# Обеспечение безопасности детей при работе в Интернет

**Вступление**

Сегодня все больше и больше компьютеров подключаются к работе в сети Интернет. При этом все большее распространение получает подключение по высокоскоростным каналам, как на работе, так и дома. Все большее количество детей получает возможность работать в Интернет. Но вместе с тем все острее встает проблема обеспечения безопасности наших детей в Интернет. Так как изначально Интернет развивался вне какого-либо контроля, то теперь он представляет собой огромное количество информации, причем далеко не всегда безопасной. В связи с этим и с тем, что возраст, в котором человек начинает работать с Интернет, становится все моложе, возникает проблема обеспечения безопасности детей. А кто им может в этом помочь, если не их родители и взрослые?

Следует понимать, что подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.

Какие угрозы встречаются наиболее часто? Прежде всего:

• **Угроза заражения вредоносным ПО.** Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.

• **Доступ к нежелательному содержимому.** Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще всего порнографического характера.

• **Контакты с незнакомыми людьми с помощью чатов или электронной почты.** Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.

## Услуги Интернет

• **Неконтролируемые покупки.** Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

Именно обеспечению безопасности наших детей при пребывании в сети Интернет и будет посвящена наша статья.

Интернет это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что как и наш реальный мир, всемирная паутина так, же может быть весьма и весьма опасна. Приведем несколько рекомендаций, с помощью которых посещение Интернет может стать менее опасным для ваших детей:

1. Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет;

**2.** Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;

**3.** Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации;

**4.** Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.;

**5.** Объясните своему ребенку, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками;

**6.** Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;

**7.** Скажите им, что никогда не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают;

**8.** Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернет – правда. Приучите их спрашивать о том, в чем они не уверены;

**9.** Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

**Как научить детей отличать правду ото лжи в Интернет?**

Следует объяснить детям, что нужно критически относиться к полученным из Интернет материалам, ведь опубликовать информацию в Интернет может абсолютно любой человек. Объясните ребенку, что сегодня практически каждый человек, может создать свой сайт и при этом никто не будет контролировать, насколько правдива размещенная там информация. Научите ребенка проверять все то, что он видит в Интернет.

**Как это объяснить ребенку?**

• **Начните, когда ваш ребенок еще достаточно мал**. Ведь сегодня даже дошкольники уже успешно используют сеть Интернет, а значит нужно, как можно раньше научить их отделять правду ото лжи;

## Темы бесед с детьми о безопасном использовании ресурсов сети Интернет

• **Не забывайте спрашивать ребенка об увиденном в Интернет**. Например, начните с расспросов, для чего служит тот или иной сайт.

• **Убедитесь, что ваш ребенок может самостоятельно проверить прочитанную в Интернет информацию по другим источникам** (по другим сайтам, газетам или журналам). Приучите вашего ребенка советоваться с вами. Не отмахивайтесь от их детских проблем.

• **Поощряйте ваших детей использовать различные источники**, такие как библиотеки или подарите им энциклопедию на диске, например, «Энциклопедию Кирилла и Мефодия» или Microsoft Encarta. Это поможет научить вашего ребенка использовать сторонние источники информации;

• **Научите ребенка пользоваться поиском в Интернет.** Покажите, как использовать различные поисковые машины для осуществления поиска;

• **Объясните вашим детям, что такое расизм, фашизм, межнациональная и религиозная вражда.** Несмотря на то, что некоторые подобные материалы можно

заблокировать с помощью специальных программных фильтров, не стоит надеяться на то, что вам удастся отфильтровать все подобные сайты.

**Семейное соглашение о работе в Интернет**

Если ваши дети хотят посещать Интернет, вам следует выработать вместе с ними соглашение по использованию Интернет. Учтите, что в нем вы должны однозначно описать права и обязанности каждого члена вашей семьи. Не забудьте четко сформулировать ответы на следующие вопросы:

- Какие сайты могут посещать ваши дети и что они могут там делать;
- Сколько времени дети могут проводить в Интернет;
- Что делать, если ваших детей что-то беспокоит при посещении Интернет;
- Как защитить личные данные;
- Как следить за безопасностью;
- Как вести себя вежливо;
- Как пользоваться чатами, группами новостей и службами мгновенных сообщений.

