«УТВЕРЖДЕНО»:
Приказом № 248/1 о/д от «_30_» _11 _2016 года
Директор МБОУ многопрофильный лицей
Беляева Надежда Юрьевна Подписано цифровой подписью: Беляева Надежда Юрьевна Дата: 2021.04.15 08:30:28 +03'00' Н.Ю. Беляева

ИНСТРУКЦИЯ

ПО БЕЗОПАСНОСТИ РАБОТЫ В СЕТИ ИНТЕРНЕТ

КИРОВО-ЧЕПЕЦК

1.1. На любом компьютере, подключенном к Интернету или к локальной сети:

1.1.1. могут запускаться посторонние программы (например, при отображении web-страниц, содержащих ActiveX или Java-апплеты), которые могут выполнять практически бесконтрольно любые действия, в том числе и деструктивные;

1.1.2. другие компьютеры в Сети могут получить (или попытаться получить) доступ к дискам и файлам локального компьютера;

1.1.3. может размещаться информация (например, файлы Cookie), используя которую, можно получить сведения о пользователе, его предпочтениях и посещениях различных сетевых ресурсов;

1.1.4. могут размещаться "троянские кони", т. е. программы, которые отсылают важную конфиденциальную информацию (например, пароли доступа в Интернет или номера кредитных карточек) с зараженного компьютера на определенные сетевые адреса. Широко распространенным вариантом вторжения является негласная установка различных программ для удаленного управления компьютером жертвы. Более безобидную разновидность "троянских коней" представляют обычные программы, для которых даже придуман отдельный термин - spyware. В большинстве своем это бесплатные программы со встроенной системой отображения рекламных баннеров, и их "нелегальная" деятельность заключается, в основном, в сборе и отправке на сайт разработчика статистики о предпочтениях пользователя (наиболее часто посещаемых web-узлах, вызвавших интерес баннерах и т.п.);

1.1.5. на компьютер может быть произведена сетевая DOS-атака, что приводит к блокированию компьютера, и, в лучшем случае, к разрыву сетевого соединения и перезагрузке системы.

вместе с запрашиваемой информации в компьютер пользователя загружается и большое количество совершенно ему не нужной информации, например, рекламные баннеры.

1.2. Появление вирусов вызвало к жизни целую индустрию программ-антивирусов, а для защиты информации на локальных компьютерах как от несанкционированного доступа извне, так и от попыток самостоятельной передачи какой-либо информации из компьютера в Сеть, а также для защиты сетевых портов от внешних атак широко применяются программы, называемые персональными брандмауэрами (firewall). Персональные брандмауэры фильтруют весь входящий и исходящий трафик на основе предустановленных или (и) определенных пользователем настроек, тем самым, обеспечивая более или менее надежную защиту всей системы не только во время пребывания в Интернете, но и при работе в локальной сети.

1.3. Необходимые действия по безопасности пребывания в сети Интернет.

1.3.1. Применяйте брандмауэр (сетевой экран) при подключении к Интернет.

В каждом компьютере, подключенном к сети Интернет, есть свои двери. Называются они порты. Они позволяют каждой программе «общаться» друг с другом через сеть, благодаря чему Вы можете скачивать разные файлы, общаться в чатах и ICQ, играть в on-line игры и многое другое. Но как всегда, существуют не только положительные стороны, но и отрицательные. Если посторонний человек, находящийся за многие тысячи километров от Вас сможет подобрать к этой двери ключик, то это обернется различными бедами. А именно: повышенный риск заражения вирусами и шпионскими программами, кража паролей и другой ценной информации, рассылка с Вашего компьютера рекламных писем (спам), причем естественно за Ваш счет будет оплачиваться трафик, удаленный доступ к Вашему компьютеру и многое другое. Избежать этого можно путем установки на компьютер специальной программы, называемой брандмауэр.

Принцип работы таков: любая программа, желающая получить доступ в сеть, отслеживается брандмауэром и при попытке подключения брандмауэр задает Вам вопрос: пускать ее в Интернет или нет. Если Вы уверены в этой программе, то разрешаете доступ, в противном случае запрещаете. Так же брандмауэр следит за всеми портами на Вашем компьютере, блокируя любое подозрительное подключение извне. В свете вышесказанного сделаем вывод, что наличие брандмауэр на компьютере не роскошь, а необходимый атрибут защищенного компьютера. Помимо этого брандмауэры помогают избежать участия вашего компьютера в таких атаках на другие компьютеры без вашего ведома.

Более ранние версии Windows, нежели Windows XP, выпускались без брандмауэра подключения к Интернет. Если на вашем компьютере установлена более ранняя версия Windows, например Windows 95/98/NT/ME/2000, а компьютер подключен к Интернет, необходимо установить

брандмауэр. Наиболее известные в брандмауэры: Outpost, Kaspersky AntiHaker, Norton Firewall, ZoneAlram.

Перед тем, как включать брандмауэр, проверьте, установлен ли у вас пакет обновлений 2 для Windows XP. Это можно сделать, щелкнув правой кнопкой по значку **«Мой компьютер»** на рабочем столе и выбрав пункт **«Свойства»** в появившемся контекстном меню. В случае, если пакет обновлений 2 не установлен, то его необходимо загрузить и установить на ваш компьютер.

1.3.2. Регулярно обновляйте программное обеспечение на вашем компьютере.

Производители программного обеспечения постоянно трудятся над улучшением своих программных продуктов, выпускают новые версии и "заплатки" (patches) к ранним версиям своих программ. Если на Вашем компьютере установлена операционная система Windows, рекомендуем вам периодически обновлять ее, устанавливая свежие "заплатки" ("патчи").

