

Медиаобразование выполняет важную функцию защиты от противоправного и манипулятивного воздействия средств массовой коммуникации, а также способствует предупреждению криминальных.

Итак, Медиабезопасность - обеспечение государством информационной безопасности граждан, защита физического, умственного и нравственного развития, а также человеческого достоинства во всех аудиовизуальных медиа-услугах и электронных СМИ.

Советы родителям

Шаг 1: выбирайте сайты, которые можно посещать вашему ребенку, а какие нельзя (блокируйте доступ к неподходящим сайтам).

Шаг 2: увеличьте уровень защиты и конфиденциальности (создайте отдельные учетные записи для разных пользователей)

Шаг 3: следите за тем, какие сайты посещают ваши дети.

Шаг 4: напоминайте детям, чтобы они не общались в Интернете с незнакомцами.

Пусть Интернет будет Вам и Вашим детям только в радость!

«Постарайтесь шагать рядом с ребёнком по дороге жизни – и ему не нужно будет удирать в виртуальный мир»

Советы родителям.

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

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

□□□□□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.

□

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, 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□

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;

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

□□□□□□•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.□

□□□□□□□□□□ 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.

Возраст 9-12 лет

В данном возрасте дети, как правило, уже слышали 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;
- 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.