Не забудьте, что формально составленное соглашение не будет выполняться! Регулярно, по мере необходимости, вносите изменения в данное соглашение. Не забывайте, что вы должны проверять выполнение соглашения вашими детьми.

**Научите вашего ребенка использовать службу мгновенных сообщений**

При использовании службы мгновенных сообщений напомните вашему ребенку некоторые несложные правила безопасности:

- Никогда не заполняйте графы, относящиеся к личным данным, ведь просмотреть их может каждый;
- Никогда не разговаривайте в Интернет с незнакомыми людьми;
- Регулярно проверяйте список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;
- Внимательно проверяйте запросы на включение в список новых друзей. Помните, что в Интернете человек может оказаться не тем, за кого он себя выдает;
- Не следует использовать систему мгновенных сообщений для распространения слухов или сплетен.

## Советы по безопасности при работе с ресурсами сети Интернет для детей разного возраста

Родителям не стоит надеяться на тайную слежку за службами мгновенных сообщений, которыми пользуются дети. Гораздо проще использовать доброжелательные отношения с вашими детьми.

**Может ли ваш ребенок стать интернет-зависимым?**

Не забывайте, что Интернет это замечательное средство общения, особенно для стеснительных, испытывающих сложности в общении детей. Ведь ни возраст, ни внешность, ни физические данные здесь не имеют ни малейшего значения. Однако этот путь ведет к формированию Интернет-зависимости. Осознать данную проблему весьма сложно до тех пор, пока она не становится очень серьезной. Да и, кроме того, факт наличия такой болезни как Интернет-зависимость не всегда признается. Что же делать?

Установите правила использования домашнего компьютера и постарайтесь найти разумный баланс между нахождением в Интернет и физической нагрузкой вашего ребенка. Кроме того, добейтесь того, чтобы компьютер стоял не в детской комнате, а в комнате взрослых. В конце-концов, посмотрите на себя, не слишком ли много времени вы проводите в Интернет.

**Советы по безопасности для детей разного возраста**

Как показали исследования, проводимые в сети Интернет, наиболее растущим сегментом пользователей Интернет являются дошкольники.

В этом возрасте взрослые будут играть определяющую роль в обучении детей безопасному использованию Интернет.

**Что могут делать дети в возрасте 5-6 лет?**

Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями.

Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, все же они сильно зависят от вас при поиске детских сайтов. Как им помочь делать это безопасно?

• В таком возрасте желательно работать в Интернет только в присутствии родителей;

• Обязательно объясните вашему ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира;

• Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети;

• Используйте специальные детские поисковые машины, типа MSN Kids Search;

• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

• Научите вашего ребенка никогда не выдавать в Интернет информацию о себе и своей семье;

• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

Ваши дети растут, а, следовательно, меняются их интересы.

**Возраст от 7 до 8 лет**

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернет ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей.

Поэтому в данном возрасте особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).

В результате, у вашего ребенка не будет ощущения, что вы глядите ему через плечо на экран, однако, вы будете по-прежнему знать, какие сайты посещает ваш ребенок.

Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты хотелось бы заметить, что в данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку.

Помочь вам запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как Kaspersky Internet Security со встроенным родительским контролем.

**Что можно посоветовать в плане безопасности в таком возрасте?**

• Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;

• Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;

• Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;

• Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый "белый" список Интернет с помощью средств Родительского контроля. Как это сделать, мы поговорим позднее;

• Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;

• Используйте специальные детские поисковые машины, типа MSN Kids Search;

• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

• Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса;

• Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО;

• Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей;

• Научите детей не загружать файлы, программы или музыку без вашего согласия;

• Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.

• Не разрешайте детям использовать службы мгновенного обмена сообщениями;

• В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией;

• Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни;

• Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых»;

• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

**9-12 лет**

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

**Советы по безопасности в этом возрасте**

• Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;

• Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;

• Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;

• Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;

• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

• Не забывайте беседовать с детьми об их друзьях в Интернет;

• Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет;

• Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними;

• Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет;

• Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение;

• Создайте вашему ребенку ограниченную учетную запись для работы на компьютере;

• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах.

