

Методические рекомендации для родителей по обеспечению контентной фильтрации домашнего Интернета.

Для ограничения доступа детей к нежелательному, опасному контенту в настоящее время имеется возможность выбрать как коммерческое, так и свободно распространяемое программное обеспечение, и сервисы, либо тарифные опции Интернет-провайдеров, либо специальные возможности антивирусных программ.

Принцип работы этих систем обычно строится на черных (запрещенных) и белых (разрешенных) списках, либо на основе фильтрации. Наиболее широкое распространение получили три алгоритма фильтрации:

фильтрация, по ключевым словам, (конкретные слова и словосочетания используются для включения блокировки веб-сайта);

динамическая фильтрация (содержимое запрашиваемого веб-ресурса анализируется в момент обращения, загрузка страниц ресурса в браузер блокируется, если содержимое определяется как нежелательное);

URL-фильтрация (запрашиваемая страница или целый домен, например, dosug.nu, могут быть определены или категоризованы как нежелательный ресурс, вследствие чего доступ к таким страницам блокируется).

Лучшие в мире системы контентной фильтрации используют URL-фильтрацию, основанную на анализе и категоризации Интернет-ресурсов. Такой механизм признан наиболее эффективным методом фильтрации контента.

Для ограничения доступа несовершеннолетних лиц к нежелательному или опасному контенту с настольных компьютеров и мобильных устройств можно использовать дополнительные опции, предлагаемые большинством Интернет-провайдеров. Для этого необходимо обратиться в службу технической поддержки провайдера (телефон данной службы обычно указан в договоре) и высказать пожелание подключения данной услуги. Далее необходимо следовать инструкциям оператора.

Можно также использовать специализированное программное обеспечение и сервисы. Наиболее популярные, некоммерческие версии: SkyDNS, NetPolice Child, Eyes Relax, Parental Control Bar, Norton Online Family, NetPolice Lite. Помимо этого, существует возможность введения ограничения доступа к нежелательным сайтам путем установки дополнений (расширений) в Интернет-браузерах, таких как: Internet Explorer, Mozilla FireFox, Chrome, Opera и других.

Обращаем внимание, что на домашних компьютерах также можно задействовать антивирусные программы с функцией «Родительский контроль», которые могут защитить ребенка от нежелательного контента. В основном это коммерческие продукты: Kaspersky Internet Security 2012, Kaspersky Crystal, Kaspersky Internet Security 7.0, KinderGate Родительский контроль, ChildWebGuardian, Spector Pro 6.0, КиберМама, Eset Nod32 и других.

Однако существуют и бесплатные продукты, например, Avira Free Antivirus 2013 с веб-приложением Avira Free SocialShield.

Использование функции родительского контроля подробно описано в инструкциях пользователя для антивируса.

Стоит обратить особое внимание на наличие функции родительского контроля при приобретении антивирусной программы или продлении лицензии на следующий год, сообщить о вашем желании распространителю программного обеспечения. Практически все современные разработчики антивирусных пакетов имеют в своём арсенале продукты для обеспечения безопасности ребенка в сети, блокировки нежелательного и опасного контента.

Возможности родительского контроля.

1. Фильтры web-сайтов.

Слова-запреты (фильтры). Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на web-странице, то она не открывается.

Создание белого списка. Более жесткий способ контроля, когда вы самостоятельно составляете белый список сайтов, которые может посещать ребенок.

Создание черного списка. В черном списке указываются сайты, на которые ребенку заходить запрещено. Приложение работает с базой данных, где содержатся сайты для взрослых. Крайне желательно, чтобы список регулярно обновлялся через Интернет, иначе появление новых ресурсов быстро сделает защиту неактуальной. Родители могут расширять черный список сайтов на свое усмотрение, при желании, используя автоматизированную информационную систему ведения и использования базы данных о сайтах, содержащих запрещённую к распространению в России информацию, утвержденную Постановлением Правительства Российской Федерации от 26 октября 2012 года № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»» (<https://reestr.rublacklist.net>).

2. Ограничение времени, проводимого ребенком за компьютером. 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.

3. Установка запретов на использование детьми отдельных программ. Во избежание различных недоразумений родители могут ограничить список используемых ребенком программных продуктов. Большинство современных операционных систем имеют в своем составе инструмент доступа пользователей к программным продуктам, что дает возможность ограничения доступа ребенка к нежелательным программным продуктам.

4. Управление доступом к игровым приложениям. Возможности родительского контроля позволяют помочь детям играть в безопасные, дружелюбные, занимательные и обучающие игры, соответствующие их возрасту. В частности, родители могут блокировать как все игры, так и только некоторые из них. Дополнительно родители могут устанавливать разрешение или запрет на доступ к отдельным играм, исходя из допустимой возрастной оценки и выбора типа содержимого.

5. Журнал отчетов о работе ребенка за компьютером. С целью анализа того, чем занимался ребенок за компьютером в отсутствие взрослых, какие программы запускал, какие сайты просматривал в Интернете, с кем общался и т.д., родительский контроль ведет аудит всех действий подрастающего пользователя. В журнал записываются адреса посещенных детьми страниц Интернет. В некоторых программах журнал с отчетом можно получать по электронной почте, что очень удобно, если родитель находится вне дома, и хочет просмотреть, какие сайты посещал ребенок.

Еще раз необходимо напомнить, что для ограничения доступа к нежелательному, опасному контенту в настоящее время имеется возможность выбрать как коммерческое, так и свободно распространяемое программное обеспечение, и сервисы, либо тарифные опции Интернет-провайдеров, либо специальные возможности антивирусных программ.