«Чем заняты подростки в интернете»

Уважаемые родители! Существует несколько способов, которые помогут родителям осуществлять интернет-фильтрацию

Первый способ:

Многие пользуются продуктами «Лаборатории Касперского». Родители даже не подозревают, что в антивирус Касперского встроена функция **«Родительский контроль».** С помощью этой функции вы сможете защитить своих детей от пагубного влияния интернета во время таких занятий, как онлайн-игры, общение в социальных сетях и просмотр сайтов и др.

Как это работает? В модуль встроены несколько функции:

- **Запрещенные слова.** Ограничивайте доступ к сайтам по ключевым словам. Можно отследить использование заданных слов в переписке в ICQ и социальных сетях, запретить общаться с определенными контактами. Можно отменить передачу в интернет личной информации (адреса, телефоны, персональные данные).
- **Время работы.** Определяйте расписание пользования компьютером и Интернетом: выбирайте допустимое время суток и продолжительность работы. Так вам не придется прогонять ребенка от компьютера и вступать в конфликт: сеанс закончится сам собой.
- **Допустимые программы**. Выбирайте, какие программы вашему ребенку разрешается запускать, а какие нет. Это удобно, если вы не хотите, чтобы он играл в определенные игры, или хотите его наказать, запретив ему пользоваться Skype.

Профиль **Ребенок** используется по умолчанию в компоненте **Родительский контроль**. Для этого профиля невозможно задать учетные записи пользователей и пароль.

Для профилей **Подросток** и **Родитель** возможно задать следующие настройки:

- ✓ включить\выключить профиль
- ✓ установить пароль для смены профиля
- ✓ задать учетные записи пользователей, для которых применим данный профиль
- ✓ установить уровень ограничения или выбрать один из предустановленных:
- ✓ низкий
- ✓ средний
- ✓ высокий
- ✓ выбрать действие при срабатывании правил компонента:
- ✓ записывать в отчет
- ✓ заблокировать доступ

- ✓ ограничить время работы в Интернете:
- ✓ ограничить суточное время работы в интернете (ограничение пользователя по количеству проведенного времени в Интернете за прошедшие сутки)
- ✓ разрешить доступ к интернету в указанное время (ограничение работы в интернете по указанному промежутку времени)

Для того чтобы изменить настройки профиля Вам необходимо проделать следующие действия:

- ✓ откройте главное окно программы
- ✓ нажмите кнопку **Настройка**
- ✓ выберите раздел **Родительский контроль** в левой части окна
- ✓ в блоке **Профили** нажмите кнопку **Настройка**
- ✓ перейдите на закладку профиля, настройки которого необходимо задать
- ✓ включите\выключите опцию **Использовать профиль**
- ✓ введите пароль для смены профиля в поле **Пароль**
- ✓ нажмите кнопку **Добавить** в разделе **Пользователи** для того чтобы добавить учетную запись, к которой будем применим профиль
- ✓ введите имя учетной записи в окне **Выбор:пользователь**
- ✓ нажмите кнопку **Проверить имена**, если Вам необходимо сверить введеную учетную запись с существующими на Вашем компьютере
- ✓ нажмите кнопку **ОК** два раза
- ✓ выберите один из трех уровней ограничения, перемещая ползунок вверх или вниз
- ✓ выберите одно из двух действий при срабатывании правил компонента
- ✓ нажмите кнопку Настройка в блоке Ограничение времени
- ✓ задайте параметры ограничения работы в интернете для данного профиля
- ✓ нажмите кнопку **ОК** два раза
- ✓ закройте главное окно программы.

Перейдя по ссылке http://support.kaspersky.ru/kis7/parental?qid=208635690, вы сможете просмотреть подробный видеоролик от компании Касперский, где предлагается пошаговая инструкция по настройке.

Второй способ:

Контент фильтры. **Ко́нтент-фильтр,** или **программа ограничения веб-ко́нтента** программное обеспечение для фильтрации сайтов по их содержимому, не позволяющее получить доступ к определённым сайтам или услугам сети Интернет. Система позволяет блокировать веб-сайты с содержимым, не предназначенным для просмотра.

Часто фильтрация проходит на уровне запросов по протоколу HTTP. Для этого URL запрошенного сайта сверяется с чёрным списком с помощью регулярных выражений. Такие списки необходимо регулярно обновлять, защита с их помощью считается малоэффективной. Более продвинутыми являются методы распознавания образов и обработки естественного языка.