Похвалите их и посоветуйте подойти еще раз в подобных случаях;

• Расскажите детям о порнографии в Интернет;

• Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами;

• Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

**13-17 лет**

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

**Советы по безопасности в этом возрасте**

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы.

Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок для "взрослых". Девочки предпочитают общаться в чатах, при этом они гораздо боле чувствительны к сексуальным домогательствам в Интернет.

Что посоветовать в этом возрасте?

• Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах);

• Компьютер с подключением к Интернет должен находиться в общей комнате;

• Часы работы в Интернет могут быть легко настроены при помощи средств Родительского контроля Kaspersky Internet Security;

• Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы;

• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

• Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме;

• Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернет;

• Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет;

• Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение;

• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях;

• Расскажите детям о порнографии в Интернет;

• Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры;

• Приучите себя знакомиться с сайтами, которые посещают подростки;

• Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям;

• Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закона.

## Как проводить Родительский контроль над поведением детей в Интернет?

Обеспечивать родительский контроль в Интернет можно с помощью различного программного обеспечения. В данной статье мы рассмотрим только некоторое ПО, в частности, Родительский контроль в Windows 7, средства Родительского контроля, встроенные в Kaspersky Internet Security. Рассмотрим их подробнее.

Идеального рецепта настройки родительского контроля не существует, поскольку тут всё зависит от целого ряда факторов: уровня компьютерной подготовки ребенка 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. Рассмотрим данные варианты на практике.

**Используем встроенные возможности Windows 7/Vista**

Встроенные средства Windows 7/Vista позволяют вводить некоторые ограничения, касающиеся работы ребенка на компьютере, — устанавливать временной интервал, в течение которого дети могут пользоваться компьютером, а также определять перечень доступных игр и приложений . Этого может оказаться вполне достаточно для ограничения компьютерной деятельности детей младшего возраста.

В Windows Vista дополнительно предусмотрен функционал для блокирования доступа к некоторым сайтам и другим интернет-сервисам. Операционная система Windows 7 встроенного вебфильтра не имеет — по замыслу разработчиков для организации расширенного родительского контроля в этой ОС предназначена программа Family Safety («Семейная безопасность») из пакета Windows Live Essentials 2011. С ее помощью можно блокировать доступ к нежелательным сайтам, определять контакты, с которыми ребенок

может общаться через Интернет (только в Windows Live Hotmail и Windows Live Messenger), и просматривать отчеты о действиях чада в Сети.

Для настройки родительского контроля встроенными средствами Windows необходимо иметь отдельную учетную запись с правами администратора, а также одну (или более, если детей несколько и требуется разграничение прав) учетную запись обычного пользователя, под которой ребенок будет заходить в систему. Разумеется, гостевой профиль должен быть отключен, а на профиль администратора установлен пароль — в противном случае ребенок рано или поздно отключит родительский контроль и будет использовать компьютер безо всяких ограничений.

Технология настройки ограничений никаких сложностей не вызывает — достаточно из панели управления открыть модуль «Родительский контроль», выбрать учетную запись, под которой заходит ребенок, и определить требуемые настройки.

Можно, например, настроить расписание работы по дням недели, что позволит ограничить общее время работы на компьютере, поскольку по окончании разрешенного периода времени будет происходить автоматический выход из системы. Не сложнее окажется отрегулировать доступ к играм, установив на них общий запрет либо запретив доступ только к отдельным установленным на компьютере играм, указав их вручную либо путем выбора возрастной категории.

Стоит отметить, что полный запрет на игры — вполне разумная (а вовсе не драконовская) мера, которая имеет смысл, если у ребенка для работы на компьютере используются два профиля: «Ученик» и «Игрок». При этом для профиля «Ученик» полностью запрещен доступ к играм, а для профиля «Игрок» установлены четкие временные рамки, что позволяет ограничить время на компьютерные игры, но разрешить доступ к компьютеру в учебных целях. В дополнение также стоит отметить, что ограничение доступа по времени легко может быть обойдено путем смены компьютерного времени, о чем рано или поздно догадается любой ребенок. Поэтому установка пароля на BIOS — условие обязательное, которое для надежности также может быть подкреплено настройкой синхронизации времени на компьютере с временны*ы*ми серверами в Интернете.

