«Безопасность подростка в сети Интернет и в СМИ»

Современный мир плотно насыщен разного рода технологиями, а так же новыми открытиями в различных сферах жизнедеятельности. Мы являемся непосредственными участниками всего, что нас окружает, и соответственно каким либо образом взаимодействуем, как между собой, так и между предметами и процессами происходящими вокруг нас. Немалый вес имеет и информация, которая все больше и больше заполняет современный мир, а вместе с ним и общество. Мы ее получаем, накапливаем, обмениваемся ей, именно она источник наших знаний, на ее фоне формируются наше мнения на какие либо процессы или события, именно она является одним из важнейших компонентов формирующих современное общество.

В настоящее время большое количество подростков получает возможность работать в сети Интернет. И тут встает проблема обеспечения информационной безопасности наших детей в сети Интернет. Расширение технических возможностей и доступности телекоммуникационных систем, развитие электронных средств связи, их совместимость с Интернетом, многообразие способов общения в режиме онлайн многократно повышают угрозу информационной безопасности детей и подростков.Изначально Интернет развивался вне какого-либо контроля, и на данный момент он предоставляет нам огромное количество информации, причем вся информация «циркулирующая» в сети является положительной, важной и полезной, и далеко не всегда безопасной. Наши дети уже с дошкольного возраста проникают в сеть ИНТЕРНЕТА. Безусловно, немалый поток информации мы получаем из всемирной паутины, и если у взрослого человека, каким-то образом уже выработаны механизмы защитных реакций, то у ребенка они еще только на стадии формирования, а соответственно он наиболее подвержен информационным угрозам. **Этим и обусловлена актуальность выбранной темы.**В связи с этим возникает проблема обеспечения безопасности детей. Помочь им могут только взрослые и родители.

2.Классификация Интернет-угроз.

1) Контентные риски (разнообразные материалы, содержащие вредоносную (опасную), противозаконную и неэтичную информацию);

2) Коммуникационные риски (установление дружеских отношений с ребенком с целью изнасилования. Злоумышленник нередко общается в интернете с ребенком, выдавая себя за ровесника либо ребенка немного старше. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование). Особое внимание хотелось бы уделить такому частому явлению интернета как «троллинг», понятия которого не существует в законодательстве РФ. То, что называют троллингом, юридически может быть квалифицировано как оскорбление. При этом следует различать разные составы — оскорбление, клевета и оценочные суждения, не содержащие признаков этих двух правонарушений. Оскорбление может также перейти в сферу уголовной ответственности, например, при разжигании ненависти по различным социальным признакам (национальность, вероисповедание и другие)

3) Потребительские риски, в частности кибермошенничество (причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.). Помимо этого, с процессом глобализации стало легким и доступным способом приобретение товаров через Интернет-магазины, однако создаются множество сайтов и групп в социальных сетях, предлагающие товары за низкую цену. Нередко такие привлекательные предложения оказываются обманом, в результате которого подросток тратит денежные средств.

4) Электронные риски (различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации).

3. Угроза жизни детей.

Зависимость подрастающего поколения от виртуального пространства — одна из причин беспокойства взрослых за своих детей. Особенно в связи с недавними событиями ухода из жизни подростков посредством «групп смерти». Всемирная организация здравоохранения отмечает, что Интернет-сайты и социальные сети, «несомненно, причастны к провоцированию и содействию суицидальному поведению», поскольку частные лица могут легко распространять через открытые интернет-сайты и социальные сети, не подвергавшиеся цензуре материалы и информацию о самоубийствах.

4.Не упустить ситуацию.

Вот на что следует обратить внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

- Беспокойное поведение

Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

- Неприязнь к Интернету

Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

- Нервозность при получении новых сообщений

Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников.

Что делать, если ребенок все же столкнулся с какими-либо рисками?

Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен Вам доверять и знать, что Вы хотите разобраться в ситуации и помочь ему, а не наказать.

- Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка;
- Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил Ваши или свои деньги в результате интернет-мошенничества и пр.) — постарайтесь его успокоить и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где Вы не рассказали ему о правилах безопасности вИнтернете;
- Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время;

- Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был Ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может Вам пригодиться (например, для обращения в правоохранительные органы);
- Если Вы не уверены в оценке серьезности произошедшего с Вашим ребенком, или ребенок недостаточно откровенен с Вами или вообще не готов идти на контакт, или Вы не знаете как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где Вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС, Сестры и др.)

5. Предупреждение кибермошенничества:

1. Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;
2. Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных;
3. Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если Ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности:

- Ознакомьтесь с отзывами покупателей:
- Проверьте реквизиты и название юридического лица – владельца магазина
- Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs)
- Поинтересуйтесь, выдает ли магазин кассовый чек
- Сравните цены в разных интернет-магазинах.
- Позвоните в справочную магазина
- Обратите внимание на правила интернет-магазина
- Выясните, сколько точно вам придется заплатить

6. Как распознать интернет и игровую зависимость.

Если Вы считаете, что Ваши близкие, в том числе дети, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Помощь может быть оказана как в специальных терапевтических группах, так и стационарно, с использованием специальных медицинских процедур.

7. Как научить ребенка не загружать на компьютер вредоносные программы

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать Ваш компьютер для

распространения вируса, рассылать от Вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

- Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
- Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.
- Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.
- Периодически старайтесь полностью проверять свои домашние компьютеры.
- Делайте резервную копию важных данных.
- Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

8. Как защитить детей от негативной информации?