1.3.3. Используйте новейшие антивирусные программы.

Антивирусные программы способствуют защите компьютера от большинства вирусов, червей, троянских программ и другого вредоносного программного кода. На многих новых компьютерах уже установлены антивирусные программы. Вместе с тем для поддержания уровня антивирусных программ необходима подписка на них. Устаревшие антивирусные программы неэффективны. Антивирусные базы таких программ необходимо регулярно обновлять, чтобы обеспечить защиту от вновь появляющихся вирусов и прочих угроз. Если вы не получаете обновления по подписке, ваш компьютер может стать уязвимым для атак злонамеренно созданных программ. Результатом действия таких программ может быть значительное увеличение трафика, уменьшение производительности компьютера, ухудшение качества работы Интернет и т.п.

Мало просто установить антивирусную программу, необходимо правильно настроить ее: необходимо включить проверку на вирусы программ "в реальном времени"; система должна проводить запланированные сканирования жесткого диска; система должна быть настроена на сканирование сообщений электронной почты.

Следует обязательно включать антивирусные программы перед использованием электронной почты или Интернета. Вирусы обычно распространяются по электронной почте и через загружаемые файлы.

Наиболее известные в антивирусные продукты, которым Вы сможете с уверенностью доверить защиту Ваших файлов: DrWeb, Kaspersky Antivirus, Avast, Norton Antivirus

1.3.3. Используйте антишпионские программы.

Особенностью Spyware является его скрытная от глаз пользователя работа. Вы можете замечать, что стартовая страница в браузере постоянно меняется на другую, что с Вашего счета у провайдера деньги уходят слишком быстро, что трафик стал гораздо больше и т.п. но антивирусная программа при сканировании докладывает, что Ваш компьютер чист, как слеза младенца. А вот в чем причина: далеко не все антивирусные программы способны обнаруживать spyware. Для обнаружения и удаления шпионских программ нужно специализированное программное обеспечение, способное с высокой долей вероятности «найти и уничтожить» поселившегося шпиона.

Наиболее известные в антивирусные продукты: AdAware SE и SpyBot Search&Desrtoy. Они обе давно существуют на рынке и зарекомендовали себя как надежное и проверенное временем средство поиска и удаления шпионских программ. Так же как и антивирус их необходимо обновлять не реже раза в месяц, а лучше раз в неделю.

1.3.4. Анализируйте ссылки перед переходом по ним.

Рекомендуется выработать простое правило: анализировать URL ссылок перед переходом по ним. Во всех популярных браузерах (в частности, в Internet Explorer, Opera и Mozilla Firefox) URL ссылки отображается в строке статуса при наведении курсора на ссылку. Даже поверхностный анализ адреса позволяет легко заметить, например, что ссылка ведет за пределы просматриваемого сайта.

Никогда не соглашайтесь с предложениями установить какие-либо компоненты, панели или модули расширения, если вы не уверенны в их безвредности.

Очень часто в процессе просмотра интернет-страниц можно столкнуться с предложением, установить некоторые модули расширения, компоненты и/или панели инструментов. Следует остерегаться таких предложений, поскольку подавляющее большинство из них является AdWare-приложениями или шпионскими программами. Наиболее агрессивно подобные приложения рекламируются на всевозможных сайтах, содержащих утилиты для взлома программ или генераторы

серийных номеров к программам. Страницы таких сайтов могут содержать скрипты, производящие многократные попытки установки подобных компонентов.

1.3.5. Никогда не переходите по ссылкам из спамерских писем.

Со спамом (нежелательной рассылкой рекламной информации) рано или поздно сталкивается любой пользователь Интернета. Следует учитывать, что ссылки в спамерских письмах могут вести на потенциально опасные сайты и применяться для различных видов атак и обмана (например, фишинга или межсайтового скриптинга). Кроме того, по статистике автора, зачастую при помощи спама производится рассылка ссылок на вредоносные программы.

1.3.6. Никогда не открывайте подозрительные вложения в письмах электронной почты.

В данном случае правило таково: необходимо крайне осторожно относиться ко всей получаемой корреспонденции. Говоря о подозрительных вложениях, следует акцентировать внимание на нескольких распространенных методиках, нацеленных на введение пользователя в заблуждение. Первая методика состоит в том, что исполняемый файл опознается системой не только по расширению, но и по содержимому. Следовательно, если исполняемому файлу изменить расширение *.exe на *.com, то система все равно опознает в нем *.exe по внутреннему заголовку и корректно запустит его. Другой распространенной методикой обмана пользователя является маскировка истинного расширения файла. Еще один метод — это рассылка вредоносных программ в архиве. В данном случае запуск вложения непосредственно из почтового клиента невозможен — нужно, как минимум, открыть архив и запустить находящееся там приложение. Как правило, практикуется рассылка архивов, защищенных паролем. Пароль в этом случае указан в тексте письма, нередко в виде картинки. Все эти меры направлены против антивируса, поскольку существенно затрудняют проверку такого вложения. Кроме рассылки архивов создатели вредоносного ПО в последнее время стали применять еще одну уловку — рассылку вредоносных скриптов или файлов справки формата CHM с вложенными скриптами и вредоносными программами.

2. Обеспечение безопасности детей при работе в Интернет.

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.

Следует понимать, что подключаясь к Интернет, ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать.

2.1. Какие угрозы встречаются наиболее часто? Прежде всего:

2.1.1. 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.

2.1.2. 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;

2.1.3. 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;

2.1.4. 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.

2.2. Рекомендаций, с помощью которых посещение Интернет может стать менее опасным для детей:

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

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

2.2.3. 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;

2.2.4. 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.;

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

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

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

2.2.8. 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;

2.2.9. 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.

