Методические рекомендации для родителей «Безопасный интернет»

Любой родитель хочет оградить своё чадо от плохих вещей в этом мире. Интернет не исключение. Сам по себе Internet не плох, он зеркало, в котором отразилась человеческая реальность. Есть в Интернете хорошие вещи? Есть! Но есть и плохое ... для детей.

Данная статья призвана помочь родителям обезопасить своих детей от нежелательного контента в сети с помощью фильтров. Причём бесплатно! От вас требуется только желание. Так как хорошая защита - эшелонированная защита из нескольких этапов, то наша защита детей так же будет многоступенчатой ... враг не пройдёт.

Вне зависимости от уровня ваших компьютерных знаний придётся узнать и уяснить пару моментов.

1) Защита через DNS. Компьютеры между собой оперируют цифрами и адреса сайтов для компьютеров тоже числа, а человеку проще и лучше оперировать осмысленным текстом. DNS - это преобразователь "текста" для людей (типа rambler.ru) в "адреса-числа" (типа 81.19.70.1) и наоборот. Первый этап защиты детей от нежелательного контента будет основан на том, что есть DNS сервера, которые во время "преобразования" могут ещё и фильтровать. Другими словами, если ребёнок лезет в браузере на сайт yandex.ru, то этот хороший сайт в DNS будет преобразован в его компьютерный-числовой-адрес (IP адрес). Но если ребёнок вольно или не вольно попадает на sex.com, то такой адрес будет преобразован НЕ в его компьютерный-числовой-адрес (IP адрес), а в адрес, где будет предупреждение о недопустимости или что такой сайт отсутствует в сети.

2) Защита поисковой выдачи. Данный этап оградит ребёнка от нежелательных результатов поисковой выдачи. Необходимо во всех браузерах на всех доступных вам компьютерах в качестве домашней страницы использовать Яндекс с Семейным фильтром.

3) Защита с помощью бесплатных программ и плагинов к браузеру. Сторонние бесплатные программные решения и услуги от Internet провайдеров.

Защита через DNS.

В Интернете из бесплатных и серьёзных защит для детей через фильтрацию DNS мы возьмём 2 представителя: ***Яндекс.DNS и OpenDNS FamilyShield (OpenDNS Семейный Щит)***. Почему 2?

1) Мало ли кто из них начнёт "тупить", а таймауты при преобразовании сказываются на скорости вашей работы в сети Internet, в независимости от вашего тарифа у провайдера.

2) Одна голова хорошо, а две лучше.

3) Во многих операционных системах есть 2 поля под указание DNS серверов.

Прежде чем перейти к прописыванию DNS серверов-защитников, нужно определиться, где лучше прописать наших защитников. DNS сервера можно прописать на оконечном устройстве - компьютер, ноутбук, планшет, смартфон или в вашем роутере-узле (если он имеется), который выводит вашу домашнюю сеть в Internet.

Каждый способ обладает плюсами и минусами.

1) Прописать на роутере - точке доступа. Ваши компьютеры получают сетевые настройки от домашнего роутера по протоколу DHCP. Роутер выдаст всем вашим устройствам и устройствам, пришедших в гости друзей, указание использовать его в качестве DNS. А сам будет использовать вышестоящие DNS сервера-защитники. В этой схеме, друзья будут защищены тоже.

2) *Но вышестоящая схема плоха, когда ваше чадо уйдёт со своим смартфоном или планшетом в кафе с друзьями и там его не будет защищать чужой роутер. Поэтому прописывание защитников-DNS на оконечном устройстве обладает своим плюсом.*

Решать вам - защищаться через вашу точку доступа и/или через конечное устройство.

***Точка доступа*.**

1. Введите IP-адрес роутера в браузере, чтобы зайти в панель администратора.
2. Введите имя пользователя и пароль.

3. В меню управления роутером найдите настройки DNS-сервера.

4. Пропишите адрес Яндекс.DNS 77.88.8.7 в качестве Primary DNS-сервера и сохраните изменения. В поле Secondary DNS-сервера пропишите адрес OpenDNS FamilyShield 208.67.222.123.

На компьютере.

Windows XP.

1. Откройте меню Пуск -> Настройка -> Панель управления -> Сетевые подключения.

2. Щелкните правой кнопкой мыши на нужном сетевом подключении и выберите пункт Свойства.

3. В окне свойств подключения выберите пункт Протокол Интернета (TCP/IP) и нажмите кнопку Свойства.

4. В открывшемся окне выберите пункт Использовать следующие адреса DNS-серверов.

5. Введите адрес Яндекс.DNS 77.88.8.7 в качестве Предпочитаемый DNS-сервер. В поле Альтернативный DNS-сервер пропишите адрес OpenDNS FamilyShield 208.67.222.123. И сохраните изменения кнопкой Ок.

Windows 7.

1. Откройте меню Пуск -> Панель управления -> Сеть и Интернет -> Центр управления сетями и общим доступом -> Изменение параметров адаптера.

2. Щелкните правой кнопкой мыши на нужном сетевом подключении и в появившемся меню выберите пункт Свойства.

3. В окне свойств подключения выберите пункт Протокол Интернета версии 4 (TCP/IP) и нажмите кнопку Свойства.

4. В открывшемся окне выберите пункт Использовать следующие адреса DNS-серверов.

5. Введите адрес Яндекс.DNS 77.88.8.7 в качестве Предпочитаемый DNS-сервер. В поле Альтернативный DNS-сервер пропишите адрес OpenDNS FamilyShield 208.67.222.123.

Windows 8.

1. Наведите мышку на меню Пуск (левый нижний угол экрана), когда появится меню,нажмите на нем правой кнопкой мыши и выберите Панель управления.

