Методические рекомендации по организации работы в сети Интернет детей и подростков.

С 1 сентября 2012 года вступил в силу федеральный закон № 436-ФЗ об информационной безопасности детей, который призван защитить подрастающее поколение от медиа-продукции, пропагандирующей наркотические вещества, алкоголь, оправдывающей жестокость и противоправное поведение, отрицающей семейные ценности.

С ростом доступности Интернет-технологий должен повышаться и уровень требований к безопасности информации в сети Интернет. Сегодня каждый понимает, что оградить ребенка от всемирной «паутины» и поставить запрет на определенную информацию возможно не всегда.

В общественных учреждениях: библиотеках, школах, учреждениях культуры и т.д., избежать отрицательного влияния глобальной сети на подростков позволяет установленная система фильтрации. Дома же, зачастую, в отсутствии такого контроля, риски свободного, бесконтрольного пользования детей интернетом возрастают.

Предлагаемые вашему вниманию методические рекомендации помогут снизить уровень воздействия негативной информации на ваших детей, защитить их психическое здоровье и воспитать осознанное использование информационных технологий.

Что такое информационная безопасность ребенка?

Информационная безопасность ребенка - это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. (Статья 2 ФЗ)

Какая информация причиняет вред здоровью и развитию детей?

· побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

· способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

· содержащая информацию порнографического характера

· отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

· обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по

отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
· оправдывающая противоправное поведение; содержащая нецензурную брань.
Интернет - это полезная и интересная вещь, если правильно ею пользоваться, но, чтобы ребенку избежать опасностей, надо знать основные правила работы в Интернет и соблюдать их.

Правила при работе ребенка с компьютером и сетью Интернет:
Разговаривайте с детьми. Вы должны знать, какие сайты они посещают, с кем общаются, что любят смотреть. Не следует разрешать ребенку пользоваться Интернетом свободно, как ему захочется.
Установите правила для использования сети Интернет. Четко определите время, которое ребенок может проводить в Интернете, и сайты, которые он может посещать.
-Научите детей быть осторожными. Расскажите ребенку о возможных опасностях сети Интернет и их возможных последствиях.
- Разработайте “домашнюю” политику. Составьте список того, что можно и чего нельзя делать любому члену вашей семьи при использовании Интернета. Например: Нельзя разглашать информацию личного характера. Объясните детям, что они не должны сообщать свою фамилию, адрес, номер телефона или давать свою фотографию.
Ребенок ни в коем случае не должен соглашаться на личную встречу с “виртуальным” другом без разрешения и присутствия родителей. Нельзя ничего покупать через веб-узел, деятельность которого осуществляется через небезопасный сервер. Перед тем как совершить покупку, необходимо всегда спрашивать разрешения взрослых.

-Ребенок должен знать, что нельзя открывать подозрительные файлы и ссылки, как бы заманчиво они не выглядели. Приучите ребенка спрашивать то, в чем он не уверен.
-Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием. Контролируйте входящие и исходящие сообщения электронной почты своего ребенка. Знакомьтесь с его “виртуальными” друзьями подобно тому, как вы знакомитесь с “реальными”;
-Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений. Интересуйтесь технологическими новинками, например, фильтрующим или другими охранными программами.
-Настройте веб-обозреватель в режиме обеспечения безопасности.
-Ознакомьтесь с содержанием интернет-ресурсов, которыми пользуется Ваш ребенок. Научитесь пользоваться чатами, электронной почтой, ресурсами моментальных сообщений и провайдеров интернет-услуг. Объясните ребенку, что при общении в сети Интернет в чатах, форумах и других

ресурсах, требующих регистрации, нельзя использовать реальное имя. Помогите ему выбрать регистрационное имя (ник), не содержащее информации личного характера, вместо фотографии выберите аватар. Следует либо не допускать использования ребенком чата, либо контролировать это занятие. Кроме того, нужно убедиться в том, что выбранный им чат является управляемыми и поддерживается заслуживающей доверия компанией или организацией;
-Пароли. Предупредите детей о том, что они не должны никому сообщать свои пароли. Поставщик услуг Интернета никогда не будет спрашивать, какой у вас пароль;
-Узнайте об интернет-привычках Вашего ребенка и его друзей.