2.3. 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?

2.3.1. 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 от лжи;

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

2.3.3. 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.

2.3.4. 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;

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

2.3.6. 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.

2.4. 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:

2.4.1. Какие сайты могут посещать ваши дети и что они могут там делать;

2.4.2. Сколько времени дети могут проводить в Интернет;

2.4.3. Что делать, если ваших детей что-то беспокоит при посещении Интернет;

2.4.4. Как защитить личные данные;

2.4.5. Как следить за безопасностью;

2.4.6. Как вести себя вежливо;

2.4.7. 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.

2.5. Научите вашего ребенка использовать службу мгновенных сообщений.

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

2.5.1. Никогда не заполняйте графы, относящиеся к личным данным, ведь просмотреть их может каждый;

2.5.2. Никогда не разговаривайте в Интернет с незнакомыми людьми;

2.5.3. Регулярно проверяйте список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;

2.5.4. Внимательно проверяйте запросы на включение в список новых друзей. Помните, что в Интернете человек может оказаться не тем, за кого он себя выдает;

2.5.5. Не следует использовать систему мгновенных сообщений для распространения слухов или сплетен.

2.6. 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?

2.6.1. Установите правила использования домашнего компьютера.

2.6.2. Постарайтесь найти разумный баланс между нахождением в Интернет и физической нагрузкой вашего ребенка.

2.6.3. Добейтесь того, чтобы компьютер стоял не в детской комнате, а в комнате взрослых.

2.6.4. Посмотрите на себя, не слишком ли много времени вы проводите в Интернет.

3. 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.

3.1. Возраст 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?

3.1.1. В таком возрасте желательно работать в Интернет только в присутствии родителей;

3.1.2. 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;

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

3.1.4. Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM);

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

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

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

3.2. 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 версии 7.0 со встроенным родительским контролем.

Что можно посоветовать в плане безопасности в таком возрасте?

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

3.2.2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;

3.2.3. 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;

3.2.4. 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;

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

3.2.6. Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM);

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

3.2.8. Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса;

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

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

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

3.2.12. Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы. Подробнее о таких фильтрах http://www.microsoft.com/rus/athome/security/email/fightspam.mspx ;

3.2.13. Не разрешайте детям использовать службы мгновенного обмена сообщениями;

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

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

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

3.2.17. 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.

3.3. Возраст 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:

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

3.3.2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;

3.3.3. 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;

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

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

3.3.6. Не забывайте беседовать с детьми об их друзьях в Интернет;

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

3.3.8. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними;

3.3.9. 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;

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

3.3.11. Создайте вашему ребенку ограниченную учетную запись для работы на компьютере;

3.3.12. 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;

3.3.13. Расскажите детям о порнографии в Интернет;

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

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

4. Возраст 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.

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.

Советы по безопасности в этом возрасте:

3.4.1. Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет[1], руководство по общению в Интернет (в том числе в чатах);

3.4.2. Компьютер с подключением к Интернет должен находиться в общей комнате;

3.4.3. 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;

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

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

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

3.4.7. 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;

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

3.4.9. 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;

3.4.10. Расскажите детям о порнографии в Интернет;

3.4.11. 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;

3.4.12. Приучите себя знакомиться с сайтами, которые посещают подростки;

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

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

4. 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 Vista, средства Родительского контроля, встроенные в Kaspersky Internet Security. Рассмотрим их подробнее.

4.1. Родительский контроль в Windows Vista

До выхода Windows Vista средства родительского контроля можно было обеспечить с помощью операционной системы и программного обеспечения сторонних производителей. Однако с выходом новой операционной системы Windows Vista положение коренным образом изменилось. В состав ОС были включены средства Parental Control (Родительский контроль). Это позволит родителям намного проще решать вопросы контроля за поведением своих детей и их безопасностью при работе на компьютере.

Для задания Родительского контроля вам потребуется создать ограниченную учетную запись, под которой ваш ребенок будет работать за компьютером. Кроме того, не забудьте установить устойчивый (строгий) пароль на вашу учетную запись Администратора (рис. 1).

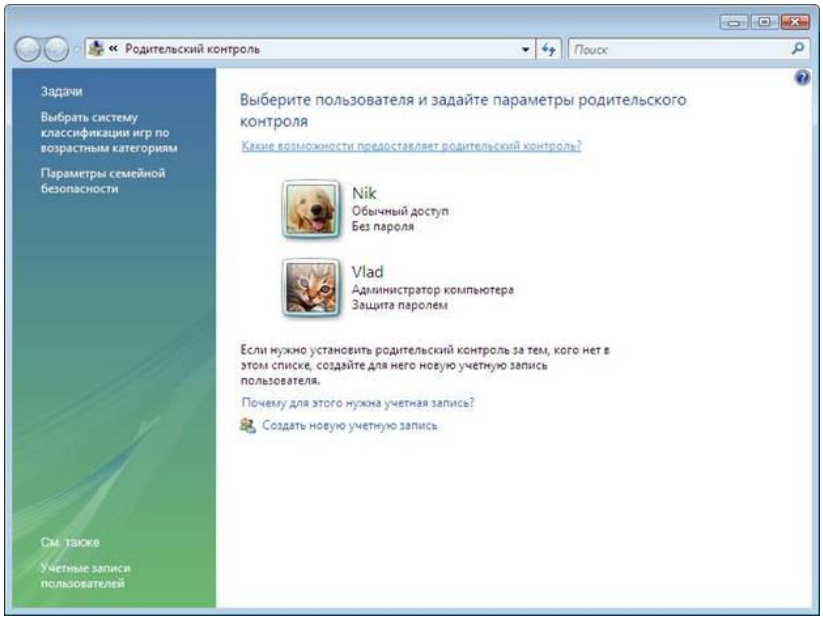

Рисунок 1 - Родительский контроль

Рассмотрим функции, решаемые с помощью родительского контроля (рис. 2):

