Памятка для родителей

Безопасность детей в социальных сетях. Родительский контроль

Нынешние дети начинают учиться считать, писать и читать практически одновременно с работой за компьютером. Хорошо это или плохо — вопрос спорный. Но несомненно, что освоение компьютера с юных лет открывает широкие возможности в плане развития и образования, которые чаще всего реализуются при активном подключении родителей в качестве направляющей и контролирующей стороны.

В России около 8 миллионов пользователей глобальной сети — дети. Они могут играть, знакомиться, познавать мир... Но в отличие от взрослых, в виртуальном мире они не чувствуют опасности. Наша обязанность — защитить их от негативного контента.

Как правило, родителям требуется организовать контроль за временем работы на компьютере (время приходится ограничивать), регулировать доступ к «вредным» программам (в частности, к играм), а также наблюдать за использованием Интернета и блокировать доступ к неподходящим для ребёнка ресурсам.

С 2004 года в первый вторник февраля празднуется Всемирный день безопасного Интернета. В условиях быстрых темпов развития информационных технологий необходимость контроля Интернета становится вопросом первостепенной важности. Рискам, таящимся в киберпространстве, особенно подвержены дети. Глобальная сеть ничуть не безопаснее игровой площадки. Это понимают во всем мире.

Сегодня не нужно работать в ФСБ, чтобы узнать о человеке все, достаточно залезть в Интернет, и Вы найдёте фамилию, возраст, адрес, место учёбы, материальное положение. Практика показывает, что дети в поисках друзей размещают о себе в Сетях только голую правду. А опытным мошенникам не остаётся ничего кроме как воспользоваться их наивностью и недостатком родительского контроля. Преступники в Интернете действуют по принципу волка в овечьей шкуре. Они пользуются тем, что дети не могут распознать взрослого, умело маскирующегося под их сверстника. Только контролируя Интернет, отслеживая переписку ребёнка, родители могут обнаружить тех, кто отправляет подозрительные сообщения их детям, пытается втереться к ним в доверие, договориться о встрече, задаёт наводящие вопросы и забрасывает просьбами выслать откровенные фотографии.

Глобальная Сеть содержит большое количество информации взрослого содержания. Интернет насчитывает сотни миллионов порнографических страниц. Порнография считается одной из самых прибыльных отраслей. Эта индустрия в Интернете приносит около 2,5 миллиардов долларов в год. А количество порнографических страниц с каждым годом растёт в десятки раз быстрее, чем грибы после дождя.

Другая серьёзная проблема - распространение наркотиков через Глобальную Сеть. Достаточно набрать в поисковике название наркотического средства, чтобы узнать всё, начиная от того, как его приготовить до того, где взять. В апреле 2012 года Президент РФ Дмитрий Медведев на заседании президиума Государственного совета России выступил за контроль Интернета на предмет пропаганды наркотиков.

В Интернете легко найти информацию суицидального характера, видеоматериалы по дракам, вскрытиям. Здесь же дети, оставшись без надлежащего контроля родителей, могут свободно познакомиться с любыми формами экстремизма.

Интернет – реальный пожиратель времени. В поисках развлечений, играя или просто зависая в чате, можно проводить часы драгоценной жизни. В последние годы набирает обороты болезнь под названием «Интернет-зависимость». Дети начинают пропускать уроки, хуже учиться, становятся раздражительными. По мнению врачей, родителям следует контролировать, чтобы младший школьник проводил за компьютером не больше четверти часа. Бесконтрольное сидение в Интернете ведёт к тому, что дети теряют зрение, перестают заниматься спортом, теряют навыки общения вне Сети. В Китае несколько подростков умерли за компьютером не в силах оторваться от экрана, чтобы поесть.

Кроме того, через Интернет легко проникают вредоносные программы в виде вложенных файлов электронных писем, троянских коней, HTML и Java-вирусов и могут привести в поломке компьютера.

