Наиболее частые угрозы в сети:

1. Угроза заражения вредоносным Программным обеспечением (ПО). Для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить почту, компакт-диски и прочие сменные носители информации или скачанные из сети Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня стало простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов.
2. Доступ к нежелательному содержимому. Сегодня любой ребенок, выходящий в Интернет, может просматривать любые материалы. К таким материалам относится насилие, наркотики, порнография, страницы с националистической или откровенно фашистской идеологией и многое другое.
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.
4. Интернет-магазины. Несмотря 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.

Реко *и от*

1. Посещаі ощряйте ваших хами и неудачаі
2. Объясні г что – либо бес этого, а поделит
3. Объясні личные данные, ефона, и любую пример, номер ц и, время возвращения домой, место работы отца или матери и т.д.;
4. Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково и в сети Интернет, и в реальной жизни;
5. 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;
6. Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

Домашний контроль работы в сети.

Родителям необходимо постоянно вести разъяснительную работу, т.к. без понимания данной проблемы невозможно ее устранить силами только учителей. Очень часто родители не понимают или недооценивают те угрозы, которым подвергается школьник, находящийся в сети Интернет. Некоторые из них считают, что ненормированное «сидение» в сети лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, тому, как вести себя с незнакомыми людьми, что можно говорить о себе, а что нет, между тем, «выпуская» его в Интернет, не представляют себе, что точно так же нужно обучить его основам безопасности в сети Интернет.

Ребенок абсолютно беззащитен перед потоком информации. Дома необходимо выработать общие правила, которые бы сводились к следующему:

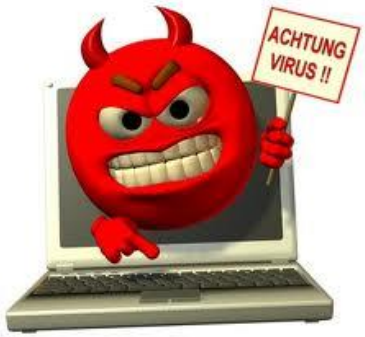
- Какие сайты могут посещать дети и что они могут там делать;
- Сколько времени дети могут проводить в Интернет;
- Как защитить личные данные;
- Как следить за безопасностью;
- Как вести себя вежливо;
- Как пользоваться чатами, группами новостей, службами мгновенных сообщений.

Следите за выполнением данных правил!!! Регулярно, по мере необходимости, вносите изменения в них.

Компьютер в наше время стал для ребенка и другом, и помощником, и даже воспитателем, учителем. Между тем, существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, нарушение психики неустойчивых школьников, представляющих для детей угрозу.

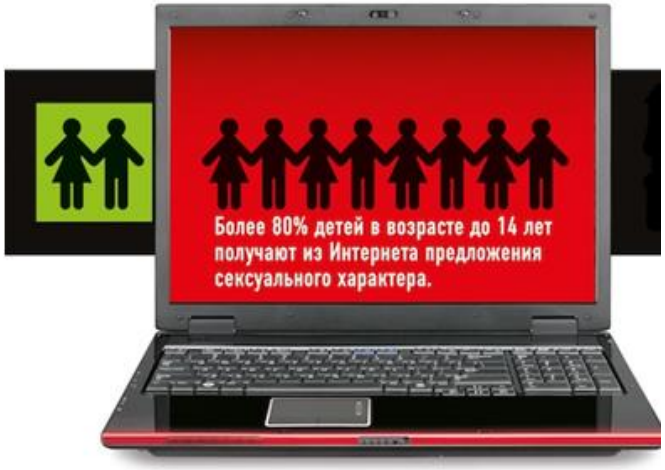
Преодолеть нежелательное воздействие информационной среды можно только совместными усилиями учителей, родителей и самих школьников. Наша задача сегодня – обеспечение безопасности детей, не способных иногда правильно оценить степень угрозы информации, которую они воспринимают или передают.

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



Функции, решаемые с помощью специального ПО:

1. 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.
2. Установка запрета на доступ детей к отдельным играм и программам. Запрет можно устанавливать исходя из допустимой возрастной оценки, выбора типа содержимого или запрета доступа к определенным данным.
3. 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. блокировать). Вместе с тем, можно разрешить или блокировать доступ к определенным веб-узлам.
4. Ведение отчетов и работе ребенка за компьютером.



Правила работы в сети Интернет и мобильных сетях связи для детей и родителей