МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по контролю за использованием несовершеннолетними сети Интернет во внеучебное время

Методические рекомендации адресованы заместителям руководителя по воспитательной работе, классным руководителям, родителям (законным представителям) обучающихся, обучающимся разного возраста.

Вместе с тем материал, приведенный в методических рекомендациях, будет полезен ученикам, абитуриентам, родителям, а также тем, кто проявляет интерес к безопасному использованию сети Интернет.

Введение

С 1 сентября 2012 года вступает в силу Федеральный закон Российской Федерации от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Следить за его соблюдением могут не только государственные органы, но и общественные организации, простые граждане. В законе прописаны виды информации, причиняющей вред здоровью и (или) развитию детей. Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью и развитию.

Кроме того, принят Федеральный закон Российской Федерации от 21 июля 2011 года № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у него искаженную картину мира и неправильные жизненные установки. Закон устанавливает порядок прекращения распространения продукции средств массовой информации, осуществляемого с нарушением законодательно установленных требований. Закон запрещает размещение рекламы в учебниках, учебных пособиях, другой учебной литературе, предназначенной для обучения детей, а также рекламу, содержащую информацию, запрещенную для распространения среди детей, в детских образовательных организациях.

Постоянное развитие интернет-технологий и их широкое проникновение в общество ставит перед государством и обществом задачу поддержания эффективного комплекса мер по профилактике, предотвращению и преодолению последствий вредоносных действий в отношении несовершеннолетних, совершаемых с применением Интернета или информационно-коммуникационных технологий. Для реализации такого комплекса мер был создан центр безопасного Интернета России при финансовой поддержке Федерального агентства по печати и массовым коммуникациям (http://www.saferunet.ru/).

Зачастую дети и подростки в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети. Сделать их пребывание в

Интернете более безопасным, научить их ориентироваться в киберпространстве — важная задача для родителей и педагогов.

Информация нежелательного характера. Контентные риски. Как их избежать?

Для полного понимания этого термина приведем определение понятия «контент». Контент – это наполнение или содержание какого-либо информационного ресурса: текст, графика, музыка, видео, звуки и т.д. (например, контент интернет-сайта); мобильный контент – мультимедийное наполнение, адаптированное для использования в мобильных устройствах (телефоны, смартфоны, коммуникаторы и т.д.): текст, графика, музыка, видео, игры, дополнительное программное обеспечение.

Информация нежелательного характера, которая несёт в себе контентные риски, – это различные информационные ресурсы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию.

К противозаконной, неэтичной и вредоносной информации относятся:

- пропаганда насилия, жестокости и агрессии;
- разжигание расовой ненависти, нетерпимости по отношению к другим людям по национальным, социальным, групповым признакам;
- пропаганда суицида;
- пропаганда азартных игр;
- пропаганда и распространение наркотических и отравляющих веществ;
- пропаганда деятельности различных сект, неформальных молодежных движений;
- эротика и порнография;
- нецензурная лексика и т.д.

В сети Интернет такую информацию можно встретить практически везде: в социальных сетях, блогах, персональных сайтах, видеохостингах и др. Не являются исключением и мобильные сервисы.

Размещение противозаконной информации в сети Интернет преследуется по закону. Это относится в первую очередь к распространению наркотических веществ, порнографических материалов, особенно с участием несовершеннолетних, призывам к разжиганию национальной розни и экстремистским действиям. В российском законодательстве есть возможность в соответствии со статьями уголовного кодекса привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов электронных текстов и видеопродукции.

Неэтичный, противоречащий принятым в обществе нормам морали и социальным нормам, контент не запрещён к распространению, но может содержать информацию, способную оскорбить пользователей и оказать вредоносное воздействие. Подобная информация не попадает под действие уголовного кодекса, но может оказать негативное влияние на психику человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, порнография, агрессивные онлайн-игры, азартные игры, информация о нездоровом образе жизни, принесении вреда здоровью и жизни, нецензурная брань, оскорбления и др.

Неэтичная и вредоносная информация может быть направлена на манипулирование сознанием и действиями различных групп людей. Такая информация часто бывает заманчивой и оказывает сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с негативным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков – непредсказуемо; под воздействием таких сайтов может пострадать не только психика, но и физическое здоровье ребёнка.

Вредоносный контент может привести к заражению компьютера вирусами и потере важных данных. Особенно опасными с этой точки зрения является просмотр через сеть Интернет тех или иных видеоматериалов. Очень многие распространители негативного контента преследуют определённую цель – заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера, получить деньги незаконным способом. Такие действия преследуются по закону в соответствии со ст. 272, 273, 274 Уголовного кодекса РФ.

Рекомендации для родителей по предупреждению контентных рисков.

Как избежать материалов с нежелательной информацией?

1. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой. 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 нужную информацию в разделе «Безопасность». Специальные программы, называемые системами родительского контроля, позволяют родителям самим решать, что их дети могут просматривать в Интернете, отсекать «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 также устанавливать непосредственно с помощью операционной системы, антивирусных программ, специальных программ.

2. Знайте, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые легко 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 определёнными параметрами или словами.

3. Создайте на компьютере несколько учетных записей, чтобы каждый пользователь мог входить в компьютер (систему) независимо и иметь собственный уникальный профиль. В таком случае ребенок будет 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 пароли. Пароль защищает компьютер и блокирует возможность его использования без разрешения владельца. Напомните вашему ребенку, что нельзя сообщать этот пароль друзьям, в противном случае пароль должен быть изменён.

4. Поддерживайте доверительные отношения с ребенком, чтобы всегда быть в курсе, с какой информацией он сталкивается в сети. Попав случайно на 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 онлайновых материалов и не доверять им без совета с вами.

5. 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 в оформлении информации, актуальность данных.

6. 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 контента.

Безопасное общение детей в сети Интернет.