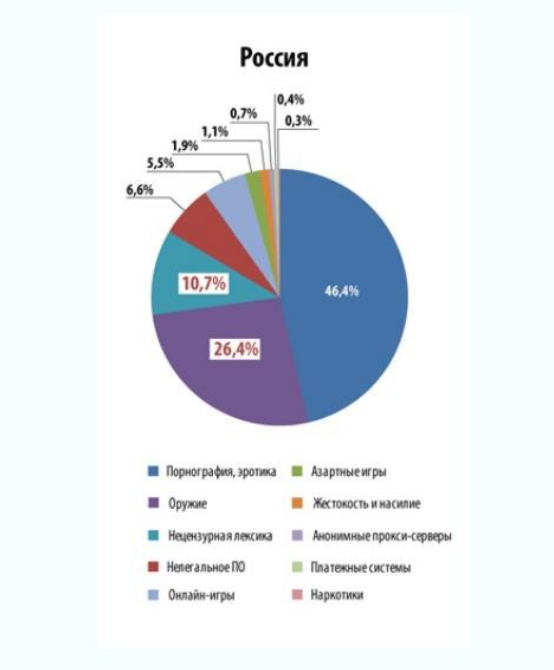
Вот почему идею празднования дня контроля Человека над Интернетом поддержали во всем мире. **С 2008 года в России существует Национальный узел Интернет-безопасности - Центр безопасного Интернета**. Он посвящён проблеме безопасной, корректной и комфортной работы в Глобальной сети. Создатели проекта уверены, что в условиях ускоренных темпов внедрения Интернета в повседневную жизнь граждан защита наших детей от рисков, скрытых в недрах всемирной паутины, требует активной позиции каждого.

Родительский контроль компьютера

Программы родительского контроля предназначены, в первую очередь, для создания ограничений ребёнку, они призваны обеспечить его безопасность, оградить от того, что, возможно, ему ещё рано знать и видеть. Одна из основных задач приложений – создание фильтра вебсайтов. Все очень просто: на одни страницы заходить можно, на другие – нельзя. Как осуществляется подобный контроль? Обычно предлагается два варианта ограничений.

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. Администратор или, в данном случае, родители могут расширять чёрный список сайтов на своё усмотрение. Статистика позволяет оценить, на какие категории сайтов с нежелательным контентом дети попадают чаще всего. Из

анализа были исключены социальные сети, онлайн-магазины, электронная почта и чаты. Рейтинг посещений сайтов представлен на диаграмме:



Довольно часто применяется более жёсткий способ контроля – создание белого списка. Ребёнок может посещать только те вебсайты, которые ему разрешили родители. Минус подобного контроля заключается в чрезмерной строгости, можно даже сказать, в жестокости. Пустили дочь за компьютер, а сайт с описаниями технических характеристик кукол не включили в белый список. Девочка в слезах. Подружки давно хвастаются новинками кукольного мира, а ребёнок даже не в курсе, о чем вообще сверстники ведут разговор, Интернета-то нормального нет. Зато не надо автоматически обновлять списки, актуальность со временем практически не теряется.

Ещё один способ родительского контроля заключается в фильтрации сайтов по их содержимому. Вы задаёте набор ключевых слов, и если что-либо из их списка обнаруживается на веб-странице, то она не открывается. Родителям, возможно, придётся отбросить прочь страх и стыд, самостоятельно вписывая мат, пошлости, уголовщину и прочие вещи, запрещённые для ребёнка.

Обеспечение безопасности ребёнка за компьютером заключается не только в ограничении доступа к вебсайтам. Есть ещё одна, если так можно выразиться, группа риска – это программы обмена мгновенными сообщениями. Ребёнок наивен, он можно нечаянно рассказать незнакомцу ваши личные данные. Злоумышленники хитры, они прикидываются ровесниками, невзначай задают каверзные вопросы. Напрашивается и вторая опасность – собеседники ребёнка могут научить его, в лучшем случае, мелким пакостям, а о примерах серьёзных бед лучше даже не вспоминать. Некоторые программы родительского контроля способны производить анализ информации, отправляемой с компьютера. Если в ней встречаются некие ключевые слова,

например, адрес, номер школы или телефона, то происходит блокировка отправки сообщения.