**Привлекаем к контролю решения класса Internet Security**

Если на компьютере используется комплексный продукт защиты класса Internet Security, то имеет смысл попытаться настроить нужный вариант ограничений с помощью модуля родительского контроля, который сегодня является обязательным компонентом таких решений. Данный вариант тем более привлекателен, что наиболее популярный среди российских пользователей в этом классе инструмент — Kaspersky Internet Security 2012 — недавно был признан лучшим в тестах родительского контроля Anti-Malware.ru в плане эффективности блокирования ресурсов порнографической и эротической тематики. Остановимся на возможностях родительского контроля в данном решении подробнее.

**Kaspersky Internet Security 2012**

*Разработчик:* Лаборатория Касперского

*Сайт программы:* http://www.kaspersky.ru/multi-device-security

*Работа под управлением:* Windows XP/Vista/7

Kaspersky Internet Security — ориентированный на домашних пользователей инструмент для многоуровневой защиты от всех интернет-угроз: вирусов, хакерских атак и спама. Данное решение базируется на параллельном использовании «облачных» и традиционных антивирусных технологий, что позволяет достичь максимального уровня безопасности компьютера. Продукт включает базовые инструменты обеспечения антивирусной безопасности, а также большой набор дополнительных модулей. В их числе — безопасная среда запуска приложений и браузеров, монитор активности программ, сетевой экран, родительский контроль и т.д.

Входящий в состав продукта модуль «Родительский контроль» позволяет регулировать доступ детей к вебсайтам и их общение в социальных сетях («ВКонтакте», «Одноклассники.ру», Facebook, Twitter и др.) и через программы обмена сообщениями (ICQ и др.), а также ограничивать время доступа к компьютеру и отдельным приложениям.

Настроить родительский контроль в Kaspersky Internet Security очень просто. Достаточно в окне модуля «Родительский контроль» выбрать учетную запись ребенка и отрегулировать настройки. Таким способом можно ограничить время работы ребенка на компьютере либо в Сети, составив расписание и/или ограничив отводимое на это суммарное время в сутки, а также определить разрешенные/запрещенные для использования приложения (в том числе по времени).

Несложно ввести ограничения на доступ к вебсайтам в зависимости от их содержимого. Настраивается система ограничений путем выбора категорий вебсайтов, доступ к которым следует заблокировать, формирования списка исключений (при необходимости) и включения/отключения режима безопасного поиска, который будет применяться во время работы пользователя с поисковыми системами (для Google и Bing.com).

Кроме того, разрешается ограничивать загрузку определенных типов файлов и осуществлять контроль переписки через интернет-пейджеры и в социальных сетях путем блокирования переписки с контактами, с которыми общение запрещено. Предусмотрен мониторинг переписки с учетом употребления указанных родителем конкретных слов и блокирование пересылки данных, содержащих персональную информацию (например, домашний адрес, номер телефона). Все действия пользователей, для которых настроен родительский контроль, фиксируются в детальных отчетах по всем категориям контролируемых событий.

**Устанавливаем специализированные инструменты**

Альтернативным вариантом организации родительского контроля может стать использование специализированных программных продуктов. Подобных решений на рынке представлено очень много, а их функциональность может быть самой разной. Мы остановимся на 3-х разноплановых продуктах от российских разработчиков — Интернет Цензор, Time Boss и «KinderGate Родительский Контроль».

**INTERNET CENZOR**

*Разработчик:* Интернет Цензор

*Сайт программы:* www.icensor.ru

*Работа под управлением:* Windows XP/Vista/7

Интернет Цензор — бесплатная программа для осуществления родительского контроля. Программа предназначена для эффективной блокировки сайтов, которые могут представлять опасность для ребенка, когда он использует Интернет.

Программа Интернет Цензор разработана отечественными специалистами для обеспечения надежного запрета на посещения нежелательных сайтов в интернете. В своей работе программа ориентируется на так называемый «белый список» сайтов, посещение которых разрешено. Все остальные сайты в интернете будут недоступны.

Всего в базе «белого списка» программы Интернет Цензор находится более миллиона сайтов проверенных вручную. В этот список включены проверенные сайты российского интернета и основные зарубежные сайты.

При использовании программы происходит фильтрация ресурсов в интернете, в зависимости от настроек программы. Приоритет имеют вручную добавленные пользователем списки сайтов, которые будут доступны или, наоборот, недоступны в зависимости от предпочтений пользователя.

