

Основные правила для школьников младших классов

Вы должны это знать:

- Всегда спрашивайте родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.
- Прежде чем начать дружить с кем-то в Интернете, спросите у родителей как безопасно общаться.
- Никогда не рассказывайте о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья.
- Не отправляйте фотографии людям, которых вы не знаете. Не надо чтобы незнакомые люди видели фотографии Вас, Ваших друзей или Вашей семьи.
- Не встречайтесь без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.
- Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.
- Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

Основные правила для школьников средних классов

Вы должны это знать:

- При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.
- Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
- Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.
- Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
- Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом
- Если вас кто-то расстроил или обидел, расскажите все взрослому.

Основные правила для школьников старших классов

Вы должны это знать:

- Не желательно размещать персональную информацию в Интернете. Персональная информация — это номер вашего мобильного телефона, адрес

- электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.
- Если вы публикуете фото или видео в интернете — каждый может посмотреть их.
 - Не отвечайте на Спам (нежелательную электронную почту).
 - Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
 - Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)
 - Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
 - Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!
 - Никогда не поздно рассказать взрослым, если вас кто-то обидел.

Основные правила для родителей

Чтобы помочь своим детям, Вы должны это знать:

- Будьте в курсе того, чем занимаются ваши дети в Интернете. Попросите их научить Вас пользоваться различными приложениями, которыми вы не пользовались ранее.
- Помогите своим детям понять, что они не должны предоставлять никому информацию о себе в Интернете — номер мобильного телефона, домашний адрес, название/номер школы, а также показывать фотографии свои и семьи. Ведь любой человек в Интернете может это увидеть.
- Если Ваш ребенок получает спам (нежелательную электронную почту), напомните ему, чтобы он не верил написанному в письмах и ни в коем случае не отвечал на них.
- Объясните детям, что нельзя открывать файлы, присланные от неизвестных Вам людей. Эти файлы могут содержать вирусы или фото/видео с «агрессивным» содержанием.
- Помогите ребенку понять, что некоторые люди в Интернете могут говорить не правду и быть не теми, за кого себя выдают. Дети никогда не должны встречаться с сетевыми друзьями в реальной жизни самостоятельно без взрослых.
- Постоянно общайтесь со своими детьми. Никогда не поздно рассказать ребенку, как правильно поступать и реагировать на действия других людей в Интернете.
- Научите своих детей как реагировать, в случае, если их кто-то обидел или они получили/натолкнулись на агрессивный контент в Интернете, так же расскажите куда в подобном случае они могут обратиться.
- Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации.

Основные правила для учителей и преподавателей

Чтобы помочь учащимся, Вы должны это знать:

- Подготовьтесь. Изучите технику безопасности в Интернете, чтобы знать виды Интернет — угроз, уметь их распознать и предотвратить. Выясните, какими функциями обладают компьютеры подопечных, а так же какое программное обеспечение на них установлено.

- Прежде чем позволить ребенку работу за компьютером, расскажите ему как можно больше о виртуальном мире, его возможностях и опасностях.
- Не позволяйте детям самостоятельно исследовать Интернет-пространство, они могут столкнуться с агрессивным контентом.
- Выберите интересные ресурсы и предложите детям изучить их вместе.
- Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации контента, спама и антивирусы.

Это важно знать!