- **Ограничение времени, проводимого ребенком за компьютером.** Можно определить время, в течение которого детям разрешен вход в систему. В частности, определить дни недели и разрешенные часы доступа в соответствующий день недели. Это не позволит детям входить в систему в течение определенного периода времени. Если в момент окончания разрешенного периода времени ребенок работает за компьютером, происходит автоматический выход из системы.
- **Установка запрета на доступ детей к отдельным играм.** Запрет можно устанавливать исходя из допустимой возрастной оценки, выбора типа содержимого или запрещая доступ к определенным играм.
- **Ограничение активности детей в Интернете.** Ограничить детей можно с помощью установки круга допустимых веб-узлов, исходя из возрастной оценки, запрета или разрешения загрузки файлов, определения условий фильтрования содержимого (т.е. вы должны определить, какое содержимое фильтры должны разрешать или блокировать). Вместе с тем можно разрешить или блокировать доступ к определенным веб-узлам.
- **Установка запретов на использование детьми отдельных программ.** Можно запретить детям доступ к определенным программам.
- **Ведение отчетов о работе ребенка за компьютером.**

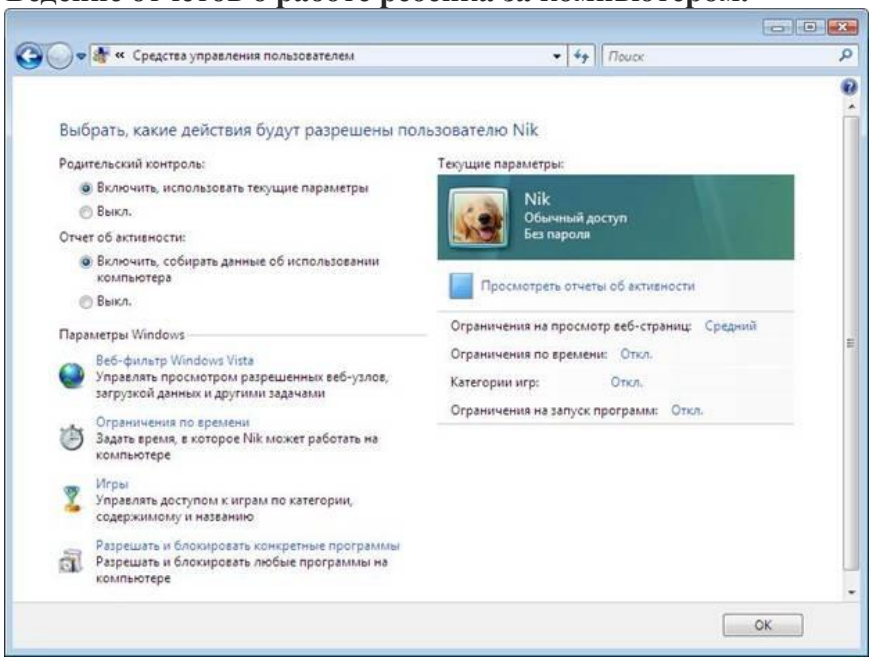

Рисунок 2 - Средства управления пользователем

4.1.1. Ограничение времени использования компьютера.

Разрешенное время доступа можно определить для каждого дня недели и заблокировать при этом доступ в любое другое время (рис.3). Для этого:

- Откройте папку «Родительский контроль».
- При появлении соответствующего запроса введите пароль администратора или подтверждение пароля.
- Выберите учетную запись, для которой вы хотите задать ограничение времени.
- В группе «Родительский контроль» выберите «Вкл».
- Щелкните «Ограничение по времени».
- В появившейся сетке выберите разрешенные часы[2].

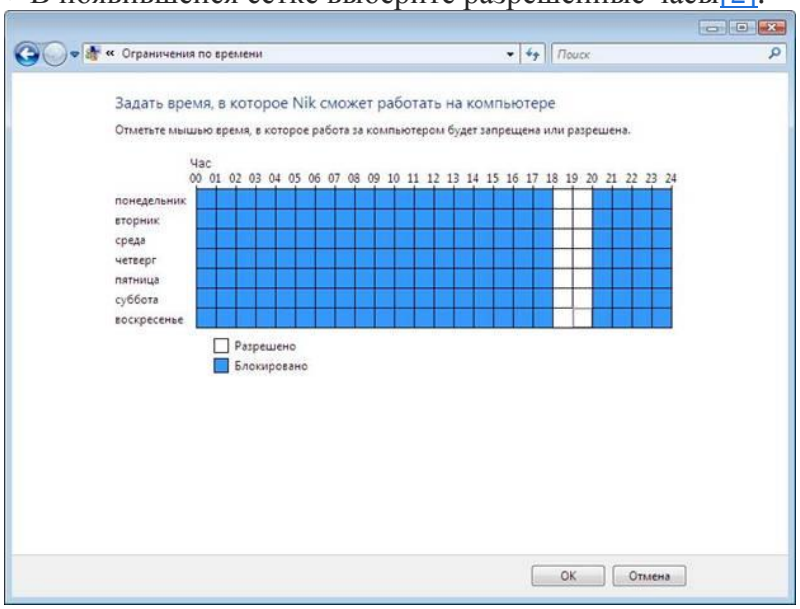

Рисунок 3 - Ограничение времени доступности компьютера для данного пользователя

В данной статье мы не будем подробно рассматривать Установку запрета на доступ детей к отдельным играм и Установку запретов на использование детьми отдельных программ.