Коммуникационные риски общения в Интернете.

Коммуникационные риски связаны с общением и межличностными отношениями интернет-пользователей. В Интернете существует много инструментов, позволяющих организовать места для общения, – социальные сети, блоги, чаты, форумы, гостевые книги, списки рассылки и пр. Примерами коммуникационных рисков могут служить знакомства в сети и встречи с интернет-знакомыми, интернет-хулиганство: преследование, запугивание и оскорбления, незаконные контакты и пр. С коммуникационными рисками можно столкнуться при общении в мобильных сервисах, чатах, онлайн-мессенджерах (ICQ, Skype, MSN и др.), социальных сетях, на сайтах знакомств, форумах, блогах и т.д. Интернет-хулиганство, киберпреследование, киберзапугивание (кибербуллинг) – это явления не только виртуальной, но и реальной жизни.

Основной площадкой для кибербуллинга в последнее время стали социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент.

Рекомендации для родителей по предотвращению интернет-хулиганства, кибербуллинга

1. Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не надо писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать.

2. Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Лучше вообще покинуть данный ресурс и удалить оттуда личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – полностью его игнорировать.

3. Обратите внимание на психологические особенности вашего ребенка. Признаки того, что ребёнок подвергается кибербуллингу, – различны, но есть несколько общих моментов: видимый эмоциональный стресс во время и после использования Интернета, прекращение общения с друзьями, прогулы учебных занятий, нестабильные оценки, резкие перемены в настроении, поведении, склонность к депрессии.

4. Если у вас есть информация, что кто-то из друзей или знакомых вашего ребёнка подвергается буллингу или кибербуллингу, то сообщите об этом классному руководителю или школьному психологу – необходимо принять меры по защите ребёнка.

5. Объясните детям, что личная информация, которую они выкладывают в Интернете (домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, личные фотографии) может быть использована агрессорами против них.

6. Помогите ребенку найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаления странички. Большинство социальных сетей и сервисов электронной почты имеют в настройках опцию «заблокировать пользователя» или «занести в чёрный список».

7. Поддерживайте доверительные отношения с ребенком, чтобы вовремя заметить, если в его адрес начнут поступать угрозы. Наблюдайте за его настроением во время и после общения с кем-либо в Интернете.

8. Убедитесь, что оскорбления (буллинг) из сети не перешли в реальную жизнь. Если поступающие угрозы являются достаточно серьезными, касаются жизни или здоровья ребенка, а также членов вашей семьи, то вы имеете право на защиту со стороны правоохранительных органов, а действия обидчиков могут подпадать под статьи Уголовного и Административного кодексов о правонарушениях.

Как помочь ребенку, если он уже столкнулся с Интернет-угрозой

1. Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности его состоянием. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.

2. Если ребенок расстроен увиденным (например, кто-то взломал его профиль в социальной сети) или попал в неприятную ситуацию (потратил деньги в результате интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в Интернете.
3. Если ситуация связана с насилием в Интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.
4. Соберите полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.
5. В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться по данной проблеме.

Рекомендации по предупреждению встречи с незнакомцами в сети

1. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе, с кем ребенок общается в сети. Обратите внимание, кого ребенок добавляет к себе «в друзья», с кем предпочитает общаться в сети – с ровесниками или людьми старше.
2. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать виртуальным знакомым свои фотографии или видео.
3. Объясните ребенку, что нельзя ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи, а также фотографии других людей без их разрешения.
4. Объясните ребенку, что при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), лучше не использовать реальное имя. Помогите ему выбрать ник, не содержащий никакой личной информации.
5. Объясните ребенку опасность встречи с незнакомыми людьми из Интернета. В сети человек может представиться кем угодно, поэтому на реальную встречу с интернет-другом надо обязательно ходить в сопровождении взрослых.

Электронные риски

Электронные риски – это вероятность столкнуться с хищением персональной информации и/или подвергнуться атаке вредоносных программ.

Вредоносные программы – различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может

нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с Интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из Интернета файлов.

Рекомендации по снижению рисков заражения компьютера вирусами и хищения персональной информации

1. Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры для предотвращения заражения компьютера и потери ваших данных. Подобные программы наблюдают за трафиком и могут остановить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.

3. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.

4. Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.

5. Регулярно делайте резервную копию важных данных, а также научите этому ваших детей.

6. Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п.).

7. Расскажите ребенку, что нельзя сообщать пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.

8. Расскажите ребенку, что если он пользуется Интернетом с помощью чужого устройства, он не должен забывать выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы. Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки – по этой информации злоумышленники могут многое узнать о вашем ребенке.

Рекомендации по предупреждению кибермошенничества

1. Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в Интернете.

2. Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать интернет-покупки.

3. Не отправляйте о себе слишком много информации при совершении интернет-покупок: данные счетов, пароли, домашние адреса и телефоны. Помните, что никогда администратор или модератор сайта не потребует полные данные

вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.
4. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.
5. Убедитесь в безопасности сайта, на котором вы или ваш ребёнок планируете совершить покупку.
6. Посещая веб-сайты, самостоятельно набирайте в браузере адрес веб-сайта или пользуйтесь ссылкой из «Избранного» (Favorites); никогда не щелкайте на ссылку, содержащуюся в подозрительном электронном письме.
7. Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют в том числе и многие банки в России.
8. Нужно как можно быстрее обратиться к настоящим сотрудникам организации, если получилось так, что конфиденциальная информация была предоставлена вами или вашими детьми неизвестным лицам, выдающим себя за сотрудников той или иной компании либо организации. При немедленном обращении компания может уменьшить ущерб, нанесенный вашей семье и другим лицам.