Во время включенного режима фильтрации, интернет-трафик будет идти через программу Интернет Цензор, поэтому попытки обойти фильтрацию не увенчаются успехом.

Программу нельзя будет просто так удалить с компьютера, так как для этого потребуется пароль от программы.

При попытке удаления или обхода фильтрации на адрес электронной почты, указанный в программе придет сообщение о таких действиях.

Бесплатную программу Интернет Цензор можно скачать с официального сайта производителя. Программа рекомендована для использования государственными и общественными структурами.

**Time Boss 2.5**

*Разработчик:* Nicekit Software

*Сайт программы:* http://nicekit.ru/parental-control/time-boss.php

*Работа под управлением:* Windows XP/Vista/7

Time Boss — простая и удобная программа для организации родительского контроля. С ее помощью родители легко могут ограничивать время компьютерной деятельности ребенка (в том числе в играх и Интернете), определять перечень доступных приложений (включая игры), вводить ограничения на ряд системных операций, запрещать доступ к отдельным папкам, а также регулировать посещение сайтов при интернет-серфинге. Программа обеспечивает контроль для всех зарегистрированных в системе пользователей и потому при необходимости может быть использована для настройки разных вариантов ограничений по различным профилям. В целях защиты от взлома подрастающим поколением разработчики предусмотрели ряд возможностей: использование пароля доступа к программе, работу в скрытом («Стелс») режиме, защиту от удаления приложения при загрузке Windows в безопасном режиме Safe mode и др. Приложение предлагается в двух редакциях: базовой Time Boss и расширенной Time Boss PRO. Редакция Time Boss PRO дополнительно предоставляет функционал для удаленного управления в рамках локальной домашней сети (можно удаленно менять настройки, оперативно добавлять время и пр.) и оснащена защитой от кейлоггеров (чтобы исключить возможность получения ребенком пароля доступа к программе).

Принцип использования Time Boss очень прост — для каждого пользователя Windows создаются профили типов «Родитель» и «Ребенок». Пользователям типа «Ребенок» настраивается компьютерное расписание, которое позволит четко определить часы для работы на компьютере в целом, а также в Интернете и с конкретными приложениями путем управления белыми и черными списками. Последнее окажется полезным для ограничения игровой деятельности — игры можно вовсе запретить, указав их в черном списке, либо разрешить только по вечерам — то есть после подготовки домашних заданий. В ходе настройки расписания разрешается не только устанавливать временны*е* интервалы, но и указывать общее допустимое количество компьютерного времени на день, а также вводить при работе принудительные перерывы. При необходимости также можно вводить системные ограничения, например отключить панель управления и заблокировать запуск системного реестра, запретить изменение даты и времени, отключить модуль «Установка и удаление программ», сделать невидимыми отдельные диски, защитить от изменений папки и др..

При желании можно попытаться предотвратить посещение ребенком нежелательных сайтов при интернет-серфинге. Правда, возможности тут ограничены блокированием по ключевым словам (задействованы ключевые слова для базовых категорий) и с учетом черного и белого списков, что, впрочем, не мешает ограничить ребенку посещение социальных сетей (например, указав для ресурса *.vkontakte.ru максимальный лимит допустимого времени) и пр. К сожалению, интернет-фильтр работает только с IE, запуск других браузеров необходимо отключить.

Что касается мониторинга компьютерной деятельности, то родители без труда смогут узнать, чем занималось их чадо на компьютере, — в Time Boss ведется журнал учета работы пользователей, в котором фиксируются все имевшие место события, с определенной регулярностью делаются снимки экрана и сохраняется подробная статистика времени работы каждого пользователя.