4.1.2. Как работает веб-фильтр родительского контроля?

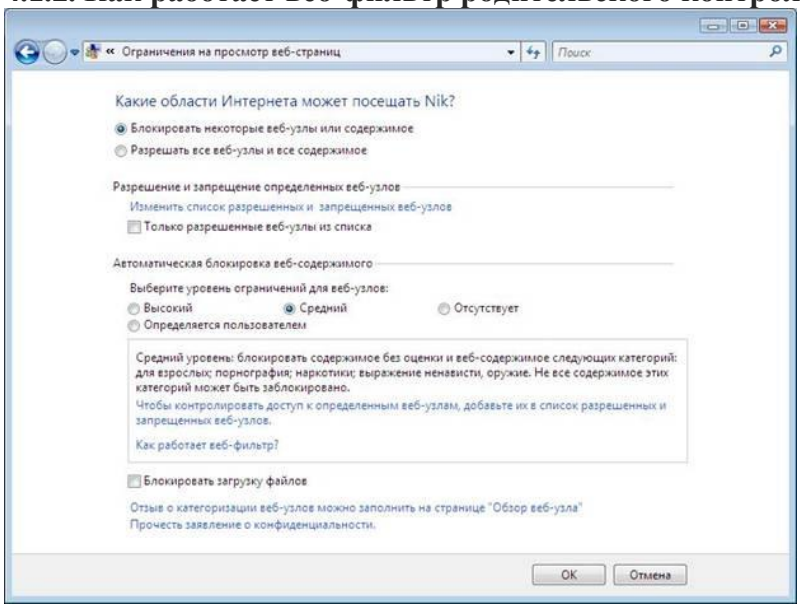

Рисунок 4 - Ограничение на просмотр веб-узлов

Веб-фильтр родительского контроля оценивает содержимое веб-узлов и может блокировать те из них, содержимое которых определено как нежелательное. Включение веб-фильтра позволит значительно уменьшить число нежелательных узлов, которые смогли бы просматривать дети, но, естественно, не гарантирует стопроцентной защиты. Так как нежелательность содержимого является субъективным критерием, следовательно, фильтры смогут блокировать далеко не все содержимое, которое вы считаете нежелательным.

4.1.3. Выбор уровня ограничений для автоматической блокировки содержимого.

Существует четыре уровня ограничений для обозначения содержимого, которое следует блокировать:

– **Высокий**. Веб-узлы для детей с понятным и подходящим для них содержимым. На таких узлах используется стиль изложения, понятный детям от 8 до 12 лет, а его содержимое доступно для детского понимания. Если выбран этот уровень, детям разрешается просматривать веб-узлы для детей, а также другие веб-узлы, внесенные в список разрешенных веб-узлов.

– **Средний**. Производится фильтрация веб-узлов на основании типа содержимого. В этом случае ребенок получит доступ к различной информации в Интернете, за исключением нежелательного содержимого. Чтобы узнать, какие веб-узлы ребенок посещал или пытался открыть, следует просмотреть отчет об активности в Интернете.

– **Низкий**. Содержимое веб-узлов не блокируется.

– **Особый**. Данный уровень также предусматривает блокирование веб-узлов на основании типов содержимого, но позволяет производить фильтрацию по дополнительным критериям.

– Вместе с тем стоит отметить, что можно разрешить или заблокировать отдельные узлы, добавив их в список разрешенных и блокируемых веб-узлов, независимо от выбранного уровня фильтрации.

Выбор типов содержимого для блокировки

Типы содержимого, на основании которых может производиться блокировка веб-узлов.

– **Порнография**. Веб-узел имеет содержимое откровенно сексуального характера, направленное на возбуждение полового влечения.

– **Для взрослых.** Веб-узел содержит информацию откровенно сексуального характера, не носящую медицинский или научный характер.

– **Половое воспитание.** Веб-узел содержит информацию о репродуктивной функции человека и половом развитии, заболеваниях, передающихся половым путем, контрацепции, безопасном сексе, сексуальности или сексуальной ориентации.

– **Агрессивные высказывания.** Веб-узел пропагандирует враждебность или агрессию по отношению к человеку или группе людей на основании принадлежности к определенной расе, религии, полу, национальности, этнического происхождения или иных характеристик; порочит других или оправдывает неравенство на основании вышеперечисленных характеристик либо научным или иным общепринятым методом оправдывает агрессию, враждебность или клевету.

– **Изготовление бомб.** Веб-узел пропагандирует или содержит инструкции по нанесению физического вреда людям или частной собственности при помощи оружия, взрывчатых веществ, розыгрышей или иных видов насилия.

– **Оружие.** Веб-узел продает, освещает или описывает огнестрельное или холодное оружие, а также предметы боевых искусств, либо содержит информацию об их использовании, аксессуарах или модификациях.

– **Наркотики.** Веб-узел рекламирует, предлагает, продает, поставляет, поощряет или иными способами пропагандирует незаконное использование, выращивание, производство или распространение наркотиков, медицинских препаратов, химических веществ и растений, вызывающих наркотическое опьянение, или атрибутов, связанных с употреблением наркотиков.

– **Алкоголь**. Веб-узел рекламирует или содержит предложения о продаже алкогольных напитков или средств для их производства, содержит рецепты или информацию о сопутствующих принадлежностях либо пропагандирует употребление и опьянение алкоголем.

– **Табак**. Веб-узел содержит рекламу, предложения о продаже или иными способами пропагандирует табакокурение.

– **Азартные игры.** Веб-узел позволяет пользователям делать ставки и играть на тотализаторах (в том числе лотереи) в Интернете, получать информацию, содействие или рекомендации по заключению пари, а также дает инструкции, оказывает содействие или обучает азартным играм.