Правила безопасности при работе в социальных сетях

Социальные сети, такие как Одноклассники, Вконтакте, MySpace, Facebook, Twitter и многие другие, позволяют людям общаться друг с другом и обмениваться различными данными, например, фотографиями, видео и сообщениями. По мере роста популярности таких сайтов растут и риски, связанные с их использованием. Хакеры, спамеры, разработчики вирусов, похитители личных данных и другие мошенники не дремлют.

Одна из ключевых проблем социальных сетей – открытость большинства учетных записей. В частности, по различным оценкам, порядка 500 миллионов пользователей социальных сетей по всему миру держат свою частную информацию в открытом доступе, а эта информация может собираться с помощью автоматизированных решений. К примеру, подобный функционал может быть встроен во всевозможные приложения, которыми славится один из самых популярных подобных сервисов – Facebook.

Ни для кого не секрет, что в социальных сетях хранится много нежелательной информации: экстремистской, призывы к разжиганию национальной ненависти, порнография и т.п.

Рекомендации при работе в социальных сетях:

- Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях от других пользователей или друзей. Не следует бездумно открывать все ссылки подряд – сначала необходимо убедиться в том, что присланная вам ссылка ведет на безопасный или знакомый вам ресурс.
- Контролируйте информацию о себе, которую вы размещаете. Обычно злоумышленники взламывают учетные записи на сайтах следующим образом: они нажимают на ссылку "Забыли пароль?" на странице входа в учетную запись. При этом для восстановления или установки нового пароля система может предложить ответить на секретный вопрос. Это может быть дата рождения, родной город, девичья фамилия матери и т.п. Ответы на

подобные вопросы можно легко найти в сведениях, которые вы опубликовали на своей странице в какой-либо популярной социальной сети. Поэтому при установке секретных вопросов необходимо придумывать их самостоятельно (если сайт, на котором вы регистрируетесь, это позволяет) или по возможности не использовать личные сведения, которые легко найти в сети.

- Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете, только потому, что так написано. Помните, что хакеры могут взламывать учетные записи и рассылать электронные сообщения, которые будут выглядеть так, как будто они были отправлены вашими друзьями. Если у вас возникло такое подозрение, будет лучше связаться с отправителем альтернативным способом, например, по телефону, чтобы убедиться в том, что именно этот человек отправил вам данное сообщение. Точно так же необходимо относиться и к приглашениям зарегистрироваться в той или иной социальной сети.
- Чтобы не раскрыть адреса электронной почты своих друзей, не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты. При подключении к новой социальной сети вы можете получить предложение ввести адрес электронной почты и пароль, чтобы узнать, есть ли в этой сети пользователи, с которыми вы уже поддерживаете отношения при помощи электронной переписки. Используя эти данные, сайт может рассылать электронные сообщения (например, приглашения присоединиться к этой сети от вашего лица) всем пользователям из вашего списка контактов. Социальные сети должны предупреждать об этом, но зачастую этого не делают.
- Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки. Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.
- Не добавляйте в друзья в социальных сетях всех подряд. Мошенники могут создавать фальшивые профили, чтобы получить от вас информацию, которая доступна только вашим друзьям.
- Не регистрируйтесь во всех социальных сетях без разбора. Оцените сайт, который вы планируете использовать, и убедитесь, что вы правильно понимаете его политику конфиденциальности. Узнайте, существует ли на сайте контроль контента, который публикуется его пользователями. К сайтам, на которых вы оставляете свои персональные данные, необходимо относиться с той же серьезностью, которую требуют сайты, где вы совершаете какие-либо покупки при помощи кредитной карты.
- Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены. На большинстве сервисов вы можете в любой момент удалить свою учетную запись, но, несмотря на это, не забывайте, что практически любой пользователь может распечатать или сохранить на своем компьютере фотографии, видео, контактные данные и другие оставленные вами сведения.
- Проявляйте осторожность при установке приложений или дополнений для социальных сетей. Многие социальные сети позволяют загружать

сторонние приложения, которые расширяют возможности личной страницы. Довольно часто такие приложения используются для кражи личных данных, поэтому к их использованию необходимо относиться так же серьѐзно, как и к установке на свой компьютер программ, которые вы можете найти в Интернете.

- Расскажите вашим детям об опасностях, которые могут подстерегать их в социальных сетях. Если ваши дети посещают социальные сети, расскажите им о правилах безопасного пользования этими ресурсами.

Интернет–фильтры

Интернет–фильтры позволяют ограничить доступ в Интернет. Такие программы блокируют доступ к определённым сайтам, например, порноресурсам, сайтам с информацией об оружии и наркотиках, а также контролируют время 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 списков», гарантирующая 100%-ную защиту от опасных и нежелательных материалов. Фильтр «Интернет Цензор» можно скачать бесплатно на официальном сайте http://www.icensor.ru/. 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 образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет.

2. KinderGate Родительский Контроль 1.0. Эта программа-фильтр (www.usergate.ru) предлагает 82 категории фильтрации веб-сайтов в 5 основных уровнях доступа (по умолчанию запрещён доступ к фишинговым ресурсам, сайтам с порнографическим контентам, а также к сайтам, содержащим вредоносный код). Самый высокий уровень фильтрации подразумевает, в числе прочего, запрет прокси-серверов, сайтов знакомств. Доступно создание расширенных правил, «черных» и «белых» списков для сайтов. Можно установить ограничение скачивания видео, звуковых файлов, изображений, архивов и EXE-файлов, документов. 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 посещённых веб-ресурсов с указанием значений входящего и исходящего трафика, а также просмотр сообщений в сетях odnoklassniki.ru и vkontakte.ru.

3. Kaspersky Internet Security 2011 (www.kaspersky.ru) – антивирусная программа, которая защищает компьютер от вирусов и в состав которой 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 сетей MSN, Jabber, IRC, Mail.ru и Yahoo). Действия

ребенка 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 произведён эвристический анализ веб-страницы. Другой момент касается запрета передачи конфиденциальных данных, например, реквизитов банковской карты или домашнего адреса. Модуль родительского контроля позволит запретить загрузку следующих типов файлов: «Музыка», «Видео», «Программы» и «Архивы».