-Решите, какие программы наиболее подходят для Вашей семьи, и установите их на своем компьютере. Пересматривайте Ваши настройки каждые 6 месяцев, чтобы убедиться, что установленные программы не требуют обновлений.
-Регулярно просматривайте журнал посещений интернет-ресурсов на компьютере, чтобы узнать, какие сайты посещал Ваш ребенок и как часто он это делал.
-Сформируйте список полезных, интересных, безопасных ресурсов, которыми может пользоваться ребенок. Четко объясните детям, посещение каких веб-узлов является приемлемым и какими правилами нужно руководствоваться при пользовании Интернетом. Приведите ясные и наглядные примеры того, что следует искать, и убедитесь в том, что дети обратятся к вам, если столкнутся с не внушающими доверия или смущающими их материалами. Выделите те сайты, которые, по Вашему мнению, Ваш ребенок должен избегать.
-Не отправляйте детей в "свободное плавание" по Интернету. Старайтесь активно участвовать в общении ребенка с Интернетом, особенно на этапе изучения.

-Беседуйте с ребенком о том, что нового для себя он узнает с помощью Интернета и как вовремя предупредить угрозы.
-Установите компьютер в помещении, используемом всеми членами семьи, а не в комнате ребенка. Это упростит контроль за пребыванием детей в Интернете. Воспользуйтесь современными технологиями;
-Следите за тем, чтобы Ваши правила соответствовали возрасту и развитию Вашего ребенка.
Помните!
Эти простые меры, а также доверительные беседы с детьми о том, каких правил им следует придерживаться при использовании Интернета, позволят вам чувствовать себя спокойно, отпуская ребенка в познавательное и безопасное путешествие по Всемирной сети.
Руководствуйтесь рекомендациями педиатров:
·до 7 лет врачи не рекомендуют допускать детей к компьютеру/Интернету;

·7-10 лет время за компьютером рекомендовано ограничить 30 мин. в день;
·10-12 лет до 1 часа за компьютером;
·старше 12 лет - не более 1,5 часов с обязательными перерывами.

Помните, что злоупотребление компьютером рискованно для физического здоровья и может вызвать у ребенка ухудшение зрения, гиподинамию, подверженность аллергиям и даже сердечнососудистые заболевания.

СПОСОБЫ КОНТРОЛЯ РЕБЕНКА В СЕТИ ИНТЕРНЕТ

Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения:

● родительский контроль (Пуск - Панель управления - учетные записи пользователей и семейная безопасность - установить родительский контроль);

Родительский контроль – это название специальных программ, которые позволяют настроить параметры работы определённого пользователя за компьютером. В частности, можно запретить доступ к сайтам определённого содержания, ограничить время работы за компьютером и т.д. Пользоваться этим могут не только родители, но и сотрудники детских учреждений: школ, библиотек, досуговых центров и т.д.

Программное приложение родительского контроля от Лаборатории Касперского.

·программы фильтрации Обзор программ и ссылки на сайты разработчиков посмотреть на сайте Лиги безопасного интернета www.ligainternet.ru;

·журнал просмотренных web-страниц.

·используйте настройки безопасного поиска (установка запрета на открывание сайтов определенной тематики) и защитите их паролем;

·используйте контентные фильтры (установка запрета на определенное содержание) и другие инструменты защиты;

·используйте безопасный режим (не видна запретная информация) в социальных сетях

Информация для родителей:

Если ваши дети пользуются Интернетом, вы, без сомнения, беспокоитесь о том, как уберечь их от неприятностей, которые могут подстерегать их в путешествии по этому океану информации. Хотя значительная часть ресурсов Интернета не может нанести вреда детям, распространение материалов, предназначенных только для взрослых или неприемлемых по какой-либо другой причине, может легко привести к неприятным последствиям. Кроме того, к сожалению, встречаются люди, которые

пытаются с помощью Интернета вступать в контакт с детьми, преследуя опасные для ребенка или противоречащие закону цели.

Возможные опасности, с которыми сопряжен доступ детей к Интернету:

-Неприемлемые материалы. В Интернете ребенок может столкнуться с материалами, связанными с сексом, провоцирующими возникновение ненависти к кому-либо или побуждающими к совершению опасных либо незаконных действий;

-Неприятности, связанные с нарушением законов или финансовыми потерями. У ребенка могут обманным путем узнать номер вашей кредитной карточки, и это вызовет финансовые потери. Ребенка также могут склонить к совершению поступков, нарушающих права других людей, что, в конечном счете, приведет к возникновению у вашей семьи проблем, связанных с нарушением законов;

-Разглашение конфиденциальной информации. Детей и даже подростков могут уговорить сообщить конфиденциальную информацию. Сведения личного характера, такие как имя и фамилия ребенка, его адрес, возраст, пол, и информация о семье могут легко стать известными злоумышленнику. Даже если сведения о вашем ребенке запрашивает заслуживающая доверия организация, вы все равно должны заботиться об обеспечении конфиденциальности этой информации;

-Проблемы технологического характера. По недосмотру ребенка, открывшего непонятное вложение электронной почты или загрузившего с веб-узла небезопасный код, в компьютер может попасть вирус, “червь”, “троянский конь”, “зомби” или другой код, разработанный со злым умыслом.