– **Содержимое без оценки.** Содержимое, которое не оценивается веб-фильтром.

4.1.4. Ограничение доступа детей к некоторым типам содержимого в Интернете.

При помощи родительского контроля можно разрешить или запретить доступ детей к отдельным веб-узлам. Также можно заблокировать некоторые веб-узлы на основании их содержимого.

4.1.5. Разрешение или запрещение доступа к отдельным веб-узлам.

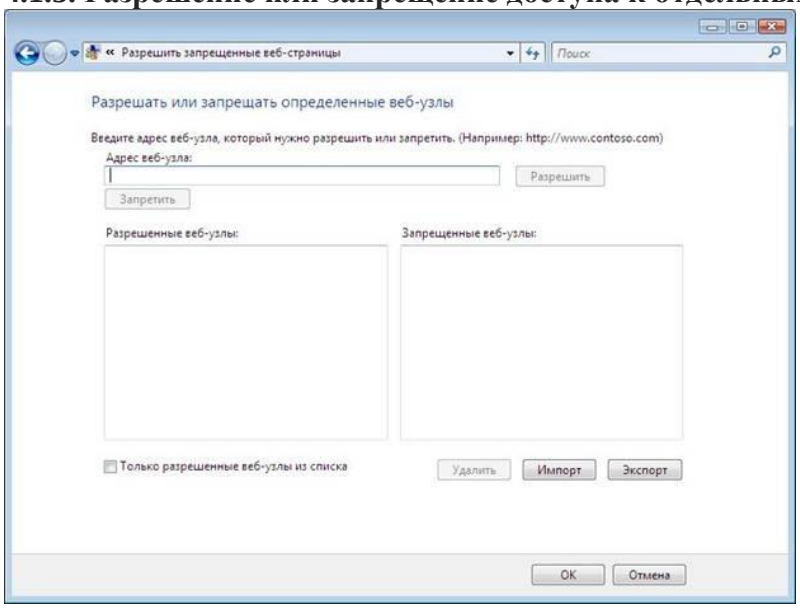

Рисунок 5 - Разрешать или запрещать определенные веб-узлы

1. Откройте «Родительский контроль».
2. Введите пароль администратора или подтверждение пароля, если появится соответствующий запрос.
3. Щелкните имя пользователя, которому нужно установить веб-фильтр.
4. В группе Родительский контроль выберите Вкл.
5. Щелкните Веб-фильтр Windows Vista.
6. Щелкните Блокировать некоторые веб-узлы или содержимое.
7. Щелкните Изменить список разрешенных и запрещенных веб-узлов.
8. В поле Адрес веб-узла введите адрес веб-узла, доступ к которому требуется разрешить или запретить, и нажмите кнопку Разрешить или Блокировка .

4.1.6. Автоматическая блокировка некоторых типов содержимого в Интернете.

Включение веб-фильтра должно значительно уменьшить число нежелательных веб-узлов, которые смогли бы просматривать дети. Однако нежелательность содержимого является субъективным критерием, и фильтр может блокировать не все содержимое, которое вы считаете нежелательным. Также в связи с постоянным появлением новых веб-узлов фильтру требуется время на анализ и оценку их содержимого.

1. Откройте «Родительский контроль».
2. Введите пароль администратора или подтверждение пароля, если появится соответствующий запрос.
3. Щелкните имя пользователя, которому нужно установить веб-фильтр.
4. В группе Родительский контроль выберите Вкл.
5. Щелкните Веб-фильтр Windows Vista .
6. Щелкните Блокировать некоторые веб-узлы или содержимое.
7. В группе Автоматическая блокировка веб-содержимого выберите необходимый уровень содержимого.

Примечание

Можно запретить загрузки, установив флажок *Блокировать загрузку файлов*.

4.2. Родительский контроль в Kaspersky Internet Security 7.0.

Следует отметить, что в случае использования Windows XP единственным действенным средством использования родительского контроля остаются средства сторонних производителей.

Вместе с тем нельзя не признать того, что некоторые параметры родительского контроля в KIS 7.0 могут помочь и в случае использования Windows Vista.

4.2.1. Для настройки Родительского контроля в KIS 7.0 вам необходимо на главной странице приложения выбрать Родительский контроль (рис. 6).