- Когда ты регистрируешься на сайтах, не указывай личную информацию (номер мобильного телефона, адрес места жительства и другие данные).
- Используй веб-камеру только при общении с друзьями. Проследи, чтобы посторонние люди не имели возможности видеть ваш разговор. Научись самостоятельно включать и выключать веб-камеру.
- Ты должен знать, что если ты публикуешь фото или видео в интернете — каждый может посмотреть их.
- Не публикуй фотографии, на которых изображены другие люди. Делай это только с их согласия.
- Публикуй только такую информацию, о публикации которой не пожалеешь.
- Нежелательные письма от незнакомых людей называются «Спам». Если ты получил такое письмо, не отвечай на него. Если ты ответишь на подобное письмо, отправитель будет знать, что ты пользуешься своим электронным почтовым ящиком, и будет продолжать посылать тебе спам.
- Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
- Не добавляй незнакомых людей в свой контакт-лист в ICQ.
- Если тебе приходят письма с неприятным или оскорбляющим тебя содержанием, если кто-то ведет себя в твоём отношении неподобающим образом, сообщи об этом взрослым.
- Если человек, с которым ты познакомился в интернете, предлагает тебе встретиться в реальной жизни, то предупреди его, что придешь навстречу со взрослым. Если твой виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к твоей заботе о собственной безопасности.
- Если у тебя возникли вопросы или проблемы при работе в онлайн-среде, обязательно расскажи об этом кому-нибудь, кому ты доверяешь. Твои родители или другие взрослые могут помочь или дать хороший совет о том, что тебе делать. Любую проблему можно решить! Ты можешь обратиться на линию помощи «Дети онлайн» по телефону: 8-800-25-000-15 (по России звонок бесплатный) или по e-mail: helpline@detionline.org. Специалисты посоветуют тебе, как поступить.

Интернет-этикет

- Когда общаешься в онлайн, относись к другим людям так, как ты хотел бы, чтобы относились к тебе. Избегай сквернословия и не говори вещей, которые заставят кого-то плохо себя чувствовать.
- Научись "сетевому этикету", когда находишься в онлайн. Что считается делать и говорить хорошо, а что нет? Например, если ты печатаешь сообщение **ЗАГЛАВНЫМИ БУКВАМИ**, твой собеседник может подумать, что ты кричишь на него.
- Если кто-то говорит что-то грубое или что-то неприятное - не отвечай. Уйди из чата или форума незамедлительно.

«Подозрительные» сайты

- Если веб-сайт выглядит подозрительно или имеет страницу с предупреждением для лиц моложе 18 лет, покинь его немедленно. Некоторые сайты не предназначены для детей.
- Не заходи на неприличные сайты и не делись ссылками на такие сайты. Если ты видишь, что что-то тебя беспокоит, обсуди это с родителями или с кем-то, кому ты доверяешь.
- Знай, как уйти с веб-сайта, если поиск по интернету приведет тебя на неприятный или неприличный веб-сайт. Нажми control-alt-delete, если сайт не позволяет тебе выйти, или выключи монитор компьютера и сообщи об этом взрослым.
- Проверь с родителями, настроен ли твой поисковый механизм так, чтобы он блокировал материалы, предназначенные для взрослых.
- Попроси родителей установить программное обеспечение для фильтрации информации из интернета, которое блокировало бы "неправильные" сайты.
- Попроси родителей помочь тебе найти безопасные и забавные сайты и сделай на них "закладки" для последующего использования.

Будь начеку!

- Если ты видишь или знаешь, что твоего друга запугивают в онлайн, поддержи его и сообщи об этом взрослым. Ведь ты бы захотел, чтобы он сделал то же самое для тебя.
- Не посылай сообщения или изображения, которые могут повредить или огорчить кого-нибудь. Даже если не ты это начал, тебя будут считать участником круга запугивания.
- Всегда будь начеку, если кто-то, особенно незнакомец, хочет поговорить с тобой о взрослых отношениях. Помни, что в сети никогда нельзя быть уверенным в истинной сущности человека и его намерениях. Обращение к ребенку или подростку с сексуальными намерениями всегда является серьезным поводом для беспокойства. Ты должен рассказать об этом взрослому, которому доверяешь, для того чтобы вы могли сообщить о неприятной ситуации в правоохранительные органы.
- Если тебя заманили или привлекали обманом к совершению действий сексуального характера или к передаче сексуальных изображений с тобой, ты обязательно должен рассказать об этом взрослому, которому доверяешь, для того чтобы получить совет или помощь. Ни один взрослый не имеет права требовать подобного от ребенка или подростка – ответственность всегда лежит на взрослом.

Интернет и дети

Без преувеличения интернет - всемирная сеть, в которой чтобы мы ни искали - это обязательно найдется. Однако не стоит забывать, что это система, внутри которой детей могут подстергать опасности.

