

## **Рекомендации для родителей по предупреждению интернет - рисков «Как избежать материалов с нежелательной информацией»:**

1. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой.

Перечень специальных программных фильтров (интернет-фильтров) приведен в приложении 1.

Почти каждый Интернет-браузер обладает настройками безопасности: какой контент должен быть заблокирован, а какой можно загружать на компьютер. Настройки браузера устанавливаются бесплатно. На сайте каждого разработчика Интернет-браузеров можно найти подобную информацию в разделе «Безопасность».

Специальные программы, называемые системами родительского контроля, позволяют родителям самим решать, какое содержимое в Интернете могут просматривать их дети, отсекают «плохие» сайты, содержащие нежелательную информацию, в соответствии с введенными настройками.

Такие программы позволяют смотреть отчеты о том, какие сайты посещал ребенок, сколько времени пользовался Интернетом, устанавливать ограничения пользования компьютером и Интернетом по времени.

Родительский контроль можно устанавливать непосредственно с помощью операционной системы (например, Windows), антивирусных программ (например, антивирус Касперского), специальных программ.

Полезные ссылки по настройке родительского контроля приведены в приложении 2.

### **Приложение 1**

#### **Рекомендуемые Интернет-фильтры**

Интернет-фильтры позволяют ограничить доступ в Интернет. Такие программы умеют блокировать доступ к определенным сайтам, например порноресурсам, сайтам с информацией об оружии и наркотиках, а также для контроля времени нахождения в сети.

1. Интернет Цензор-интернет-фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов. В основе работы программы лежит технология "белых писксов", гарантирующая 100% защиту от опасных и нежелательных материалов.

Программа содержит уникальные вручную проверенные "белые списки", включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации.

Интернет Цензор может использоваться как в домашних условиях, так и в организациях –образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет.

Фильтр «Интернет Цензор» можете скачать бесплатно на официальном сайте <http://www.icensor.ru/>

2. KinderGate Родительский Контроль 1.0 Эта программа – фильтр ([www.usergate.ru](http://www.usergate.ru)) предлагает 82 категории фильтрации веб-сайтов в 5 основных уровнях доступа (по умолчанию запрещен доступ к фишинговым ресурсам, сайтам с порнографическим контентом, и тем, что содержат вредоносный код). Самый высокий уровень фильтрации подразумевает, в числе прочего, запрет прокси-серверов, пиринговых сетей и сайтов знакомств.

Можно изменить уровень фильтрации в разделе «Правила > Запрет категорий». Доступно создание расширенных правил, «черных» и «белых» списков для сайтов. Можно установить ограничение скачивания (загрузки) видео, звуковых файлов, изображений, архивов и EXE-файлов, документов. Причем, данное приложение понимает любые сетевые протоколы, используемые для загрузки файлов.

В программе реализован модуль морфологического анализа, позволяющий блокировать веб-страницы с нецензурной лексикой. Для ограничения времени, проводимого ребенком за компьютером, предусмотрен специальный инструмент «Расписание работы». Кроме этого доступна статистика посещенных веб-ресурсов с указанием значений входящего и исходящего трафика, а также просмотр сообщений в сетях [odnoklassniki.ru](http://odnoklassniki.ru) и [vkontakte.ru](http://vkontakte.ru).

3. Kaspersky Internet Security 2011 ([www.kaspersky.ru](http://www.kaspersky.ru), 105 Мбайт) – антивирусная программа, которая защищает ваш компьютер от вирусов и в состав которого входит модуль родительского контроля. Приложение способно не только ограничивать время, проводимое за компьютером, но и контролировать общение детей при использовании различных Интернет-пейджеров, например, ICQ (поддерживаются клиентские приложения для 27 сетей MSN, Jabber, IRC, Mail.ru и Yahoo).

Действия подрастающего поколения в социальных сетях (FaceBook, MySpace, Twitter) тоже не останутся без внимания модуля родительского контроля, причем, в определенных случаях, можно не только создать «черный список» для контактов, но и произвести запись сообщений. Для ограничения доступа к веб-ресурсам предусмотрено 14 категорий – родителям достаточно включить нужные. Если ресурс, к которому ребенок стремится получить доступ, не найден в базе данных, будет произведен эвристический анализ веб-страницы. Другой интересный момент касается запрета передачи конфиденциальных данных, например, реквизитов банковской карты или домашнего адреса (на тот случай, если чадо вознамерится оплатить какие-либо услуги). Модуль родительского контроля позволит запретить загрузку следующих типов файлов: «Музыка», «Видео», «Программы» и «Архивы». Однако данный запрет действует лишь при использовании протокола HTTP, и если ваш ребенок знаком с премудростями FTP или использует локальный прокси с нестандартным портом, то без труда обойдет такое ограничение. К сожалению, модуль

родительского контроля KIS 2011 не поддерживает фильтрацию по протоколам.