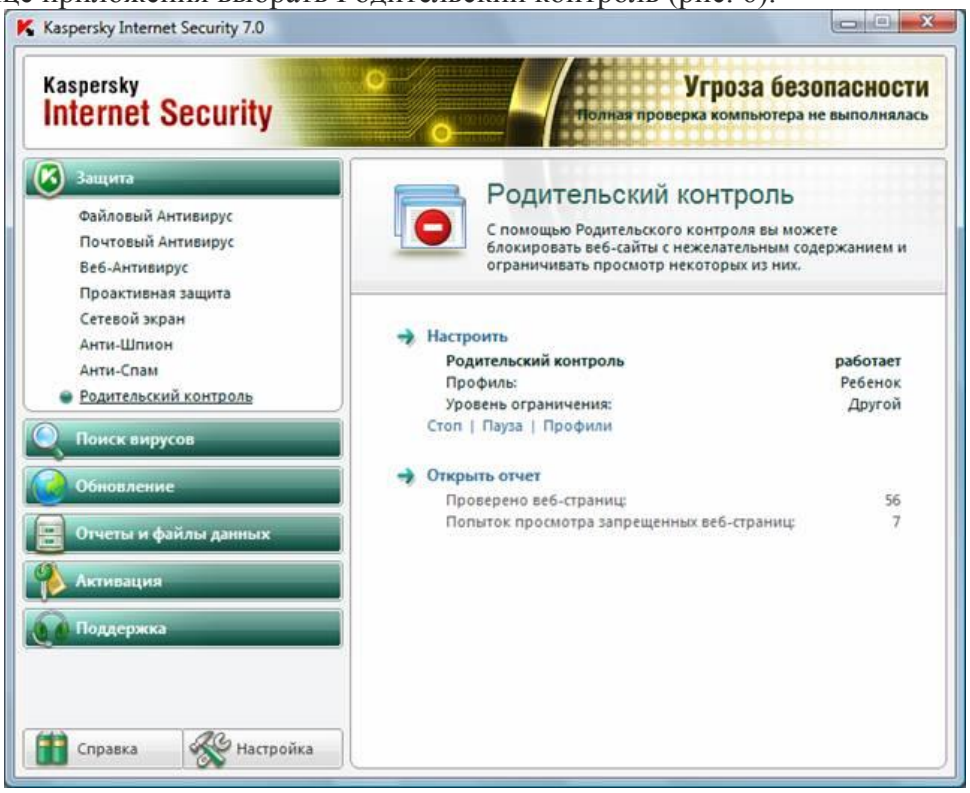

Рисунок 6 - Настройка Родительского контроля в KIS 7.0

Далее необходимо настроить соответствующий профиль как для родителей так и для ребенка (рис. 6). Следует учесть, что по умолчанию Родительский контроль выключен.

После включения всем учетным записям компьютера будет присвоен профиль «Ребенок».

Профиль – это набор правил, регламентирующих доступ пользователя к определенным интернет-ресурсам. По умолчанию созданы три предустановленных профиля:

- **Ребенок (данный профиль используется по умолчанию).**
- **Подросток.**
- **Родитель.**

Для каждого из предустановленных профилей разработан оптимальный набор правил с учетом возраста, опыта и других характеристик каждой группы. Так, например, профиль **Ребенок** обладает максимальным набором ограничений, а в профиле **Родитель** ограничений нет. Удалять предустановленные профили нельзя, но вы можете изменять параметры профилей **Ребенок** и **Подросток** по своему усмотрению.

После установки приложения профиль **Ребенок** является профилем, который используется по умолчанию для всех пользователей, с учетной записью которых не связан ни один профиль.

Для того чтобы использовать предустановленные профили **Подросток** и **Родитель,** установите флажок **Использовать профиль** в окне **Настройка профилей**. В результате выбранные профили будут отображены в раскрывающемся списке блока **Профили** в окне настройки компонента **Родительский контроль.**

В блоке **Пароль** вы можете задать пароль, ограничивающий доступ пользователей к веб-ресурсам под данным профилем. Дальнейшее переключение пользователей на данный профиль будет возможно только после указания заданного пароля. Если поле **Пароль** оставлено пустым, на этот профиль сможет переключиться каждый пользователь компьютера. Для профиля **Ребенок** пароль не задается.

В блоке **Пользователи** вы можете прикрепить определенную учетную запись Microsoft Windows к выбранному профилю Родительского контроля.

Для того чтобы выбрать учетную запись, которую вы планируете связать с профилем, нажмите на кнопку **Добавить** и в стандартном окне Microsoft Windows укажите необходимую учетную запись.

Для того чтобы настраиваемый профиль не применялся к учетной записи пользователя, выберите этого пользователя в списке и нажмите на кнопку **Удалить**.

Чтобы отредактировать настройки параметров профиля:

– **Откройте окно настройки приложения и выберите компонент Родительский контроль в разделе Защита.**

– **Выберите предустановленный профиль, параметры которого вы хотите изменить, из раскрывающегося** списка в блоке **Профили** и нажмите на кнопку **Настройка**.

4.2.2. Настройка фильтрации.

Ограничения, применяемые к профилям Родительского контроля, основаны на применении фильтров. *Фильтр* – это ряд критериев, по которым Родительский контроль принимает решение о возможности загрузки того или иного веб-сайта.

Чтобы изменить параметры фильтрации для текущего уровня ограничений:

1. Откройте окно настройки приложения и выберите компонент **Родительский контроль** в разделе **Защита**.
2. Выберите профиль из раскрывающегося списка в блоке **Профили** и нажмите на кнопку **Настройка** в блоке **Уровень ограничения**.
3. Отредактируйте параметры фильтрации на соответствующих закладках окна **Настройка профиля: <название профиля>**.

4.2.3. Ограничение времени доступа к интернет-ресурсам.

В дополнение к средствам Родительского контроля, созданным в Windows Vista, KIS 7.0 позволяет установить ограничение времени доступа к Интернет (рис. 7).

