

# COMODO

## Internet Security

### МОИ НАСТРОЙКИ

АВТОР: Maverick Forever

#моинастройки

3. ИНТЕРФЕЙС
4. ОБНОВЛЕНИЯ И ВЕДЕНИЕ ЖУРНАЛА
5. КОНФИГУРАЦИЯ
6. АНТИВИРУСНЫЙ МОНИТОРИНГ
7. НАСТРОЙКИ HIPS
8. НАСТРОЙКИ SANDBOX И АВТО-SANDBOX
9. VIRUSCOPE
10. НАСТРОЙКИ ФАЕРВОЛА
11. ГЛОБАЛЬНЫЕ ПРАВИЛА И СЕТЕВЫЕ ЗОНЫ
12. КОНТЕНТ-ФИЛЬТР И НАСТРОЙКА РЕЙТИНГА ФАЙЛОВ
13. ИТОГ

Пункт «показывать извещения от Центра сообщений COMODO» убирает всплывающее рекламное окошко в правом нижнем углу на рабочем столе. Рекомендую отключить.



## Интерфейс

Тема:

Язык:

- Показывать извещения от Центра сообщений COMODO
- Показывать информационные сообщения
- При запуске показывать приветствие
- Показывать виджет на рабочем столе
- Показывать информационные сообщения, когда окна задач свернуты или задачи выполняются в фоновом режиме
- Сопровождать оповещения звуковым сигналом
- Показывать кнопку "Улучшить" в главном окне

Защита паролем

- Защитить настройки паролем [Задать пароль](#)

## Ничего интересного.



### Обновления

Проверять обновления программы раз в

1  дней

Автоматически загружать обновления программы

Если опция включена, обновления программы будут загружаться автоматически. Когда их установить, вы будете решать самостоятельно.

Проверять обновления баз данных раз в

6  часов

#### Опции

Не проверять обновления, если используются [эти соединения](#)

Не проверять наличие обновлений при работе от аккумулятора

[Настройки прокси-сервера](#)



### Ведение журнала

Настройки ведения журналов позволяют организовать регистрацию критических событий, связанных с обнаружением вредоносных программ, работой фаервола и т.д.

Записывать события в локальный файл журнала (формат COMODO)

Записывать события в журнал событий Windows

#### Управление файлами журнала

Файл журнала, достигший  МБ

удалить и создать новый

перенести в [указанную папку](#)

#### Статистика пользователя

Анонимно отправлять в COMODO данные об использовании приложения.

Когда эта опция включена, статистика использования (сведения о конфигурации, авариях, ошибках и т.п.) будет анонимно передаваться в COMODO. Эта информация будет использоваться нашими инженерами в целях улучшения качества продукта и с соблюдением политики конфиденциальности COMODO.

Рекомендую сменить конфигурацию сразу же после установки и уже потом переходить к настройке комплекса.



Конфигурация

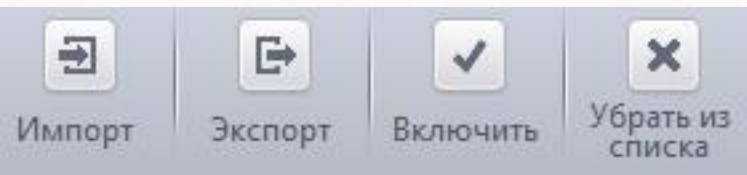
В этом разделе вы можете импортировать и экспортировать конфигурации, а также производить смену текущей конфигурации.

Конфигурация	Статус
COMODO - Internet Security	
COMODO - Proactive Security	Включена
COMODO - Firewall Security	

Я всегда ставлю режим «Proactive Security», т.к. в данном режиме проактивная защита переходит на максимальный уровень защиты: все критические СОМ интерфейсы и файлы защищены. По сути эта эталонный режим защиты в данном комплексе.

Остальные режимы защищают лишь наиболее часто подверженные заражению файлы и папки.

Подробнее от этом можно узнать [ЗДЕСЬ](#).



Конфигурацию можно экспортировать на другой ПК.