2. Откройте Сеть и Интернет -> Центр управления сетями и общим доступом -> Изменение параметров адаптера.

3. Щелкните правой кнопкой мыши на нужном сетевом подключении и в появившемся меню выберите пункт Свойства.

4. В окне свойств подключения выберите пункт Протокол Интернета версии 4 (TCP/IP) и нажмите кнопку Свойства.

5. В открывшемся окне выберите пункт Использовать следующие адреса DNS-серверов.

6. Введите адрес Яндекс.DNS 77.88.8.7 в качестве Предпочитаемый DNS-сервер. В поле Альтернативный DNS-сервер пропишите адрес OpenDNS FamilyShield 208.67.222.123.

Mac OS X.

1. Зайдите в Системные настройки -> Сеть.

2. Выберите сеть, для которой вы хотите настроить DNS (AirPort, Ethernet).

3. Нажмите на кнопку Дополнительно, перейдите на вкладку DNS.

4. Пропишите адрес Яндекс.DNS 77.88.8.7 и сохраните изменения.

Ubuntu.

1. Щелкните на значке сетевого подключения, в списке выберите Edit connections (Изменить соединения).

2. Выберите сеть, для которой вы хотите настроить DNS, и нажмите Edit (Изменить).

3. Перейдите на вкладку IPv4 Settings (Параметры IPv4), в группе Method (Метод, Способ Настройки) выберите Automatic (DHCP) addresses only (Автоматически (DHCP, только адрес)).

4. Введите адрес Яндекс.DNS 77.88.8.7 в поле Addresses (Адреса, Серверы DNS) и сохраните изменения.

В смартфоне или планшете.

Android 4.x

1. Зайдите в Настройки, выберите пункт Wi-Fi.

2. Долгим нажатием (нажать и удерживать до появления диалогового окна) выберите желаемую Wi-Fi сеть.

3. В появившемся диалоговом окне выберите Настроить сеть.

4. Поставьте внизу галочку Показать расширенные настройки.

5. В пункте Настройка IP в выпадающем списке выберите Статический.

6. Введите в поле DNS 1 адрес Яндекс.DNS 77.88.8.7. В поле DNS 2 пропишите адрес OpenDNS FamilyShield 208.67.222.123.

7. Нажмите Сохранить.

Apple iOS.

1. Зайдите в Настройки -> Wi-Fi, нажмите на стрелку напротив используемой вами сети.

2. Найдите пункт DNS и впишите в него адрес Яндекс.DNS 77.88.8.7.

Защита поисковой выдачи.

Данный этап защитит ребёнка во время поиска информации. Можно воспользоваться Семейным поиском Яндекс, который фильтрирует поисковые запросы и не выдаёт результаты, не предназначенные ребёнку. Защита основана на том, что по умолчанию все новые открытые вкладки в браузере используют в качестве домашней страницы поисковую систему Яндекс с Семейным фильтром. Вероятнее всего, что ребёнок не будет переходить на другие поисковые системы, а воспользуется уже предложенным с фильтрацией.

Google Chrome.

1. Войдите в настройки браузера: Верхний правый значок из трёх горизонтальных линий -> Настройки.

2. Выберите: Начальная группа -> Следующие страницы.

3. Нажмите Добавить, в поле Добавить страницу впишите http://family.yandex.ru

4. Нажмите ОК

Mozilla Firefox.

1. Войдите в настройки браузера: Правка -> Настройки.

2. Во вкладке Основные выберите: При запуске Firefox Показать домашнюю страницу.

3. В поле Домашняя страница укажите: http://family.yandex.ru

Opera.

1. Войдите в настройки браузера: Opera -> Настройки -> Общие настройки.

2. Во вкладке Основные выберите: При запуске Начать с домашней страницы.

3. В поле Домашняя укажите: http://family.yandex.ru

4. Нажмите ОК.

Защита с помощью бесплатных программ и плагинов к браузеру.

В данном разделе рассматриваются программные продукты, которые могут бесплатно помочь родителю защитить детскую психику от ужасов в Интернете и сделать его белым и пушистым.

Плагин блокировки баннеров AdBlock. Данный плагин в основном занимается "вырезкой" рекламных баннеров, за счёт которых живут вебмастера. Мимоходом, кроме как лишать вебмастеров заработка, плагин к браузерам AdBlock может помочь в ограждении ребёнка от показа непристойных баннеров на плохих сайтах. Получается, что те вебмастера, создающие свои говно сайты, вынуждают использовать AdBlock, который лишает заработка нормальных вебмастеров.

Google Chrome.

1. Войдите в настройки браузера: Верхний правый значок из трёх горизонтальных линий -> Настройки.

2. Выберите слева Расширения - Ещё расширения.

3. Поищите AdBlock, который появится в категории Расширения.

4. Установите кнопкой Бесплатно.

Mozilla Firefox.

1. Войдите в меню браузера: Инструменты -> Дополнения.

2. Слева Получить Дополнения и указать поиск как AdBlock.

3. Установить AdBlock.

Также постоянно выпускаются все новые дополнения и плагины для разных браузеров и различных операционных систем. Если поискать, всегда можно найти подходящий вам вариант.

Мобильные операторы сотовой связи могут помочь родителям в блокировке нежелательного контента. Например, Родительский контроль и Детский интернет у Мегафона. Родительский контроль у МТС. Безопасный Интернет у Билайна. Эти операторы во многих регионах нашей страны предоставляют так же и проводной доступ в Интернет. Посетите, наконец-то, свой Личный кабинет и подключите эти защищающие услуги.

Надеюсь эти бесплатные решения надёжно защитят вас и ваших детей!

Памятка

Методические рекомендации для родителей по обеспечению контентной фильтрации домашнего Интернета для обучающихся 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 категорированы 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, 2 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 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.