В вашей семье один ребёнок или несколько детей, есть компьютер, подключенный к Интернету. Как обезопасить младшее поколение от негативных последствий пребывания в Сети? Первое, что сразу напрашивается – компьютер не должен стоять в детской комнате. Лучше всего, если он будет в зале, где кто-нибудь родителей сможет постоянно следить за тем, чем занимается ребёнок. В противном случае, он запрётся в комнате, и вы даже, возможно, не догадаетесь, что чадом скачано несколько фильмов эротического содержания, а в местном чате ему рассказали, как самому делать петарды.

Ребёнку надо показать Интернет, заинтересовать полезными, с вашей точки зрения, сайтами, объяснить, что можно делать, а что нельзя. Нельзя соглашаться на встречи с незнакомыми людьми, нельзя сообщать личные данные, нельзя самостоятельно совершать покупки в сетевых магазинах. Ну а вместо нравоучений сыну «не смотри на голых женщин», уместней воспользоваться специальными программными продуктами, которые закроют ему доступ к взрослым ресурсам.

Идеального рецепта настройки родительского контроля не существует, поскольку тут всё зависит от целого ряда факторов: уровня компьютерной подготовки ребёнка и его родителей, компьютерных предпочтений и степени сознательности подрастающего поколения и, наконец, от отношения самих родителей к данной проблеме. Вариантов организации родительского контроля несколько. Можно ограничиться встроенными средствами Windows, задействовать модули родительского контроля в решениях класса Internet Security, подключиться к сервисам для фильтрации нежелательных сайтов либо установить специализированные программы родительского контроля.

Обучение детей основам безопасности при работе с Интернетом

Научите детей никому не сообщать пароли

Дети создают имена пользователей и пароли для доступа на сайт школы, игровые сайты, в социальные сети, для публикации фотографий, совершения покупок в Интернете и других операций.

Согласно исследованиям 75 процентов детей в возрасте от 8 до 9 лет сообщают свои пароли другим лицам, 66 процентов девочек в возрасте 7-12 признались, что сообщали свой пароль другим лицам.

Первое правило безопасности при работе в Интернете: пароли следует держать в секрете. Научите детей хранить свои пароли столь же бережно, как информацию, которую они хотя защитить.

Правила, которые дети должны знать и соблюдать:

Никогда не сообщайте свои пароли другим. Не показывайте никому свои пароли, даже друзьям.

Обеспечьте защиту для записанных паролей. Будьте внимательны к тому, где вы храните или записываете пароли. Не храните пароли в рюкзаке или бумажнике. Не оставляйте данные о паролях в местах, где вы бы не хотели оставить информацию, защищённую с их помощью. Не храните пароли в файле на компьютере. Преступники ищут там в первую очередь.

Никогда не предоставляйте свой пароль по электронной почте или в ответ на запрос по электронной почте. Любое сообщение электронной почты, в котором вас просят указать пароль или перейти на вебсайт, чтобы проверить пароль, может представлять собой разновидность мошенничества, которая называется фишингом.

К ним относятся запросы с сайтов, вызывающих доверие, которые вы можете постоянно посещать. Мошенники часто создают поддельные сообщения электронной почты, содержащие такие же логотипы как и на реальных сайтах и написанных таким языком, чтобы не вызывать сомнения в своей достоверности.

Не вводите пароли на компьютерах, которые вы не контролируете. Не пользуйтесь общедоступными компьютерами в школе, библиотеке, в интернет-кафе или в компьютерных лабораториях, кроме как для анонимного просмотра страниц в Интернете.

Не используйте эти компьютеры с учётными записями, где требуется вводить имя пользователя и пароль. Преступники могут за очень небольшие деньги приобрести устройства, регистрирующие нажатия клавиш, которые устанавливаются в течение нескольких секунд. С помощью подобных устройств злоумышленники могут собирать информацию, вводимую на компьютере, через Интернет.

2. Помощь детям в безопасном использовании социальных сетей

Ваши дети могут пользоваться сайтами социальных сетей, которые предназначены для детей, такими как Webkinz или Club Penguin, или сайтами, предназначенными для взрослых, такими как Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook и другие.

Дети используют социальные сети для общения с лицами, которые могут проживать на другом конце земного шара, или со своими знакомыми, с которыми они каждый день видятся в школе.

Дети должны понимать, что многие из этих сайтов социальных сетей могут просматриваться всеми, кто имеет доступ в Интернет.