4. Интернет-фильтр «Кибер Папа» – бесплатная программа, которая ограничивает возможности ребенка выхода за пределы детского Интернета при использовании любого браузера. Скачать программу можно на официальном сайте http://cyberpapa.ru/. Программа работает по принципу «белого списка» и чрезвычайно проста в использовании. После ее инсталляции 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.

5. KidsControl – программа предназначена для ограничения доступа детей к нежелательным интернет-ресурсам, а также для контроля времени нахождения в сети. Скачать программу можно на официальном сайте http://www.kidscontrol.ru/. С ее помощью можно установить ограничение доступа к нежелательным ресурсам по различным категориям – сайтам для взрослых, online-играм и казино, форумам, – указав галочкой на определенную категорию, и установить ограничение с помощью чёрного списка.

Настройка функции родительского контроля в операционной системе Microsoft Windows 7

Функции «родительского контроля» предусмотрены в операционной системе Windows 7, которая устанавливается на большинство новых компьютеров и ноутбуков. В частности, Windows 7 даёт возможность ограничивать время, которое ребенок проводит за компьютером: вы можете разрешить ему играть в игры или пользоваться социальными сетями 2-3 часа в день. Кроме того, 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.

Для того чтобы активировать функцию родительского контроля в Windows 7:

1. Нажмите ***Панель управления/Учетные записи пользователей и семейная безопасность/Родительский контроль***. Щёлкните на учетную запись пользователя, чью работу за компьютером вы хотели бы контролировать. Если учётной записи нет, щёлкните ***Создать новую учётную запись*** (рис. 1).

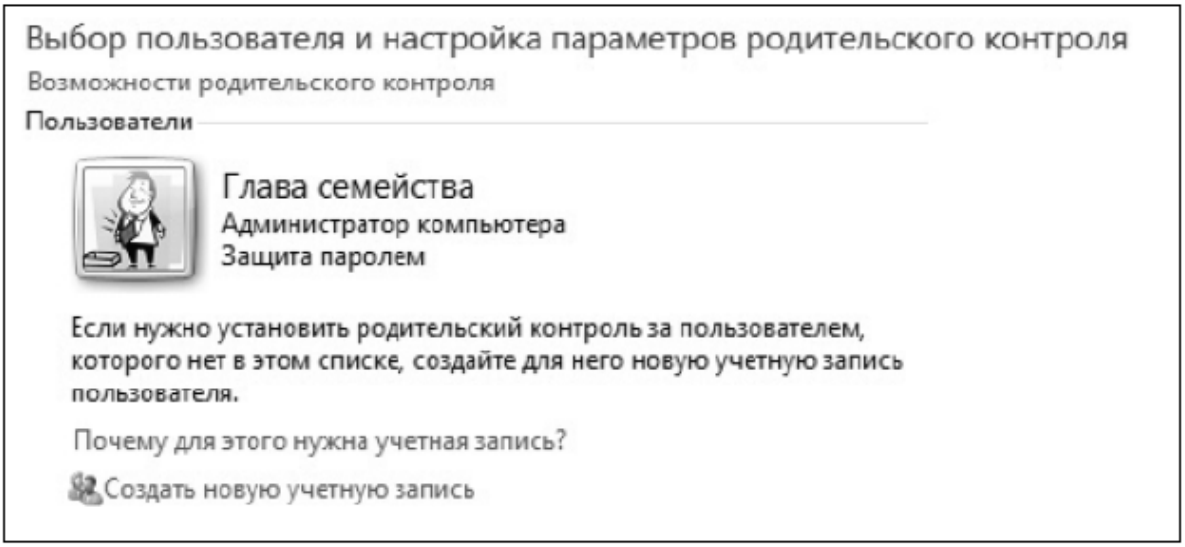


Рис. 1. Создание учётной записи

2. В появившемся окне в настройке ***Родительский контроль*** выберите ***Включить, используя текущие параметры***. Теперь вы можете установить ограничения по времени использования компьютера, а также играм и программам, которые можно запускать (рис. 2).

Рис. 2. Установка ограничения по времени

3. Для того чтобы установить ограничения времени использования компьютера, щёлкните ***Ограничения по времени***, в появившемся расписании выделите мышью дни и часы, в которые разрешается использовать компьютер.
4. Для того чтобы разрешить или блокировать конкретную программу, щёлкните ***Разрешение и блокировка конкретных программ***.

