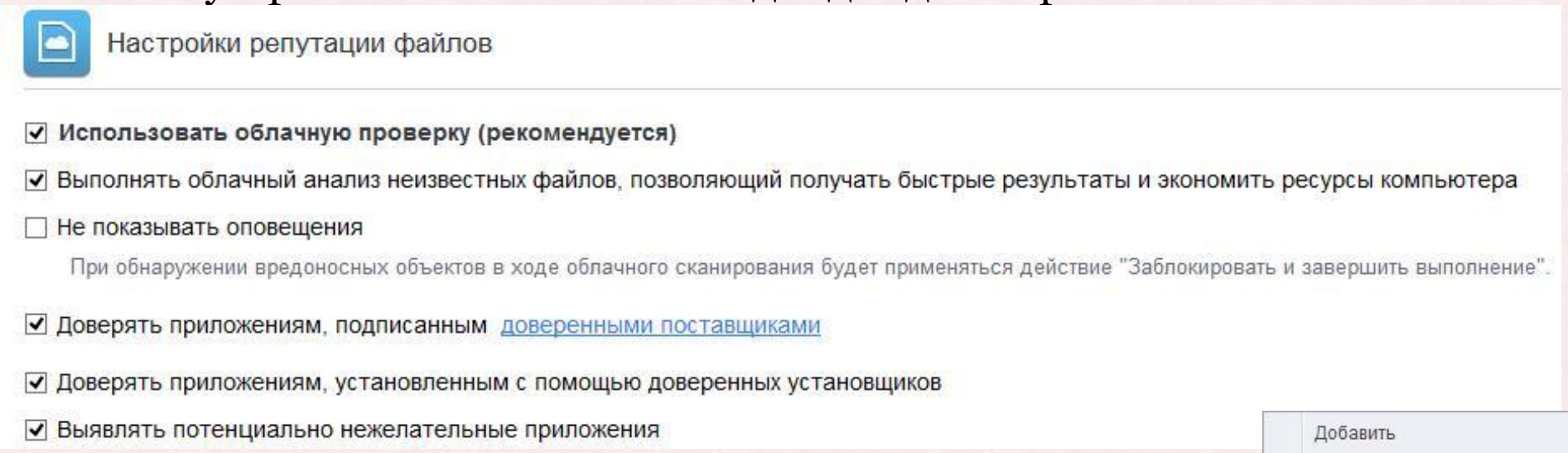
Контент-фильтр у меня активен, но его работа практически не заметна. Веб-защита у COMODO находится в зачаточном состоянии. Рекомендую использовать какое-нибудь расширение для браузера. Например: AdGuard и BitDefender TrafficLight.



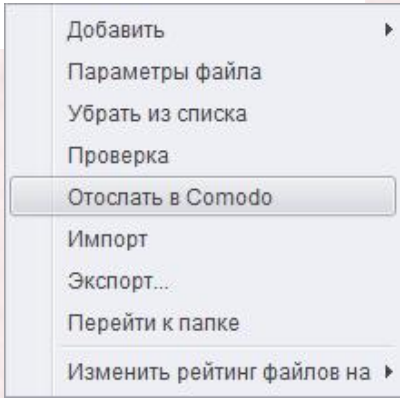


НАСТРОЙКИ РЕПУТАЦИИ ФАЙЛОВ

Облачная проверка у меня включена и проблем нет. Рекомендую ее включить. В целом у COMODO она неплохо работает.
Также у меня активен список доверенных поставщиков. Не вижу смысла не доверять данным от COMODO.
Хотя, для повышения безопасности можно отключить эти опции, но меня и так все устраивает. Это больше подойдет для параноиков.