## Антивирусный мониторинг

 Производить сканирование в реальном времени (рекомендуется)

Непрерывный антивирусный мониторинг производится параллельно с выполнением пользовательских задач

 Оптимизировать процесс сканирования (рекомендуется)

Используются технологии повышения производительности компьютера при сканировании в реальном времени.

## Настройки

 Формировать кэш, если компьютер в режиме ожидания При запуске компьютера сканировать память Не показывать оповещения

Направлять в Карантин ▾

 Разархивировать и сканировать файлы: \*.jar, \*.exe, \*.rar

Добавил кое-какие форматы.

 Время показа оповещений на экране:

999 сек.

 Максимальный размер файла:

100 МБ

 Максимальный размер скрипта:

4 МБ

 Уровень эвристического анализа:

Высокий ▾

P.S. Виды сканирования не использую.



## Настройки HIPS

**Использовать HIPS**

Безопасный режим ▾

[Настройки мониторинга](#)

HIPS - проактивная система предотвращения вторжений, компонент, ответственный за мониторинг важнейших аспектов активности операционной системы и защиту компьютера от вредоносных действий.

Не показывать оповещения

Разрешать запросы ▾

В оповещениях предоставлять подробные пояснения

Создавать правила для безопасных приложений

Время показа оповещений на экране:  сек.

### Расширенные настройки

Адаптировать режим работы при низких ресурсах системы

Блокировать неизвестные запросы, если приложение не запущено

Включить режим усиленной защиты (потребуется перезагрузка)

Выполнять эвристический анализ командной строки для определённых приложений

Обнаруживать внедрение shell-кода [Исключения](#)

Показывать оповещения при попытках других программ изменять текущие настройки установленных браузеров

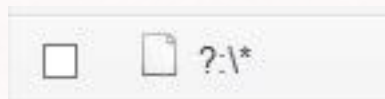
Наборы правил я оставил без изменений.

Также, на всякий случай, в «защищённые объекты» я внёс правило «?:\\*» для защиты от:

- Gpcode.

- Vat-скриптовых вредоносных программ, которые удаляют/скрывают все файлы.

- Вредоносного ПО, которое заражает все исполняемые файлы или все файлы сценариев.





## Настройки Sandbox

Области общего доступа - это области, совместно используемые как приложениями из Sandbox, так и другими приложениями, т.е. запись и чтение данных в этих областях не виртуализированы.

- Не виртуализировать доступ к [указанным файлам и папкам](#)
- Не виртуализировать доступ к [указанным ключам и значениям реестра](#)

## Расширенные настройки

- Включить автозапуск сервисов, установленных в Sandbox
- Выделять виртуализированные программы подсвеченной рамкой
- Обнаруживать программы, требующие повышенных привилегий, например, программы для установки или обновления приложений
- Показывать оповещения, если неизвестные программы требуют повышенных привилегий

## Виртуальный рабочий стол

- Защитить Виртуальный рабочий стол [паролем](#)



## Авто-Sandbox

- Использовать Auto-Sandbox**

Опция включает автоматическую изоляцию в Sandbox исполняемых файлов и кода в соответствии с заданной ниже политикой.

- Проверять происхождение файлов

Если вы отключите эту опцию, решения о запуске файлов в Sandbox будут приниматься только на основе рейтинга файлов и их расположения.

После установки COMODO IS, Авто-Sandbox я включаю лишь только после того как устанавливаю все необходимые мне программы. Рекомендую поступать также.

В самой песочнице я не запускаю никаких программ.



Viruscope следит за деятельностью запущенных процессов и показывает предупреждения если обнаружит подозрительную активность, угрожающую конфиденциальности/безопасности. Помимо мониторинга данная система позволяет отменить уже внесённые подозрительными процессами изменения.

Естественно включил. Но пока не видел оповещений от данной системы, т. к. всё чисто. 😊



Viruscope

**Использовать Viruscope**

Viruscope - это система, позволяющая проводить динамический анализ поведения запущенных процессов и вести запись их активности.

**Не показывать оповещения**

Выбор этой опции позволяет автоматически переносить обнаруженные вредоносные объекты в карантин и отменять произведенные ими действия.

**Применять действие Viruscope только к приложениям в Sandbox**

Viruscope будет осуществлять мониторинг только приложений в Sandbox, запущенных виртуально или запущенных с ограничениями.