Настройка интернет-цензора

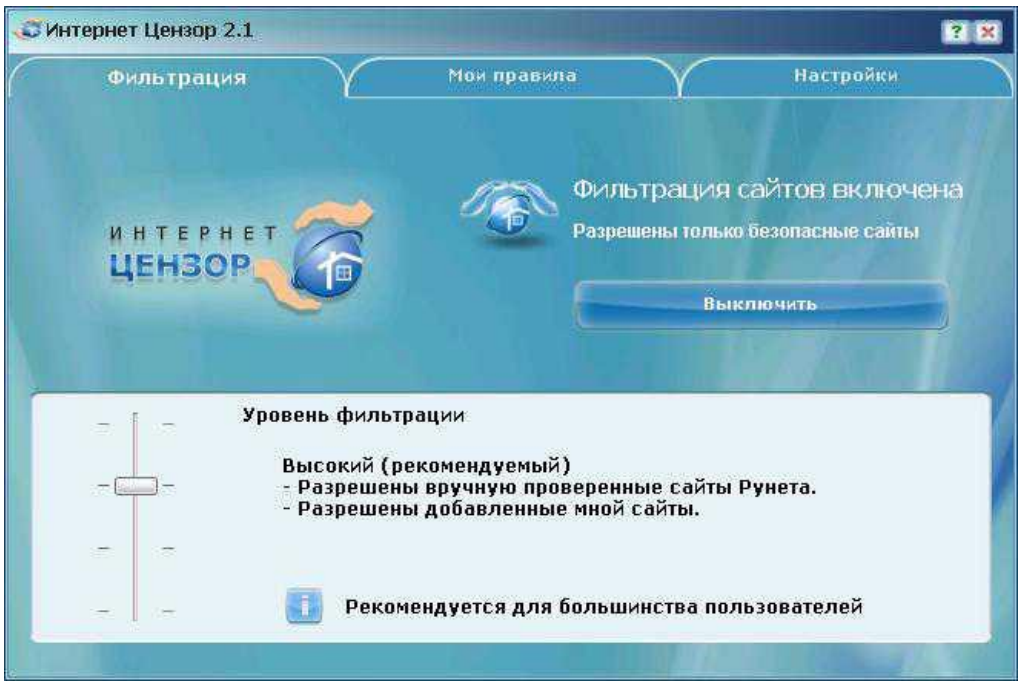
Чтобы открыть управляющее приложение, курсором мыши выберите изображение программы в панели инструментов и сделайте клик левой клавишей.

Перед вами появится окно с вводом пароля:

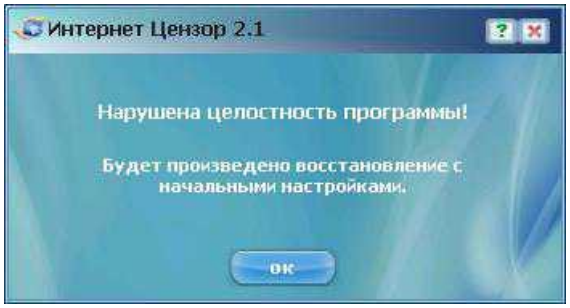
Введите пароль, который вы указали при установке программы.

Если вы забыли пароль, кликните по надписи «Напомнить пароль» для восстановления пароля на электронную почту.

Если введен правильный пароль, откроется окно программы:



Если значок свернутой программы мигает, меняя цвет с синего на красный, то это сигнал о том, что была попытка взлома программы (ребенок пытался удалить или вывести из строя «Интернет Цензор»). В этом случае на почтовый адрес, введенный вами при установке программы, будет отправлено соответствующее оповещение. Если вы кликнете на значок приложения, то откроется окно:



Следуйте инструкции, которую вы увидите в окне программы. **Управляющее приложение** поможет вам настроить программу «Интернет Цензор» под конкретные потребности.

Интерфейс приложения содержит 3 вкладки:

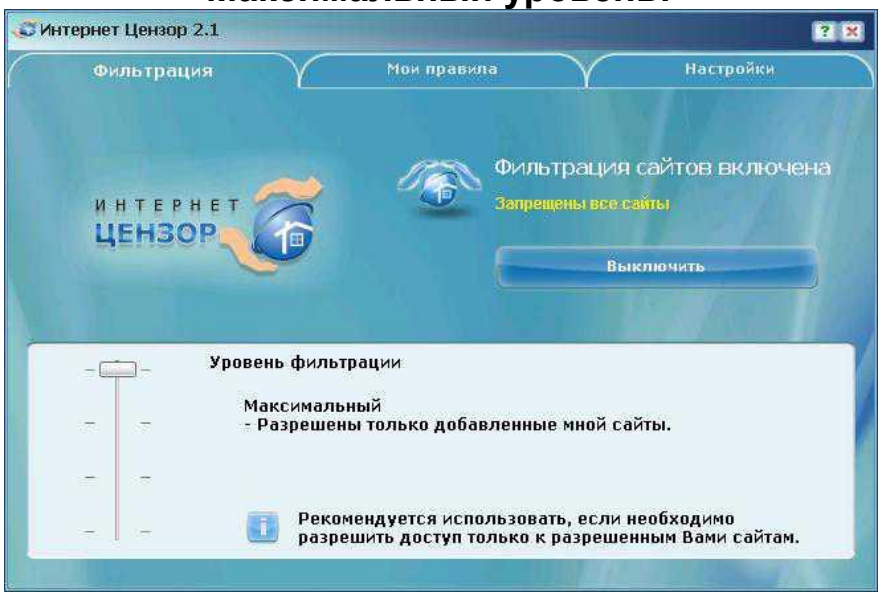
- Фильтрация
- Мои правила
- Настройки

Рассмотрим каждую из вкладок подробнее.

Вкладка «Фильтрация»

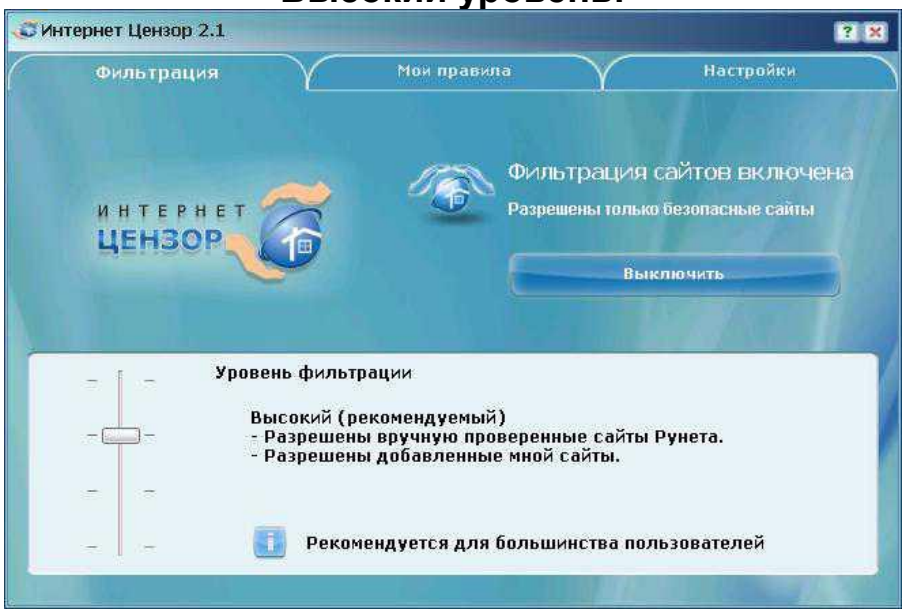
На этой вкладке вы можете управлять уровнями фильтрации. Каждый следующий уровень фильтрации (движение ползунка сверху вниз) является расширением предыдущего. Рассмотрим каждый уровень отдельно.