Безопасность детей при пользовании интернетом

При использовании интернета детьми возможны следующие ситуации, угрожающие как безопасности вашего компьютера, так и личной безопасности ребенка:

- "Попутные" заражения (т.е. вредоносные программы, загружаемые автоматически при просмотре зараженных сайтов).
- Заражение при использовании файлообменных (P2P) сетей, дающих другим пользователям доступ к вашему компьютеру.

- Нежелательная реклама, в том числе всплывающие окна и рекламные программы, которые часто устанавливаются автоматически вместе с бесплатным ПО, загружаемым из интернета.
- Получение ребенком информации сексуального характера (или иной неприемлемой информации).
- Загрузка ребенком из интернета пиратских материалов (например, музыкальных или видеофайлов).
- Ребенка могут обманным путем убедить предоставить личные данные (его собственные или ваши).
- Ребенок может стать жертвой запугивания через интернет.
- Ребенок может стать жертвой домогательств педофила (например, в онлайн-чатах).

Как защитить ребенка при пользовании интернетом?

В интернете ребенок также легко уязвим, как и в реальном мире, и очень важно, чтобы родители знали, как и от чего необходимо защитить его. Чтобы свести к минимуму риск перечисленных выше угроз, вы можете принять следующие меры:

Поговорите со своими детьми о возможных опасностях, с которыми может быть сопряжено их пребывание в интернете.

Постарайтесь включить работу на компьютере в число дел, которыми вы занимаетесь всей семьей.

Поощряйте своих детей обсуждать с вами свой онлайн-опыт, в особенности его тревожные или неприятные аспекты.

Многие решения Internet Security позволяют ограничить доступ с вашего компьютера к информации определенного характера. Кроме того, в состав браузера Internet Explorer входит модуль "Ограничение доступа" (Content Advisor) – Сервис | Свойства обозревателя | Содержание (*Tools / Internet Options / Content*).

Следуйте приведенным в этом разделе советам по защите компьютера от вредоносных программ и хакерских атак и объясните своим детям, почему это важно для их и вашей безопасности.

Сформулируйте правила, указывающие, что вашим детям разрешается делать в интернете, а что нет.

Данные правила должны давать четкие ответы на следующие вопросы (помните, что по мере взросления детей ваши ответы могут и должны меняться):

- Можно ли регистрироваться на сайтах социальных сетей и других веб-сайтах?
- Можно ли делать покупки через интернет?
- Можно ли загружать музыкальные и видеофайлы, а также программы?
- Можно ли использовать программы мгновенного обмена сообщениями? Если ответ "да", объясните детям, что они не должны общаться с незнакомыми им пользователями.
- Можно ли участвовать в онлайн-чатах?

Для безопасности ваших детей в интернете:

Поговорите с ними о возможных опасностях;

Пользуйтесь интернетом вместе;

Поощряйте обсуждение онлайн-опыта;

Сформулируйте правила работы в интернете;

С помощью настроек программного обеспечения ограничивайте доступ ребенка к

определенному контенту;

Не забывайте также следовать всем другим правилам защиты от вредоносных программ и хакерских атак.

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. 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 контенту.** 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;
- **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 от лжи;
- **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**.

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 (<http://search.msn.com/kids/default.aspx?FORM=YCHM>);
- 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 выглядите 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?

- 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 (<http://search.msn.com/kids/default.aspx?FORM=YCHM>);
- 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. Подробнее о таких фильтрах <http://www.microsoft.com/rus/athome/security/email/fightsпам.msp> ;

- 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 слышаны 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 более 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[1], руководство по общению в Интернет (в том числе в чатах);
- Компьютер с подключением к Интернет должен находиться в общей комнате;
- 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 модерлируемых 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.

На сегодняшний день информационная компетентность для выпускника является не привилегией, а необходимостью для успешной социализации. Многообразие источников и видов информации не должна стать препятствием для развития конкретного ученика, а, наоборот, благодатной почвой для развития информационной компетентности.

Эволюция компьютеров и программного обеспечения привела к достаточной простоте их освоения для самых неподготовленных пользователей, в том числе младших школьников и даже дошкольников. Всё большее количество детей получает доступ к компьютеру в раннем возрасте – дома, у друзей, в кружках. Компьютерные технологии качественно изменяют содержание, методы и организационные формы обучения и при определённых условиях могут способствовать раскрытию, сохранению и развитию индивидуальных способностей обучаемых, их личностных качеств; формированию познавательных способностей; стремлению к самосовершенствованию. С помощью компьютера они быстрее усваивают тот или иной материал, вовлекаются в учебный процесс в качестве активных участников. Да и современному учителю все сложнее и сложнее видеть себя в образовательном процессе без помощи компьютера.