**KinderGate Родительский Контроль 1.2**
*Разработчик:* Entensys Corporation
*Сайт программы:* www.kindergate.ru
*Работа под управлением:* Windows XP/Vista/7

Программа «KinderGate Родительский Контроль» — инструмент для организации контроля доступа детей в Интернет, рассчитанный на домашних пользователей и образовательные учреждения. Данное решение позволяет блокировать нежелательный контент (поддерживается URL-фильтрация по черным или белым спискам и фильтрация по категориям), вредоносные сайты, а также прокси-серверы и сайты-анонимайзеры, через которые можно было бы обойти подобную блокировку. В целях защиты от взлома юными хакерами предусмотрено обязательное использование пароля для доступа к программе. Решение включает функционал для мониторинга действий ребенка в Сети: отслеживание посещаемых ресурсов при серфинге, мониторинг сообщений в сетевых мессенджерах (поддерживаются протоколы ICQ, Jabber, MSN, Mail.ru, YMSG) и наблюдение за перепиской ребенка в социальных сетях «ВКонтакте», «Одноклассники» и Facebook. Кроме того, предусмотрен инструментарий для запрета загрузки разных видов контента (видео, аудио, изображения и пр.), настройки расписания доступа в Интернет и блокировки контекстной рекламы и баннеров.

В техническом плане использование программы «KinderGate Родительский Контроль» сложностей не вызывает. Предполагается, что домашний компьютер, на который собираются устанавливать это решение, используется преимущественно ребенком; при необходимости работы родителей систему контроля временно отключают путем запуска окна программы (естественно, требуется знание пароля). Для настройки ограничений необходимо сделать простые настройки. Например, для настройки фильтрации сайтов по их содержимому достаточно активировать вкладку «Запрет категорий» и перетащить бегунок на нужный уровень блокирования (рис. 15). Столь же несложно ввести запрет на загрузку определенного типа файлов и конкретных ресурсов, а также настроить режим доступа в Интернет по времени или календарю. Допускается использование и более сложных правил фильтрации — скажем, можно запретить категорию «Веб-почта», но разрешить доступ к ресурсу mail.yandex.ru в качестве исключения. При необходимости можно включить функцию «Безопасный поиск» (позволяет заблокировать запросы сомнительного характера в поисковых системах Яндекс, Google и др.) и режим морфологического анализа ресурсов (обеспечивает блокирование веб-страниц с запрещенными словами), а также настроить запись мгновенных сообщений. Вся деятельность ребенка в Интернете фиксируется в логах и отображается в виде отчетов (посещаемые ресурсы, трафик, заблокированные сайты).

## Заключение

Не стоит думать, что Интернет – это безопасное место, в котором ваши дети могут чувствовать себя защищенными. Надеюсь, что вы понимаете, что использование только средств воспитательной работы без организации действенного контроля – это практически бесполезное занятие. Точно так же как и использование репрессивных средств контроля без организации воспитательной работы. Только в единстве данных средств вы сможете помочь вашим детям чувствовать себя в безопасности и оградить их от влияния злоумышленников.

Как известно, всё (включая использование компьютера) хорошо в меру, и если ваш ненаглядный отпрыск часами повышает свой уровень в любимой игрушке или сидит в чате, то следует принимать решительные меры. Какие? Это зависит от конкретной ситуации, однако очевидно, что нужно приложить все возможные усилия, чтобы заинтересовать ребенка другими видами деятельности в целях обеспечения его гармоничного развития. Параллельно, поскольку находиться с собственным чадом всё время рядом невозможно, а обещаниям «поиграть ровно полчасика и выключить компьютер» на практике оказывается грош цена, имеет смысл наложить определенные ограничения на компьютерную деятельность с помощью специального инструментария.

Однако даже после настройки компьютерных ограничений «на всё и вся» не стоит обольщаться — наложение запретов лишь активизирует многих юных компьютерщиков на поиски путей их обхода. Таких путей при желании можно найти немало — начиная от банальной смены даты и создания новых пользователей в Windows и заканчивая более продвинутыми вариантами обхода: работой через прокси, использованием анонимайзеров для подмены адресов посещаемых ресурсов и т.д. Большинство подобных вариантов обхода может быть предусмотрительно заблокировано соответствующими системными запретами или настройками родительского контроля.

**При составлении использованы материалы сайтов:**


1. http://compress.ru/article.aspx?id=23035
2. http://nicekit.ru/parental-control/time-boss.php
3. http://vladbez.spaces.live.com
4. http://windows.microsoft.com/ru-ru/windows/set-parental-controls#1TC=windows-7
5. http://www.kaspersky.ru/multi-device-security
6. www.icensor.ru
7. www.kindergate.ru