Максимальный уровень:



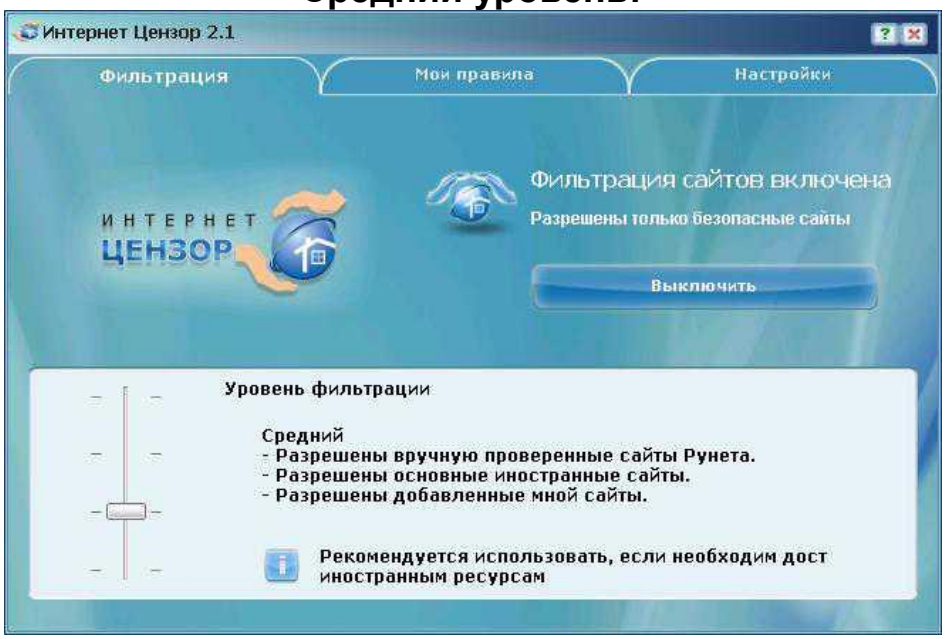
На этом уровне фильтрации разрешены только добавленные вами в «белый список» сайты на вкладке «Мои правила». Все остальные сайты Интернета будут блокироваться программой.

Высокий уровень:



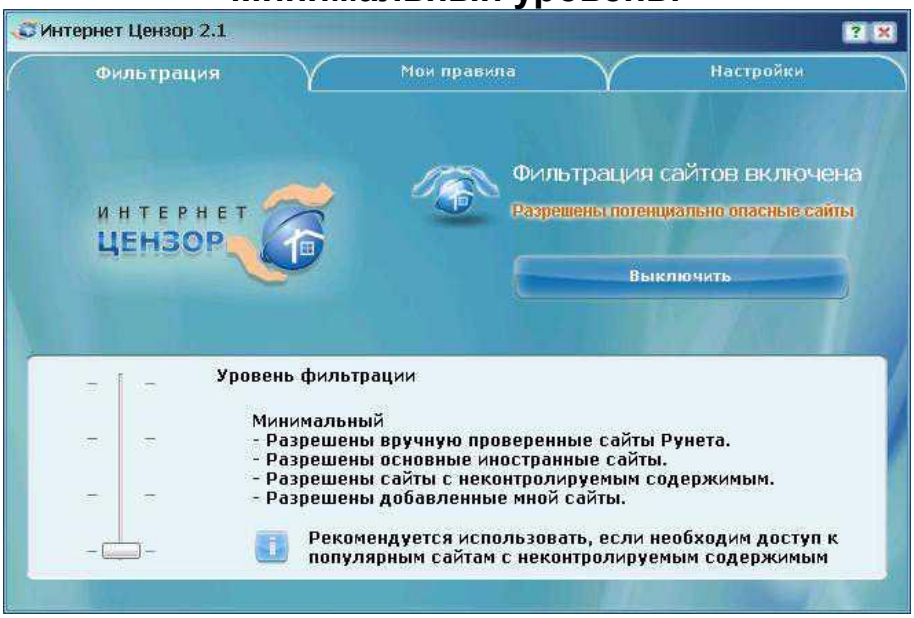
На этом уровне, кроме разрешенных вами сайтов, разрешена вручную проверенная база русского Интернета. Данный уровень является оптимальным, и мы рекомендуем использовать его.

Средний уровень:



На этом уровне то же, что и на **Высоком уровне** плюс база основных иностранных сайтов.

Минимальный уровень:



На этом уровне разрешено то же, что и на **Среднем уровне** плюс ресурсы с неконтролируемым содержимым:

- социальные сети,
- файлообменники и файлораздачи, в том числе сайты пиринговых сетей,
- фото- и видеохостинги (youtube.com, rutube.ru и т.д.),
- блоги (кроме профессиональных и тематических, например, allboxing.ru),
- чаты,
- онлайн-игры.