4. Интернет-фильтр «Кибер Папа» бесплатная программа, которая ограничивает возможности ребенка выйти за пределы детского Интернета при использовании любого браузера. Программа работает по принципу «белого списка» и чрезвычайно проста в использовании. После инсталляции программы и включения фильтра, ребенок может переходить только по страницам проверенных детских сайтов (блокируются также все статические и динамические объекты веб-страниц, не принадлежащие к списку проверенных детских ресурсов). Отключить фильтр могут только родители, используя известный им пароль от программы. Скачать можно программу на официальном сайте <http://cyberpapa.ru/>

5. KidsControl-программа предназначена для ограничения доступа детей к нежелательным Интернет ресурсам, а также для контроля времени нахождения в сети. С помощью программы вы можете становить ограничение доступа к нежелательным ресурсам по различным категориям – сайтам, с содержанием информации для взрослых, online-играм и казино, форумам, указав галочкой на определенную категорию, и установить ограничение самостоятельно с помощью черного списка. Скачать можно программу на официальном сайте <http://www.kidscontrol.ru/>

## Приложение 2

### Настройка родительского контроля в операционной системе

Функции "родительского контроля" есть даже в популярной сегодня операционной системе Windows 7, которая устанавливается на большинство новых компьютеров и ноутбуков. В частности, Windows 7 дает возможность ограничивать время, которое ребенок проводит за компьютером: вы можете, скажем, разрешить ему играть в игры или пользоваться социальными сетями 2-3 часа в день. Остальное время молодой человек пусть проведет на улице или в каком-нибудь развивающем кружке, которых, к счастью, сейчас предостаточно не только в Москве и других крупных городах. Еще операционная система от Windows позволяет устанавливать запрет на доступ детей к тем или иным играм или программам. Например, если вы не хотите, чтобы ребенок смотрел мультфильмы или фильмы, хранящиеся на жестком диске, можно запретить запуск мультимедийного плеера. О том, как включить "родительский контроль" в Windows 7 и других операционных системах этого семейства, можно узнать на сайте [windows.microsoft.com/ru-](http://windows.microsoft.com/ru-ru)

RU. Если подвести курсор мыши к меню "Помощь", вы увидите выпадающее меню. Выберите в нем вашу систему -Windows 7, Vista и так далее. После этого в открывшемся разделе найдите пункт "Безопасность" и перейдите в него. В нижней части правого меню вы увидите раздел "Родительский контроль", где находятся подробные сведения о

возможностях этой функции и даются советы по настройке. Настройка безопасности в поисковых системах Родителям следует знать, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые с легкостью можно настроить самостоятельно. В большинстве популярных поисковых систем есть опция так называемого «Безопасного поиска», которая предполагает фильтрацию сайтов сомнительного содержания в поисковой выдаче. При активации этой функции поисковые машины производят фильтрацию не только по выдаче сайтов, но и по выдаче картинок на любой запрос. У почтовых сервисов можно настроить специальные фильтры, чтобы блокировались все сообщения с определенными параметрами или словами.

В Google фильтрация результатов поиска включается в разделе "Настройки поиска", который появляется при клике мыши на значок шестеренки в правом верхнем углу заглавной страницы [www.google.ru](http://www.google.ru). В меню "Безопасный поиск" установите режим "Строгая фильтрация", который предусматривает отсеивание непристойных картинок и текста. Не забудьте нажать кнопку "Сохранить настройки".

Применять фильтр к результатам поиска позволяет и Яндекс. В разделе "Настройки -Остальное" есть пункт "Настройка результатов поиска", а в нем -меню "Фильтрация страниц".

### **Настройка безопасности в поисковых системах**

Родителям следует знать, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые с легкостью можно настроить самостоятельно. В большинстве популярных поисковых систем есть опция так называемого «Безопасного поиска», которая предполагает фильтрацию сайтов сомнительного содержания в поисковой выдаче. При активации этой функции поисковые машины производят фильтрацию не только по выдаче сайтов, но и по выдаче картинок на любой запрос. У почтовых сервисов можно настроить специальные фильтры, чтобы блокировались все сообщения с определенными параметрами или словами.

Создайте на компьютере несколько учетных записей, когда каждый пользователь сможет входить в компьютер (систему) независимо и иметь собственный уникальный профиль. Ребенок сможет входить в систему только под своим логином и паролем, не имея административных прав на контроль системных настроек, установку программ. Учетная запись администратора должна быть у родителя, тогда только родитель сможет контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера.

Для работы в Интернете необходимо создавать надежные и защищенные пароли. Пароль защищает компьютер и блокирует возможность его использования без разрешения его владельца. Напомните вашему ребенку, что ему нельзя сообщать этот пароль своим друзьям, а если он стал им известен, то пароль должен быть изменен.

Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе с какой информацией он сталкивается в сети. Попав случайно на какой-либо опасный, но интересный сайт, ребенок с большой вероятностью из любопытства захочет познакомиться и с другими подобными ресурсами. Важно заметить это как можно раньше и объяснить, ребенку, чем именно ему грозит просмотр подобных сайтов, а также обновить настройки безопасности браузера или программного фильтра. Младшим детям нужно подробно объяснить, что это за материалы, для чего

Их публикуют, какие опасности они несут, в чем состоит вред такой информации. Старших детей необходимо научить критически относиться к

Содержанию онлайн-материалов и не доверять им без совета с Вами.

Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Необходимо проверять информацию, увиденную в Интернете. Для этого существуют определенные правила проверки достоверности информации. Признаки надежного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность представления информации, цель создания сайта, актуальность данных.

Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог гораздо конструктивнее, чем

Постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента. Настройка родительского контроля в операционной системе.