Для классификации сайтов по разным признакам текст запрашиваемой страницы анализируется на количество разных ключевых слов. Эти и другие свойства текста используются для вычисления вероятности попадания в опасную категорию. Если эта вероятность превышает заданный уровень (например, 95, доступ к странице блокируется.

Самые простые программы позволяют ввести слова, поиск которых будет вести система вручную. Самые сложные устройства имеют большой словарь и предполагают уже готовую базу ссылок, которые классифицированы. Как правило, в сложных устройствах производители обеспечивают периодическое обновление базы ссылок. Те веб-сайты, которые не были распознаны автоматически, просматривает человек и присваивает категорию сайта вручную.

Как правило контент-фильтры бывают платными и бесплатными.

На портале http://korzh.net/2011-11-besplatnyj-kontent-filtr-dlya-linux-i-windows.html прилагается пошаговая инструкция по настройке бесплатной контент фильтрации.

Рассмотрим пример по настройке фильтрации в браузере Mozilla Firefox. Для этого нужно воспользоваться некоторыми дополнениями:

- ✓ дополнение **Wot.** это бесплатная надстройка к браузеру, которая предупреждает Интернет-пользователя во время поиска информации или совершения покупок о потенциально небезопасных веб-страницах. WOT совместим с такими браузерами как Internet Explorer, Mozilla Firefox, Opera Google Chrome.
- ✓ дополнение **Adblock Plus** — расширение для браузеров и другого ПО, позволяющее блокировать загрузку и показ различных элементов страницы: чрезмерно назойливых или неприятных рекламных баннеров, всплывающих окон и других объектов, мешающих использованию сайта.
- ✓ **дополнение Public Fox. Он нужен для того, чтобы дети не смогли отключить дополнения, отвечающие за контент-фильтрацию. Позволяет установить пароль для настроек.**

Далее необходимо установить дополнения.

Необходимо браузер mozilla firefox

В меню «**Инструменты — Дополнения**» *(Tools Add-ons)*

Необходимо перейти во вкладку **«поиск дополнений»** *(Get Add-ons)* и набрать в поиске слово «wot», далее **enter**.

Сразу же, первой строкой, появился нужный плагин WOT. Выбираем кнопку **«Добавить в Firefox»** *(add to iceweasel)*

через несколько секунд ,нажимаем кнопку **«Установить сейчас»** *(install now)*

Ждём окончания установки. После того как установка закончится, файрфокс попросит нас перезапустить браузер. Перезапускаем, нажав кнопку **«Перезапустить Firefox»** *(Restart iceweasel)*

После перезапуска открывается окно установленных дополнений, его закрываем.

Далее окно настроек расширения. Закрываем и настраиваем всё вручную.

Оказываемся на открытой вкладке **«WOT: руководство и настройки»**. Заходим в меню **«Предупредить»**

Выбираем уровень защиты **«очень эффективный»**. И ставим везде галочки **«защищать меня, если рейтинг не доступен»**. Переключатели ставим в положение **«блокировать»**. Самое важный пункт для нас это **«безопасность для детей»**. Это максимальная фильтрация.

Но при таком уровне будут блокироваться сайты с неизвестной репутацией. Т.е. контент фильтрация будет проходить очень жёстко. Оптимальную для конфигурацию необходимо подобрать самостоятельно. Главное оставить пункт **«безопаность для детей».**

Выбираем **«применить настройки»**

Рассмотрим ещё одну вкладку меню, которая может послужить. Открываем вкладку **«Расширенные»**. Может быть полезно поле, где можно указать сайты через запятую, которые будут в белом списке

Устанавливаем дополнение Adblock

Заходим в меню **«Инструменты — Дополнения»** *(Tools Add-ons)*

Переходим на вкладку **«поиск дополнений»** *(Get Add-ons)* и набираем в поиске слово **«Public Fox»** и нажимаем **enter**

Нажимаем кнопку **«Добавить в Firefox»** *(add to iceweasel)*

Ожидаем и нажимаем кнопку **«Установить сейчас»** *(install now)*

Ждём окончания установки, перезапускаем файрфокс

После перезапуска видим окно с установленными дополнениями. Выбираем Public Fox и нажимаем **«Настройки»** *(Preferences)*

Рассмотрим окно настроек более подробно. Первым делом введём пароль для этого дополнения