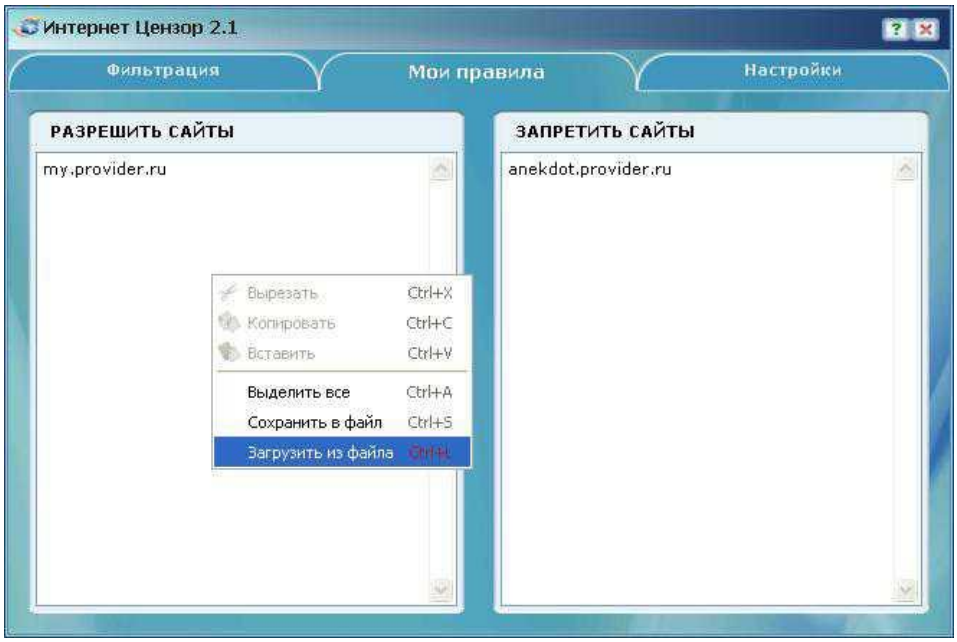
Вкладка «Мои правила»

На этой вкладке вы можете указать адреса интернет-сайтов, к которым должен быть разрешен или запрещен доступ. Внесенные вами изменения вступят в действие немедленно. Если введенные вами данные или часть данных изменит свой цвет на красный, то это значит, что была допущена ошибка в тексте. В этом случае вам следует сделать необходимые исправления.

Сайты, которые вы вносите в свои «черный» и «белый» списки, рекомендуется сохранять также и в отдельном текстовом файле. Если вам придется переустановить программу, все настройки сбросятся. В этом случае вы просто скопируете список ресурсов из текстового файла в списки программы.

Если вы захотите сохранить данные из «черного» или «белого» списка в текстовый файл, то при клике правой кнопкой мыши в области списка доступно меню с пунктом **Сохранить в файл**:

Вы также можете загрузить сайты из текстового файла в список, выбрав пункт **Загрузить из файла**:



Вкладка «Настройки»

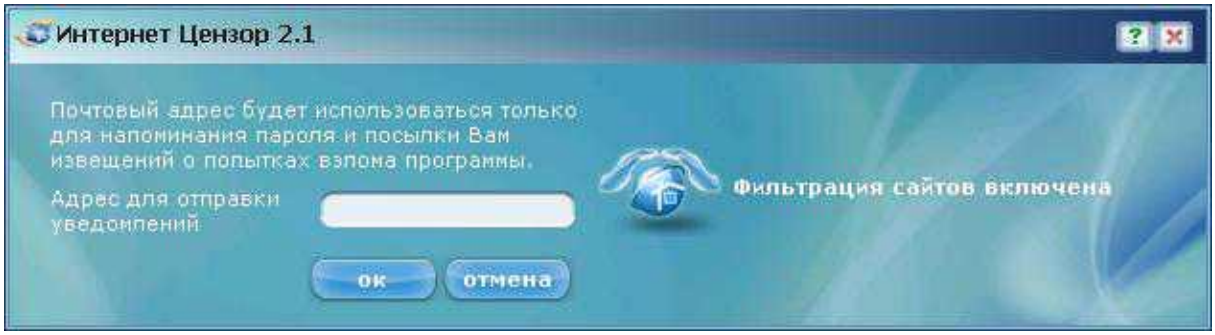
На этой вкладке вы можете:

- проверить обновления базы компании,
- изменить текущий пароль,
- изменить введенный вами ранее почтовый адрес, который используется для получения вами уведомлений о работе системы,
- наложить дополнительный запрет на активность в сети.

Если вы захотите изменить старый пароль, перед вами откроется окно:

Введите сначала старый пароль, а затем новый. Подтвердите новый пароль и нажмите кнопку «ОК».

Окно смены почтового адреса выглядит так:



Введите в поле тот адрес электронный почты, по которому вы хотите в дальнейшем получать сведения о работе программы. Напоминаем, что этот почтовый адрес используется исключительно для отправки на него уведомлений о попытке взлома программы на вашем компьютере.

Запрет на дополнительную активность в сети

В этом случае вы можете запретить:

- использование интернет-пейджеров, таких как программы обмена мгновенными сообщениями типа ICQ (а также других клиентов сети ICQ, например, QIP), Mail.ru Агент;
- использование клиентов файлообменных сетей, например, BitTorrent.

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 определёнными 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. 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».

Службы помощи

Фонд поддержки детей, находящихся в трудной жизненной ситуации (http://www.fond-detyam.ru) – общероссийский проект «Телефон доверия». По телефону 8-800-2000-122 предоставляются психологические консультации по проблемам насилия и принуждения к сексуальной эксплуатации, оказывается помощь жертвам подобных преступлений, а также консультации по всем психологическим проблемам детей и подростков. Все консультации и звонок на телефонный номер Линии помощи бесплатны; консультации предоставляются круглосуточно. На сайте Фонда можно получить консультации, вступив в переписку со специалистами Фонда.

На сайте ***Я – родитель*** (http://www.ya-roditel.ru) размещены полезные материалы, адресованные родителям, обеспокоенным интернет-угрозами детям.