Меры предосторожности:

Побеседуйте с детьми. Первое, что необходимо сделать, — это объяснить детям, что нахождение в Интернете во многом напоминает пребывание в общественном месте. Многие опасности, подстерегающие пользователя Интернета, очень схожи с риском, возникающим при общении с чужими людьми, и дети должны понимать, что, если они не знают человека, с которым вступили в контакт, лично, это означает, что они общаются с незнакомцем, что запрещено и в реальной, а не только в виртуальной действительности.

ВНИМАНИЕ!

Проверьте с помощью теста «Основы безопасности в Интернете», нет ли пробелов в ваших знаниях о своей личной безопасности в Интернете и о защите своего компьютера от хакеров и вирусов.

Тест (http://www.pushkinlib.spb.ru/opros_internet.html)

«Основы безопасности в Интернете»

Осторожно, вирус!

1. Что является основным каналом распространения компьютерных вирусов?

Веб-страницы

Электронная почта

Флеш-накопители (флешки)

Правильный ответ: электронная почта

2. Для предотвращения заражения компьютера вирусами следует:

Не пользоваться Интернетом

Устанавливать и обновлять антивирусные средства

Не чихать и не кашлять рядом с компьютером

Правильный ответ: устанавливать и обновлять антивирусные средства

3. Если вирус обнаружен, следует:

Удалить его и предотвратить дальнейшее заражение

Установить какую разновидность имеет вирус

Выяснить как он попал на компьютер

Правильный ответ: удалить его и предотвратить дальнейшее заражение.

4. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:

Применение брандмауэра

Обновления операционной системы

Антивирусная программа

Правильный ответ: применение брандмауэра

5. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?

Уничтожение компьютерных вирусов

Создание и распространение компьютерных вирусов и вредоносных программ

Установка программного обеспечения для защиты компьютера

Правильный ответ: создание и распространение компьютерных вирусов и вредоносных программ

Осторожно, Интернет!

1. Какую информацию нельзя разглашать в Интернете?

Свои увлечения

Свой псевдоним

Домашний адрес

Правильный ответ: домашний адрес

2. Чем опасны социальные сети?

Личная информация может быть использована кем угодно в разных целях

При просмотре неопознанных ссылок компьютер может быть взломан

Все вышеперечисленное верно

Правильный ответ: все вышеперечисленное верно

3. Виртуальный собеседник предлагает встретиться, как следует поступить?

Посоветоваться с родителями и ничего не предпринимать без их согласия

Пойти на встречу одному

Пригласить с собой друга
Правильный ответ: посоветоваться с родителями и ничего не предпринимать без их согласия
4. Что в Интернете запрещено законом?
Размещать информацию о себе
Размещать информацию других без их согласия
Копировать файлы для личного использования
Правильный ответ: размещать информацию других без их согласия
5. Действуют ли правила этикета в Интернете?
Интернет - пространство свободное от правил
В особых случаях
Да, как и в реальной жизни
Правильный ответ: да, как и в реальной жизни

Рекомендуем!
-Безопасный интернет (http://i-deti.org/) - электронные ресурсы для детей и родителей по безопасной работе в Интернет.
- На сайте Центра безопасного Интернета есть ряд рекомендаций для разных возрастов о поведении в сети, целые статьи, посвященные самым разным вопросам, к примеру, тому, в чем опасность общения через Интернет http://www.saferunet.ru. Эти рекомендации будут полезны и родителям, которые хотели бы оградить своих детей от преждевременного знакомства с некоторыми особенностями современной сети Интернет.
-Очень многие важные организации волнуются за безопасность детей в Интернете и составляют для них пособия о том, как правильно вести себя в сети. Например, у «Лаборатории Касперского» есть целый сайт (http://www.kaspersky.ru/keeping_children_safe) посвященный советам детям и родителям
-Компания МТС учредила образовательный проект «Дети в Интернете» (http://detionline.com/mts/about) о том, как правильно вести себя в Интернете, узнать, как не попасть в беду в сети и использовать ее возможности с максимальной пользой и удовольствием.
-Дети в Интернете - обзорная статья, угрозы и решения.

-Уроки мобильной грамотности от Билайн - 12 аудиоуроков, посвященных безопасности при использовании мобильных средств связи, подготовленных в виде аудиоспектаклей компанией Билайн совместно с "Детским радио"

-Журнал " Дети в информационном обществе", Дети России Онлайн

P.S. Безопасный интернет - детям!
социальные ролики:
(http://5psy.ru/raznoe/bezopasnost-deteie-v-internete-podborka-materialov.html)

По материалам интернет-изданий.