Использование компьютерных технологий в учебном процессе отвечает психофизиологическому развитию учащихся, допускает простоту в организации занятий, оказывает заметное влияние на содержание, формы и методы обучения. Применение мультимедийных презентаций позволяет сделать уроки более интересными, включает в процесс восприятия не только зрение, но и слух, эмоции, воображение, помогает детям глубже погрузиться в изучаемый материал, сделать процесс обучения менее утомительным, позволяет повысить эффективность и мотивацию обучения. А ведь в настоящее время учителя сталкиваются с проблемой снижения уровня познавательной активности учащихся на уроке, нежеланием работать самостоятельно, да и просто учиться.

Благодаря использованию мультимедийных технологий в обучении:

1. Увеличивается активность учащихся на уроке.
2. Появляется возможность оперативного тестирования учащихся.
3. Экономится время и предоставляется возможность решения большего числа задач.
4. При проведении урока с использованием мультимедийных технологий соблюдается основной принцип дидактики – наглядность, что обеспечивает оптимальное усвоение материала школьниками, повышает эмоциональное восприятие, развивает пространственное воображение и все виды мышления у детей.

С другой стороны, стремительное развитие компьютерных технологий качественно меняет окружающую жизнь и порождает множество новых проблем, в частности, **проблему формирования информационной культуры и безопасности среди подрастающего поколения.**

Существуют различные мнения о том, когда нужно давать детям доступ в Интернет. Зарубежные специалисты сходятся в том, что запрет на Интернет может быть действенным

только до тех пор, пока это не ограничивает потребности ребенка в сфере образования. Современные школы уже подключены к Интернет, и преподавание информатики начинается со второго класса. Компьютер и Интернет, как всякие сложные технологические продукты, наряду с неоспоримыми преимуществами могут нанести серьезный вред ребенку. Одним из главных вопросов, связанных с компьютеризацией, является изучение **влияния ЭВМ на организм, психическое состояние и развитие ребенка**. При современном уровне развития техники вредными для детей и, вообще, пользователей любых возрастов, являются скорее не излучения, а **умственное и нервное переутомление**.

Вот выдержка из аннотации к книге Заряны и Нины Некрасовых "Как оттащить ребенка от компьютера и что с ним делать", вышедшей в издательстве "София": «Дети и подростки прирастают к розетке тогда, когда реальный мир не может предложить им других полноценных занятий. Не надо бороться с компьютером, борьба не укрепляет семьи. Надо просто понять истинные потребности своих детей – и найти в себе силы и время общаться, играть, слушать их. Просто посмотреть на все (в том числе и на компьютеры, ТВ, мобильник, плеер и прочие розеточные изобретения) глазами детей и подростков. И тогда виртуальный мир станет помощником вашей семье, для чего он, собственно, и предназначен».

Взрослым важно помнить, что даже самые искушенные дети не видят опасностей Интернета и не осознают рисков его использования. Проблема заключается в том, что у детей еще не сформированы критерии различия. Ребенку, в силу особенностей его психологического развития, интересно все. Оставить ребенка один на один с компьютером в Интернете, это все равно, что бросить его одного на улице большого и незнакомого города. Когда ребенок часами сидит один за компьютером, происходит почти то же самое – скорее всего, он слоняется по виртуальным улицам и подворотням. Поэтому родители и педагоги сначала сами должны научиться азам компьютерной безопасности, а потом научить этому своих детей. Для этого нужна хорошо продуманная **методика обучения основам информационной безопасности**.

Исходя из выше сказанного, можно сделать вывод: работу по ограничению вредного воздействия компьютера на ребенка можно разделить на две составляющие:

1. соблюдение санитарно – гигиенических норм (временной режим работы за компьютером, своевременные перерывы, гимнастика) **для сохранения здоровья детей;**
2. **обеспечение информационной безопасности.**

Выполнение этих условий необходимо выполнить не только школой, но и родителями дома.