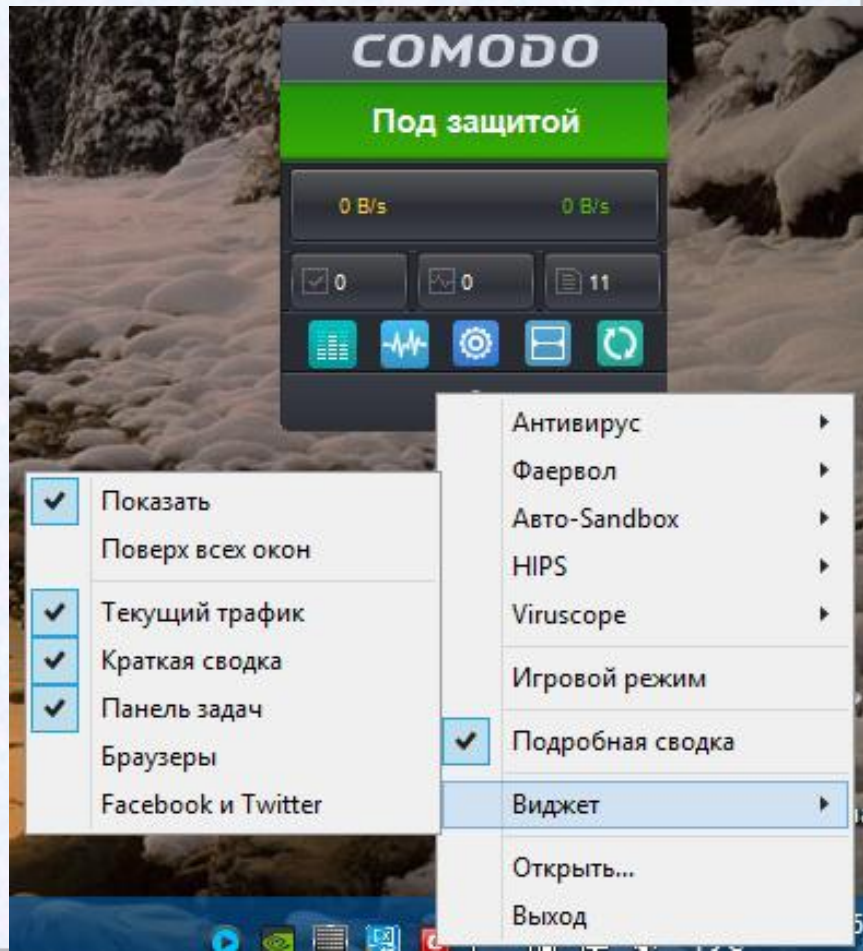
Неизвестные файлы можно вручную отправлять на сервера COMODO для дальнейшего анализа. Сделать это можно через виджет, или расширенные настройки – список файлов.



НАСТРОЙКИ ВИДЖЕТА

Виджет у COMODO не только красивое дополнение показывающее основной статус программы, но еще и довольно таки многофункциональный помощник. Настройки представлены ниже.

Все элементы виджета активны. Он отображает основной статус программы (зеленая область), и также выдает ряд дополнительной информации, такой как: количество изолированных объектов (0), количество выполняемых операций (0) и количество неизвестных объектов (11). Если нажать на любую кнопку, по откроется соответствующее окно с вариантами действий. Его можно полностью отключить.



ИТОГ

Я не специалист в IT-отрасли и не претендую на место оного и называть меня так не следует; я обычный пользователь, может быть чуточку опытнее большинства, но тем не менее ничего нового я вам не смогу сказать. У меня есть лишь опыт, желание и возможность. Опыт использования CIS, желание пользоваться им дальше и возможность показать вам основные моменты данной программы.
Я постарался наглядно представить вам все свои настройки, естественно мельком, особо не вдаваясь в подробности, но надеюсь что этого будет достаточно для начала и вы, поборов страх перед новым, доселе неизвестным «монстром» ступите в темноту его пещеры и поймете что он не так страшен, а пещера озаряется светом.
Надеюсь вы почерпнете для себя что-то новое и используя это превзойдете свой негативный опыт на пути к познанию. Не нужно бояться COMODO как какого-то хищного зверя. Главное разобраться с ним, настроить под себя и он станет непреодолимой крепостью, защищающей вас; станет вашим другом.
Не делайте негативных выводов по чужим отзывам. Пробуйте сами!
Кроме CIS есть ИДЕОЛОГИЯ COMODO. Я принимал участие в переводе статей и проникшись идеей заложенной в них, уже не смогу променять CIS на что-то другое.
Почитайте статьи и тогда вы лучше будете понимать CIS, ведь помимо цифр и пикселей есть целая идеология.

Creating Trust Online!

Спасибо за внимание!