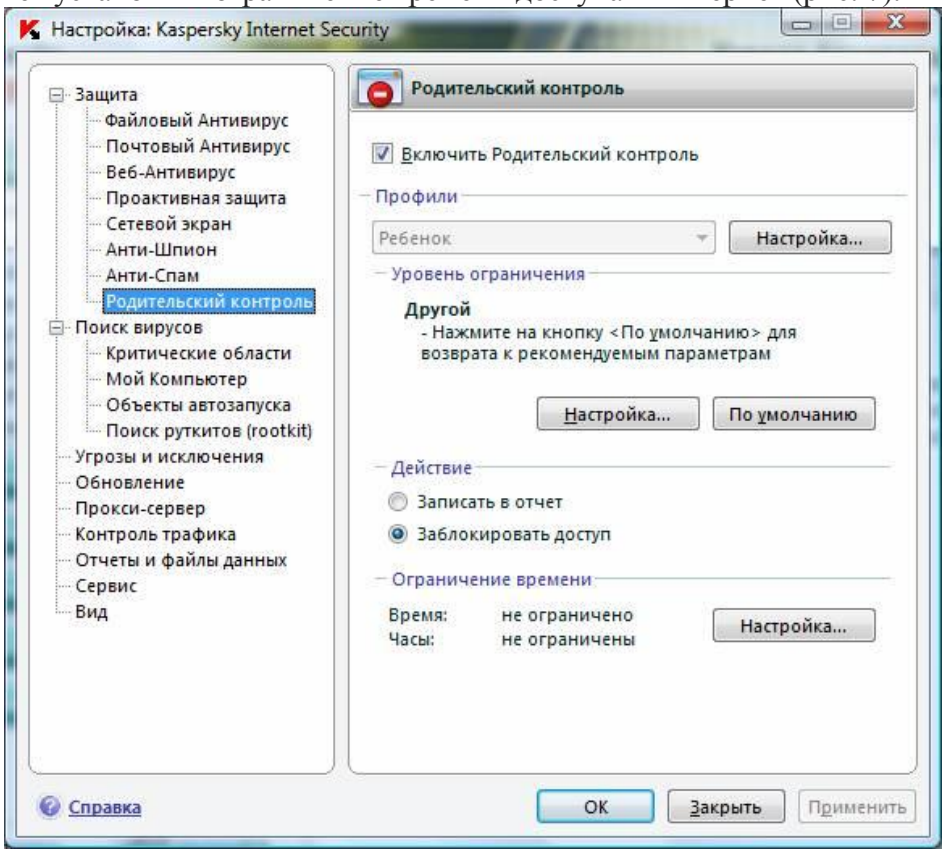

Рисунок 7 - Настройка Родительского контроля

Чтобы установить ограничение на работу в интернете по суммарному количеству времени в течение суток, установите флажок **Ограничить суточное время работы в интернете** и задайте условие ограничения.

Чтобы ограничить доступ к интернету определенными часами в течение суток, установите флажок **Разрешить доступ к интернету в указанное время** и задайте временные интервалы, когда работа в интернете разрешена. Для этого воспользуйтесь кнопкой **Добавить** и в открывшемся окне укажите временные рамки. Для редактирования списка разрешенных интервалов работы используйте соответствующие кнопки (рис. 8).

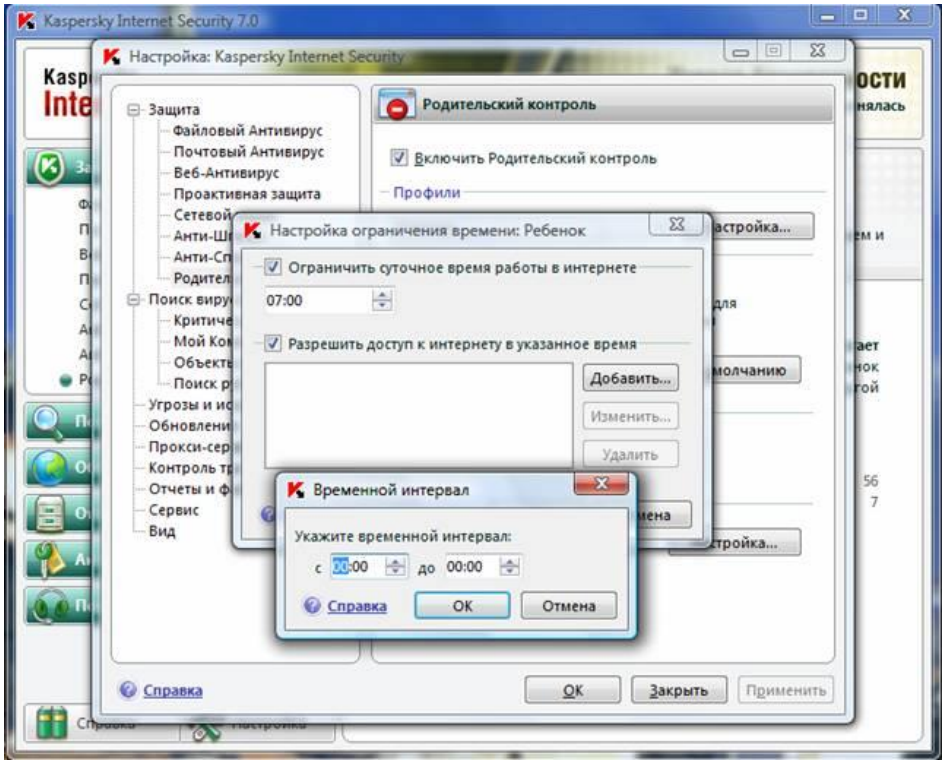

Рисунок 8 - Настройка временного интервала доступа в Интернет

Если вы задали оба временных ограничения, причем значение одного из них превышает другое по количеству отведенного времени, то будет выбрано наименьшее значение из заданных.

Пример: для профиля Ребенок вы ограничили суммарное суточное время работы в интернете тремя часами и дополнительно разрешили доступ в интернет только с 14:00 до 15:00. В итоге доступ к веб-сайтам будет разрешен только в течение этого временного интервала, несмотря на общее разрешенное количество часов. Вы можете задавать несколько временных интервалов в рамках одних суток.

Таким образом, вы сможете указать временной интервал в то время, когда вы сможете контролировать своего ребенка.

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.

---

[1] Часы работы в Интернет могут быть легко настроены при помощи средств Родительского контроля Kaspersky Internet Security 7.0

[2] Вместе с тем необходимо понимать, что ребенок, который знает как в BIOS переустановить дату и время компьютера, может с легкостью обойти это ограничение. Так что необходимо дополнительно установить пароль на BIOS.

Ссылка: http://www.oszone.net/6213/