Далее настроим защиту нужных нам компонентов. Выставляем галочки, что запрещено изменять в firefox без пароля:

Lock Add-ons windows *(so users won't unistall this)* — Запрещаем изменять/удалять дополнения

Lock Firefox options — запрещаем изменять настройки firefox

Lock 'about:config' settings page — запретить настройку через страницу 'about:config'

Lock addition of Bookmarks — запрещаем редактировать закладки

Lock History sidebar — запрещаем редактировать и просматривать историю

Lock 'Clear Private Data' window — запрещаем очищать приватные данные *(историю, кэш и т.д.)*

в результате:

Далее идёт поле **«File Extensions that you dont want downloaded»**, что в переводе означает **«Расширения файлов, которые запрещены для скачивания»**. Это нужно для того, чтобы запретить детям качать типы каких то файлов. Например **exe файлы**, или любые другие, фильмы или музыку. Для этого надо просто перечислить расширения файлов для запрета через запятую. Или можно запретить всё, символом **«*»**. Например:

Теперь позаботимся о том, чтобы дети не смогли перенастроить расширение WOT, отключить контент фильтрацию. Для этого:

Добавим в blacklist ссылки. Для этого нажимаем кнопку **«add»**. В открывшемся окне пишем com/*. Нажимаем **«ОК»**, и далее в появившихся диалогах жмём кнопку **«ОК».**

Добавим ещё. Нажимаем кнопку add. В открывшемся окне пишем mywot.com/*

В результате:

Таким же способом можно внести нежелательные для открытия ссылки. Т.е. составить свой «чёрный» список сайтов.

Расширение Public Fox настроено. Нажимаем Кнопку **«ОК».**

Убираем пункт «WOT» из инструментов

Эта часть более сложная, но в ней исключается любая возможность отключить расширение, отвечающие за фильтрацию. А это пункт меню в инструментах.

В Windows

заходим: «**C**:\Documents and Settings**chas**\Application Data\Mozilla\Firefox\Profiles**default**\chrome». Жирным выделены пути, которые могут не совпадать с предложенным. **C:** — буква диска может зависеть от того, на каком диске у вас располагается система. **chas** — имя Вашего пользователя в системе. **iw6qhtbk.default** — Ваш профиль в firefox.

В этой папке находится файл **userChrome-example.css**. Переименуем его в **css.**

Открываем его в блокноте *(желательно открывать текстовым редактором с поддержкой кодировки utf8)* для редактирования. Но если его нет под рукой, не страшно. Главное, надо следовать точно инструкции.

Добавляем в конец файла строчку: **#wot-context-tools { display: none !important; }**

Заходим в меню **файл — Сохранить как**. Выбираем **«кодировка» — «UTF-8»** . Нажимаем кнопку **«Сохранить»**. На вопрос **«Заменить»** отвечаем **«да».**

Перезапускаем firefox. Заходим в меню **«Инструменты»**. Видим, что меню **«WOT»** исчезло.

В linux

Если Вы сами хорошо знакомы с линуксом, то можете сделать проще. необходимо зайти **/home/user/.mozilla/firefox/3ji8e26a.default/chrome**

(3ji8e26a.default — профиль, у Вас он называется по другому) и там изменить файл, как и какой смотреть ниже.

Чтобы способ был более универсальным для разных версий линукса, воспользуемся консолью *(терминал)*.

Открываем терминал

Прописываем команду **cd /home/user/.mozilla/firefox/** *(вместо user подставляем имя своего пользователя)*

Набираем команду **ls -al**. Нам выводятся все каталоги и файлы в папке.

Находим подобную подобную папку 3ji8e26a.default. И пишем команду **cd 3ji8e26a.default/chrome** *(3ji8e26a.default — подставляем свой профиль)*

Скопируем файл с новым именем, пишем: **cp userChrome-example.csscss**

Откроем с помощью редактора файл. Используйте любой текстовый редактор, предлагается использовать **gedit**. Поэтому, пишем команду: **gedit userChrome.css**

Перемотаем в конец и добавим строчку: **#wot-context-tools { display: none !important; }**

Сохраняем, закрываем редактор и перезапускаем firefox. Открываем меню **«Инструменты»** *(Tools)*.

И проверяем наличие пункта меню **«WOT»,** если его нет, то все сделано правильно. В настройки WOT можно зайти через дополнения, которые защищены паролем.

Теперь настроен браузер firefox, он фильтрует, дети отключить фильтрацию не могут. Есть чёрные и белые списки, которые можно редактировать.

