**Рекомендации для родителей по медиабезопасности**

**Пункт 1:**

Как можно **больше общайтесь** со своим ребенком, чтобы избежать возникновения Интернет-зависимости. Приобщайте ребенка к культуре и спорту, чтобы он не стремился заполнить свободное время компьютерными играми. Запомните! Не существует детей, которых бы не интересовало ничего, кроме компьютера. Помните! «Ребенку для полного и гармоничного развития его личности необходимо расти в семейном окружении, в атмосфере счастья, любви и понимания».

**Пункт 2:**

Существуют определенные механизмы **контроля пользования Интернетом**, например:

* размещать компьютер в общих комнатах, или быть рядом, когда дети пользуются Интернетом;
* совместное с ребенком пользование Интернетом;
* устанавливать специальные системы фильтрации данных,

самостоятельно закрывающие доступ к определенной информации. Критерии фильтрации задает взрослый, что позволяет устанавливать определенное расписание пользования интернетом.

Например, в состав браузера Internet Explorer входит модуль "Ограничение доступа" (Content Advisor) – Сервис | Свойства обозревателя | Содержание (*Tools | Internet Options | Content*).

Также к перечисленным программам по контролю Интернета можно добавить: NetPolice, K9 Web Protection, КиберПапа, функции родительского контроля, которые есть в большинстве антивирусов, детский браузер Гогуль, Чистернет.

**Пункт 3:**

Возможные **Соцсети, в которых могут сидеть Ваши дети** – это Вконтакте, Одноклассники, Facebook, Фотострана, MySpace. Также обратите внимание на ресурс «Мой Мир» на почтовом сайте Мail.

*При общении в Сети у ребенка завязываются виртуальные отношения с новыми «знакомыми» и «друзьями», которые кажутся безобидными, поскольку Интернет-друг является как бы «ненастоящим». Предупредите своего ребенка, что под именем «нового друга» может скрываться мошенник или извращенец. Виртуальное хамство и розыгрыши часто заканчиваются киберпреследованием и киберунижением, доставляя объекту травли множество страданий.*

**Пункт 4:**

Научите детей **не оставлять** в публичном доступе **личную информацию**: контакты, фото, видео. Запомните принцип Интернет: «Все, что вы выложили, может быть использовано против вас». Желательно оставлять только электронные способы связи. Например, специально выделенный для подобного общения е-mail или номер icq.

**Пункт 5:**

**Станьте «другом»** Вашего ребенка в Соцсетях. Это Вам поможет контролировать *виртуальные отношения* ребенка с новыми «знакомыми» и «друзьями». Объясните ему, что Другом должен быть только тот, кто хорошо известен.

**Пункт 6:**

**Контролируйте время**, которое Ваш ребенок проводит в Интернете. Длительное времяпрепровождение в Сети может быть связано с «заигрываниями» со стороны педофилов, особенно в блогах, социальных сетях.

**Пункт 7:**

Несмотря на моральный аспект, периодически **читайте электронную почту ребенка,** если вы видите, что после прочтения почты Ваш ребенок расстроен, растерян, запуган.

**Пункт 8:**

Главное средство защиты от мошенника, педофила – ребенок должен твердо усвоить, что *виртуальные знакомые должны оставаться виртуальными.* То есть – **никаких встреч в реальном мире** с теми друзьями, которых он обрел в Интернете. По крайней мере, без родительского присмотра.

**Пункт 9:**

Средство защиты от хамства и оскорблений в Сети – **игнорирование** пользователя - ни в коем случае **не поддаваться на провокации**. Объясните ребенку, как пользоваться настройками приватности; как блокировать нежелательного «гостя»: добавить пользователя в «черный список», пожаловаться модератору сайта.

**Пункт 10:**

**Избежать неприятного опыта с покупками в Интернет-магазинах** можно, придерживаясь нескольких правил: проверьте «черный список», читайте отзывы в Интернете. Вас должна насторожить слишком низкая цена товара, отсутствие фактического адреса и телефона продавца на сайте, стопроцентная предоплата.

**Пункт 11:**

Для защиты компьютера от вирусов **установите специальные** для этого **программы** и периодически обновляйте их. Объясните ребенку, что нельзя сохранять на компьютере неизвестные файлы, переходить по ссылкам от незнакомцев, запускать неизвестные файлы с расширением \*exe, так как большая вероятность, что эти файлы могут оказаться вирусом или трояном.