Управление статусом распознавателей, установленных на этом компьютере:

Название	Версия	Статус
recognizer_v8.2.0.5027.dll	8.2.0.5027	

Подробнее можно узнать [ЗДЕСЬ](#).



## Настройки Фаервола

 **Использовать фильтрацию трафика (рекомендуется)**

Пользовательский набор правил ▾

Опция активирует Фаервол, предназначенный для фильтрации входящего и исходящего трафика компьютера.

## Настройки оповещений

 Не показывать оповещения

Разрешать запросы ▾

 Показывать оповещения Trustconnect

Только в незащищенных Wi-Fi сетях ▾

 Показывать анимацию на значке в области уведомлений Создавать правила для безопасных приложений Уровень частоты оповещений

Высокий ▾

 Время показа оповещений на экране:  сек.

## Расширенные настройки

 Включить фильтрацию IPv6-трафика Включить фильтрацию loopback-трафика  
(например, 127.x.x.x, ::1) Блокировать фрагментированный IP-трафик Анализировать протокол Включить защиту от ARP-спуфинга

При данных настройках для каждой новой программы, если она попытается получить доступ к сети, появляется 1-2 оповещения.

Данная настройка фаервола не напрягает бесконечными оповещениями, и в то же время я контролирую всё. Мне нравится.

Чтобы включить такие же «глобальные правила» нужно «блокировать входящие соединения».

Главное окно программы – Задачи – Задачи Фаервола – Скрыть порты – Блокировать входящие соединения.



## Глобальные правила

На данном компьютере активны следующие глобальные правила:

<input type="checkbox"/>	Правила
<input type="checkbox"/>	✓ Разрешить IP Исходящие из MAC Любой в MAC Любой , где протокол: Любой
<input type="checkbox"/>	✓ Разрешить ICMPv4 Входящие из MAC Любой в MAC Любой , где ICMP сообщение: Требуется фрагментация
<input type="checkbox"/>	✓ Разрешить ICMPv4 Входящие из MAC Любой в MAC Любой , где ICMP сообщение: Превышение времени
<input type="checkbox"/>	⊘ Блокировать IP Входящие из MAC Любой в MAC Любой , где протокол: Любой



## Сетевые зоны

Автоматически обнаруживать частные сети

Не показывать оповещения, считая что место подключения к Интернету:

Общественное место ▼



## Контент-фильтр

**Использовать Контент-фильтр (рекомендуется)**

Данная опция настраивает Фаервол на фильтрацию доступа на сайты в соответствии с указанными ниже правилами и профилями.

Правила	Категории	
<input type="checkbox"/>	Правила	Применить правило
<input type="checkbox"/>	Разрешённые сайты	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Заблокированные сайты	<input checked="" type="checkbox"/>



## Настройки рейтинга файлов

**Использовать облачную проверку (рекомендуется)**

Выполнять облачный анализ неизвестных файлов, позволяющий получать быстрые результаты и экономить ресурсы компьютера

Не показывать оповещения

При обнаружении вредоносных объектов в ходе облачного сканирования будет применяться действие "Заблокировать и завершить выполнение"

Доверять приложениям, подписанным [доверенными поставщиками](#)

Доверять приложениям, установленным с помощью доверенных установщиков

Выявлять потенциально нежелательные приложения

Включил облачную проверку, т.к. нет оснований не доверять облаку COMODO.

Списки доверенных поставщиков я не трогал.

Я показал свои настройки антивирусного комплекса COMODO Internet Security. Они заточены под умеренный показ оповещений, т.к. я люблю контролировать все поползновения в системе, но при этом не хочу видеть сотни всплывающих предупреждений.

Фаервол для каждой программы, пытающейся получить доступ к сети, выдаёт 1-2 оповещения. HIPS – около 1-3. Естественно бывают и исключения, но в большинстве случаев именно столько и получается. Заражений системы пока что не было. CIS ни разу не подводил за 7 лет его использования.

Естественно эти настройки не всем подойдут, поэтому не бросайтесь бездумно копировать их, а ищите свой вариант. Пробуйте, благо CIS весьма гибок в настройках.



**Creating Trust Online!**