I этап

Организация режима работы на компьютере:

- разработка и утверждение режима работы кабинетов с компьютерами (**Приложение 1**);
- проведение инструктажей по охране труда и технике безопасности в кабинетах с установленными персональными компьютерами (**Приложение 2**);
- оформление уголков безопасности с размещением в них всех инструкций, физических упражнений и упражнений для глаз при работе за компьютером (**Приложение 3**);
- организация и проведение физкультминуток при проведении занятий (**Приложение 4**);
- проведение лектория для родителей учащихся по режиму работы детей за компьютером.

II этап

Организация режима доступа к образовательным ресурсам Интернет:

- проведение инструктажей по доступу к образовательным ресурсам Интернет;
- разработка методического пособия «Интернет – ресурсы для образовательного процесса»;
- установка программ-фильтров на школьные компьютеры;
- проведение лектория для родителей учащихся по режиму доступа детей к образовательным ресурсам;
- памятка родителям «Десять фактов, которые нужно сообщить детям ради безопасности в Интернет».

Существует множество программ, позволяющих ограничить время работы за компьютером, отфильтровать содержимое Интернета, обезопасить маленького пользователя. Они называются программами Родительского контроля. Родительский контроль встроен в Windows Vista. Это дает возможность контролировать использование компьютера ребенка в четырех направлениях:

- a. ограничивать время, которое он проводит за экраном монитора,
- b. блокировать доступ к некоторым сайтам,
- c. блокировать доступ к другим интернет-сервисам,
- d. запрещать запуск некоторых игр и программ.

При среднем уровне защиты, работает фильтр на сайты, посвященные оружию, наркотикам, разного рода непристойностям и содержащим нецензурную лексику.

III этап

Обеспечение информационной безопасности работы в Интернет.

Видеть в современной технике только добро или только зло – это крайности, которых следует избегать. Техника всего лишь инструмент в человеческих руках, предназначенный для достижения тех или иных целей. И как при использовании любого инструмента, работа в Интернет требует определенной техники, а точнее – **культуры безопасности**.

При всей важности технических средств, понятно, что они являются всего лишь частью осуществления **политики информационной безопасности**. Она включает воспитательные и образовательные мероприятия.

В проведении политики информационной безопасности школы принимают участие все заинтересованные в этом лица: педагоги, учащиеся, их родители. Документально политика использования ресурсов сети Интернет зафиксирована в **«Правилах использования сети Интернет в муниципальном общеобразовательном учреждении средняя общеобразовательная школа №13» (Приложение 5)**.

В школе создан **Общественный Совет по вопросам регламентации доступа к информации в Интернете, в состав которого входят представители администрации школы, учителя, учащиеся, родители**. Основная функция Совета – контроль использования учащимися ресурсов сети Интернет. Разработан пакет документов, регламентирующий работу Совета:

1. Положение об Общественном совете школы по вопросам регламентации доступа к информации в Интернете (**Приложение 6**);
2. Инструкция для сотрудников средней общеобразовательной школы №13 и членов Общественного Совета школы о порядке действий при осуществлении контроля за использованием учащимися сети Интернет (**Приложение 7**).

В помощь классным руководителям для проведения классных часов и родительского

лектория разработаны:

1. Памятка учащимся «О чем надо знать при работе в Интернет (**Приложение 8**)
2. Памятка родителям по управлению безопасностью детей в Интернет.

В помощь учителям-предметникам разработаны методические рекомендации:

1. Памятка по оформлению методических материалов для размещения на сайте;
2. Памятка по составлению мультимедийной презентации.

Формирование информационной культуры и безопасности – процесс длительный и сложный, но важный и необходимый. Интернет может быть и всемирной энциклопедией, объединяющей информационные ресурсы во всем мире. Но он может превратиться и в зловещую паутину, губящую людей, если люди будут искать в ней нечистоты и превращать ее во всемирную помойку. Задача взрослых (педагогов, родителей) – формирование разносторонней интеллектуальной личности, высокий нравственный уровень которой будет гарантией ее информационной безопасности.