В связи с развитием новых технологий в области виртуального пространства, в том числе с распространением сети Интернет, возникла проблема, связанная с доступом несовершеннолетних к информации сомнительного содержания и противоречащей общепринятой этике. В настоящее время любой человек, в том числе и несовершеннолетний, владеющий знаниями в области компьютерных технологий, может получить доступ к данным, хранящимся в Интернете, или создать свой собственный веб - ресурс. Отсутствие контроля со стороны родителей за использованием детьми сети Интернет - одна из причин доступности негативной информации несовершеннолетним. Памятка родителям по безопасному использованию детьми сети Интернет. Основные правила, которые помогут оградить Ваших детей от информации сомнительного содержания и противоречащей общепринятой этике.

Правило №1

Родители должны знать интересы и цели детей, которые используют сеть Интернет.

Правило №2

Необходимо исключить доступ детей к ресурсам сети Интернет, содержание которых противоречит законодательству Российской Федерации, может оказать негативное влияние на несовершеннолетних (информацию, пропагандирующую порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение, сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.).

Правило №3

В случае самостоятельного доступа детей к сети Интернет, родители должны контролировать использование информации несовершеннолетними. О характере и объеме информации, полученной детьми в интернет –

ресурсах, необходимо узнавать в «Журнале обозревателя» программы "InternetExplorer" . Как ограничить доступ детей к негативной информации в сети Интернет? С целью ограничения доступа детей к «вредным» материалам родители и другие члены семьи могут установить на компьютеры программу «Касперский Интернет секьюрити 2010»: в настройке программы применить вкладку «Родительский контроль», при этом произойдет блокировка информации, связанной с порнографическими сюжетами, жестокостью, нецензурной лексикой и др., оказывающей негативное влияние на детей и подростков.

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 возраста 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 боле чувствительны к сексуальным домогательствам в Интернет.

- Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, 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 модерируемых 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.

9. Настройка родительского контроля.

Поскольку программ, предлагающих функционал родительского контроля, достаточно много и все они имеют свою документацию, не будем здесь подробно описывать, как активировать родительский контроль. Инструкции разработчиков программных решений очень подробны. Тем не менее, мы дадим ссылки на документацию и краткие характеристики.

1. Сервис SkyDNS

Сервис предлагает комплекс услуг по блокировке нежелательного контента, включая блокировку рекламы. Версия «для дома», стоимостью 360 рублей в год, позволяет блокировать сайты по многим признакам, например, можно заблокировать все социальные сети, черный список минюста, сайты знакомств и т. д. Сервис имеет свою огромную базу адресов с характеристикой контента. Есть настройка «белого» списка, есть «черные» списки.

Главное преимущество сервиса — гибкие и удобные настройки при невысокой цене. Блокирует сайты, содержащие вирусы. Простая на- стройка, не требующая специальных знаний.

Из минусов — сервис ничего не способен ограничивать непосредственно на компьютере, он фильтрует только доступ к Интернет-ресурсам.

Надежность высокая, обойти при правильной настройке — достаточно тяжело.

2. Dr. Web Security Space и Kaspersky Internet Security

Документация Dr.Web
Документация Kaspersky Internet Security
Документация встроена также и в сам продукт.

Прежде всего, это полноценные антивирусные решения, функция родительского контроля реализована «в довесок». Тем не менее, очень популярное решение для домашнего компьютера, выполняющее свои задачи вполне эффективно. Позволяет блокировать не только нежелательные сайты и сайты с вирусами, но и ограничивать использование компьютера по времени, устанавливать запрет на запуск определенных приложений, блокирует доступ к указанным папкам и файлам на компьютере.

Обойти настроенный родительский контроль на этих продуктах очень просто, если не провести дополнительные настройки. Дело в том, что разрешения настраиваются для отдельных пользователей операционной системы. Из чего, кстати, следует, что нужно создать отдельного пользователя операционной системы с ограниченными правами для ребенка.

Что делает более-менее продвинутый подросток? Он загружает компьютер в безопасном режиме, выбирает пользователь «Администратор», который в обычном режиме скрыт и потому не имеет пароля, создает себе временного пользователя с неограниченными правами. Сделать это очень просто и подростки этому учатся моментально. Почему-то в документации на этот момент внимания не обращают. Однако, закрыть такую брешь легко — достаточно активировать скрытого пользователя «администратор» и задать ему пароль. Как это сделать — в конце этого приложения.

Плюсы — гибкая настройка, большие возможности контроля, помимо родительского контроля есть антивирус и файрволл.

Минус — нужны дополнительные настройки операционной системы (создание учетной записи для ребенка, создание пароля для учетной записи «администратор»).

3. Как активировать учетную запись «администратор»?

Нажмите «Пуск», щелкните правой кнопкой на «Компьютер» и откройте пункт «Управление». Нас интересует ветка «Локальные пользователи».

В открывшемся окне дважды щелкните на пользователе «Администратор», в появившемся меню снимите птичку с пункта «Отключить учетную запись» и нажмите «ОК».

На этом все. Учетная запись «Администратора» активирована. Далее необходимо задать пароль для этой учетной записи.

Данная проблема актуальная для операционной системы Windows 7 версий выше Homepremium.

4. Как создавать учетные записи, менять пароли к ним
Пуск — Панель управления — учетные записи пользователей. Тут можно менять пароли и создавать новые учетные записи. Напомним, для работы родительского контроля у ребенка должна быть своя учетная запись Интернет (не администратора!), для которой будут ограничены права.