На сайте Центра безопасного Интернета в России http://www.saferunet.ru необходимо кликнуть на красный баннер «горячая линия» и сообщить о противоправном контенте. На сайте размещена линия помощи – консультации по вопросам интернет-угроз. По всем вопросам, связанным с безопасным использованием Интернета, – посредством тематических веб-форм обращений на сайте или через электронную почту helpline@saferunet.ru; по общим вопросам, в том числе по вопросам, связанным с безопасным использованием Интернета, – посредством тематических веб-форм на специальном сайте http://www.psyhelpline.ru.

Линия помощи «Дети – онлайн» http://www.detionline.com – служба телефонного и онлайн-консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи.

Обратиться на линию помощи можно по телефону 8-800-250-00-15 (звонить с 9.00 до 18.00 по рабочим дням, время московское, звонки по России – бесплатные), по электронной почте helpline@detionline.com.

Список терминов

Блог (англ. blog, интернет-журнал событий, интернет-дневник, онлайн-дневник) – веб-сайт, основное содержимое которого – регулярно добавляемые записи (посты), содержащие текст, изображения или мультимедиа.

Браузер (от англ. *Web browser)* – программное обеспечение для просмотра веб-сайтов, то есть для запроса веб-страниц, их обработки, вывода и перехода от одной страницы к другой.

Видеохостинг – сайт, позволяющий загружать и просматривать видео в браузере, например, через специальный проигрыватель.

Вишинг – разновидность фишинга – распространенного сетевого мошенничества, при котором клиенты какой-либо платежной системы получают сообщения по электронной почте якобы от администрации или службы безопасности данной системы с просьбой указать свои счета, пароли и т.д. При этом ссылка в сообщении ведет на поддельный сайт, на котором и происходит кража информации. Сайт этот уничтожается через некоторое время, и отследить его создателей в Интернете достаточно сложно.

Интернет-мошенничество или кибермошенничество – один из видов киберпреступления, целью которого является обман пользователей.

Кибербуллинг – виртуальный террор, чаще всего подростковый.

Контент (от англ. content – содержание) – абсолютно любое информационно значимое, содержательное наполнение информационного ресурса или веб-сайта. Контентом называются тексты, мультимедиа, графика.

Социальная сеть – платформа, онлайн-сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений.

Фарминг – процедура скрытного перенаправления жертвы на ложный IP-адрес. Для этого может использоваться навигационная структура.

Фишинг – вид интернет-мошенничества, основанный на незнании пользователями норм сетевой безопасности, целью которого является получение доступа к конфиденциальным данным – логинам и паролям. Фишинг-атаки проводятся через электронную почту, всплывающие сообщения и ссылки на фишинговые веб-сайты с целью обманным путем выявить у получателя личную информацию, часто финансового характера.

Нигерийские письма – распространённый вид мошенничества, получивший развитие с появлением массовых рассылок по электронной почте (спама).

Полезные сайты для родителей

1. http://www.nachalka.com/bezopasnost – Безопасность детей в Интернете
2. http://detionline.com/ – Дети России Онлайн. Сделаем Интернет безопаснее вместе
3. http://www.ifap.ru/library/book099.pdf – Безопасность детей в Интернете
4. http://www.microsoft.com/ru-ru/security/default.aspx – Центр безопасности Microsoft
5. http://stopfraud.megafon.ru/parents/ – Безопасный Интернет от Мегафон
6. http://www.fid.su/projects/journal/ – Фонд развития Интернет. Журнал «Дети в информационном обществе»
7. http://www.mts.ru/help/useful_data/safety/ – Безопасный Интернет от МТС
8. http://safe.beeline.ru/index.wbp – Безопасный Интернет от Билайн
9. http://www.saferunet.ru/ – Центр безопасного Интернета в России
10. http://edugalaxy.intel.ru/index.php?automodule=blog&blogid=56&showentry=861 – Настраиваем безопасный поиск в Интернете
11. http://www.kaspersky.ru/crystal2011 – Kaspersky CRYSTAL
12. http://www.friendlyrunet.ru/safety/74/index.phtml – Фонд «Дружественный Рунет»
13. http://netpolice.ru/filters/ – Фильтры NetPolice
14. http://content-filtering.ru/index/ – Информационно-аналитический ресурс «Ваш личный Интернет»
15. http://www.socobraz.ru/index.php/Сообщество_родителей – Сообщество родителей СОЦОБРАЗ
16. http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx – Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей?
17. http://www.microsoft.com/ru-ru/security/family-safety/childsafety-internet.aspx – Обучение детей основам безопасности при работе с Интернетом
18. http://windows.microsoft.com/ru-RU/windows7/products/features/parental-controls – Родительский контроль в Windows 7
19. http://play.mirchar.ru/sovety-roditelyam-po-obespecheniyu-bezopasnosti-detey.html – Консультации для родителей по обеспечению безопасности детей в Интернет
20. http://interneshka.net/parents/index.phtml – Советы родителям о безопасности в Интернете
21. http://www.ifap.ru/library/book336.pdf – Медиаобразование для родителей: освоение семейной медиаграмотности
22. http://icensor.ru/ – Бесплатный интернет-фильтр для детей «Интернет Цензор»
23. http://www.internet-kontrol.ru/ –Защита детей от вредной информации в сети Интернет
24. http://www.oszone.net/6213/ – Обеспечение безопасности детей при работе в Интернет
25. http://wiki.saripkro.ru/index.php/Интернет-безопасность_для_родителей – Интернет-безопасность для родителей
26. https://www.securelist.com/ru/analysis/208050705/Deti_onlayn_tekhnika_bezopasnosti – Дети онлайн: техника безопасности
27. http://www.sch169.ru/doc/pam.pdf – Как защититься от интернет-угроз