Третий способ: наиболее простой и не требует больших усилий, справиться с ним может любой человек, владеющий компьютером на уровне пользователя.

В системе Windows есть файл, отредактировав который, вы сможете создать свой «*черный*» список сайтов, доступ к которым с компьютера будет закрыт. Имя этому файлу — **Hosts**.

Файл hosts нужен системе для сопоставления ip-адресов с их доменными именами, аналогично DNS-серверам. Но уникальное в этом файле, что он напрямую управляет доступами к сайтам. Зная точное доменное имя сайта, внеся его в файл hosts, закрывается доступ к этому сайту.

Первое, что нужно помнить — если вы не являетесь администратором компьютера и не имеет соответствующих прав, то отредактировать файл hosts вам не удастся. Приступим к собственно редактированию:

1.Идем в папку «*C:\Windows\System32\drivers\etc*» (*путь может измениться если у вас система на другом диске или в другой директории*);

- ✓ Открываем «Мой компьютер»
- ✓ Находим папку «WINDOWS»
- ✓ Переходим в папку «Sistem32»
- ✓ Открываем папку «Drivers»
- ✓ Находим папку «Etc»
- ✓ Находим файл «hosts»

2.Открываем файл **hosts**, используя стандартный блокнот;

Откроется файл **hosts** и стандартно он должен выглядеть так:

Можно приступать непосредственно к редактированию файла и блокированию доступа в сайтам. Для этого в файл добавляем строки вида «*127.0.0.1 закрытый сайт*«, где *закрытый сайт* — это и есть то имя сайта, доступ к которому мы закрываем (*vkontakte.ru, odnoklassniki,ru и т.д.*). например:

Сохраняем файл. В примере заблокированы сайты социальных сетей «Вконтакте» и «Одноклассники». При попытке войти на указанные сайты в браузере появится следующая надпись:

РОДИТЕЛЬСКИЙ КОНТРОЛЬ (НАИМЕНОВАНИЯ ПРОГРАММ)

1. **Kaspersky Safe Kids http://www.kaspersky.ru/safe-kids-np**
2. **ESET Parental Control**

http://eset.ua/ru/products/for_home/parental_control

3. **SkyDNS (https://www.skydns.ru/)**

Приложение к письму
ГУ МВД России
по Саратовской области
от «_18_» марта 2016 года № 13/_611_

Список
интернет адресов «сомнительных» сообществ и пользователей сети «Вконтакте», которые «пропагандируют» подростковые суициды

Сообщества:
- https://vk.com/public108451927
- https://vk.com/okolo_nashey_love
- https://vk.com/blvcktrip
- https://vk.com/vpustotel
- https://vk.com/club67359375
- https://vk.com/project1642
- https://vk.com/dat221k25
- https://vk.com/osnovamira

Пользователи сети «Вконтакте»:
- https://vk.com/id261372650
- https://vk .com/derpy133t
- https://vk.com/id263458169
- https://vk.com/id272929306
- https://vk.com/id301321674
- https://vk.com/deadboy
- https://vk.com/sereons2
- https://vk.com/cher3pashka
- https://vk.com/lsoenl
- https://vk.com/espada_daniel
- https://vk.com/4utistk4
- https://vk.com/runews1

ООДУУПиПДН ГУ МВД России по Саратовской области

Приложение к письму
ГУ МВД России
по Саратовской области
от «18» марта 2016 года № 13/612

Список
интернет адресов «сомнительных» сообществ и пользователей сети «Вконтанке», которые «пропагандируют» подростковые суициды

Сообщества:
- https://vk.com/public108451927
- https://vk.com/okolo_nashey_love
- https://vk.com/blvcktrip
- https://vk.com/vpustotel
- https://vk.com/club67359375
- https://vk.com/project1642
- https://vk.com/dat221k25
- https://vk.com/osnovamira

Пользователи сети «Вконтакте»:
- https://vk.com/id261372650
- https://vk .com/derpy133t
- https://vk.com/id263458169
- https://vk.com/id272929306
- https://vk.com/id301321674
- https://vk.com/deadboy
- https://vk.com/sereons2
- https://vk.com/cher3pashka
- https://vk.com/lsoenl
- https://vk.com/espada_daniel
- https://vk.com/4utistk4
- https://vk.com/runews1

ООДУУПиПДН ГУ МВД России по Саратовской области