Родительский всеобуч
«Цифровое воспитание или кибербезопасность ребенка в современном мире»

Цель: сформировать правильное поведение родителей по вопросу кибербезопасности детей.

Задачи:

1. Показать родителям важность и значимость цифрового воспитания детей.
2. Рассказать родителям о правилах общения в сети Интернет.
3. Ознакомить родителей с источниками информации по проблеме безопасности ребенка в сети Интернет.

Использованные источники информации:

- Глобальная сеть: правила пользования. Рекомендации для родителей http://static.mts.ru/uploadmsk/contents/1655/safety/rules_for_parents.pdf
- Безопасность в интернете: портал для учащихся, учителей и родителей http://laste.arvutikaitse.ee/rus/html/etusivu.htm
- Обеспечение безопасности детей при работе в Интернет http://www.oszone.net/6213/#_ftn1

Педагог:

Бежит по клавишам рука
И пальцы высекают слово:
Пока-привет, привет-пока -
Банальностями сыплем снова!
Какая магия влечет,
Сесть к монитору заставляет?
Но все быстрее кровь течет!
И к слову слово прибавляем.
Соединил нас Интернет,
Сквозь расстояния и годы,
Привет-пока, пока-привет…
Ну что? А как у вас погода?
Что нового? И как дела?
В семейной, ну и в жизни личной?
Что видел ты? Где ты была?
Все – класс! И у меня – отлично!

Сегодня мы не представляем свою жизнь без компьютера и сети Интернет. В настоящее время ведется множество неоднозначных разговоров о пользе и вреде всемирной сети. Дети и подростки - активные пользователи интернета, ведь он предоставляет подрастающему поколению невероятные возможности для совершения открытий, общения и творчества. Но у любого явления есть свои светлые и темные стороны, и зачастую дети и молодежь в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети.

Интернет представляет собой открытое окно в мир, который также принадлежит взрослым и содержит материалы, не подходящие для детей, поэтому с использованием киберпространства связаны определенные риски.

Как должны родители и взрослые помочь детям избежать все возможные неприятности, чтобы сделать их пребывание в интернете более безопасным, научить их ориентироваться во всемирной сети? Простого ответа не существует. Риски могут быть разными в зависимости от возраста и компьютерной грамотности ребенка.

Конечно же, отказ от использования этих современных технологий не является решением проблемы защиты детей в онлайн-пространстве. Это все равно что запретить ездить автотранспорту по улицам и придворовым территориям, чтобы дети не попадали в ДТП. Во избежание несчастных случаев нужно лишь научить ребенка быть осторожным,

соблюдать определенные правила, быть ответственным пешеходом, следовать положительному примеру взрослых. Аналогично наиболее важной задачей взрослых является предупреждение детей об опасностях Интернета, чтобы они вели себя осторожно, обдуманно. Кроме того, необходимо обсуждать с детьми все те вопросы, которые могут у них возникнуть при использовании Интернета.

Возможные риски, с которыми могут столкнуться наши дети в интернете.

Итак**, риск первый - это безопасность личной информации на собственном компьютере**, что означает защиту от вирусов, вредоносного ПО и постоянное обновление программного обеспечения. Как защитить в этом случае своих детей? Прежде всего, повысить уровень защиты данных. Это можно сделать путем использования настроек фильтра и параметров фильтрации содержимого, которые доступны во многих программах. Кроме того, велика угроза заражения вредоносным ПО. Ведь для его распространения и проникновения в компьютеры используется целый спектр методов. Среди них 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. Этот метод часто используется хакерами для распространения троянских вирусов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уловки злоумышленника.

Чтобы избежать риска потерять личную информацию на компьютере, нужно соблюдать достаточно простые правила безопасности:

- Регулярно обновляйте операционную систему.
- Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.
- Используйте антивирусную программу, которая постоянно обновляет свои базы, и еженедельно проверяйте компьютер на наличие вирусов.
- Создавайте резервные копии важных файлов, так называемые, "бэк-апы" (например, на отдельном, только для этого и предназначенном винчестере или usb-накопителе).
- Будьте осторожны при загрузке содержимого в Интернет. Помните: после публикации информации во всемирной сети ее больше невозможно будет контролировать и удалять каждую ее копию.
- Будьте внимательны при загрузке контента из Интернета: при малейшем сомнении откажитесь от "закачки" данных на свой компьютер.
- Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п). Никому не сообщайте пароли!
- При пользовании интернетом на чужом устройстве, не сохраняйте пароли и не забывайте выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы.
- Объясните все эти правила своим детям!

Риск второй - разглашение контактных данных.

В Интернете (чатах, социальных сетях и т.п.) дети могут общаться с другими детьми и заводить новых друзей, что подразумевает обмен определенной личной информацией, по которой можно установить личность ребенка, контактную информацию (полное имя, почтовый адрес и номер телефона), подробности его быта, режима дня и и т.д. Личность человека можно также установить, связав различные типы предоставленных данных (например, название школы, спортивного клуба, места проживания и т.д.). Подобная информация может быть использована в преступных целях.

Поэтому, давая положительный пример своим детям, старайтесь сами соблюдать осторожность при разглашении контактных данных или другой личной информации.

Любые отправляемые фотографии или раскрываемые незнакомцу личные сведения могут стать общедоступными в Интернете. Интерактивные дневники могут надолго стать доступными для прочтения широкой общественностью. После публикации в Интернете текста или фотографии их невозможно контролировать. Их можно легко скопировать во множество разных мест, и их полное удаление может оказаться невозможным.

Соблюдайте правила безопасности вместе с детьми, обсуждая их необходимость:

- Обговорите с детьми возможные опасные последствия предоставления личной информации и те ситуации, когда рекомендуется скрывать личную информацию (с учетом возраста и психологической уравновешенности каждого ребенка).
- Помните: никогда не следует сообщать пароли никому, даже давним друзьям. Кроме того, пароль необходимо регулярно менять. Научите этому своих детей.
- Интернет является общественным местом. Перед публикацией любой информации или своих фотографий (а также фотографий других людей) следует помнить, что любой человек в мире сможет получить доступ к этой информации.
- Ребенок должен знать, что в любой момент может поговорить с родителями об отрицательном опыте, полученном в Интернете, понимая, что получит поддержку и помощь от взрослых, а не порицание и наказание.

Риск третий - это доступ к нежелательному содержимому.

Это может быть насилие, наркотики, порнография, страницы, подталкивающие к самоубийствам, отказу 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.

Такая информация часто бывает заманчивой и может оказывать сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с подобным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков непредсказуемо; под впечатлением от таких сайтов дети могут пострадать не только в эмоциональном плане, но также прямой урон может быть нанесен и их физическому здоровью.

Уберечь детей от данной нежелательной информации поможет настройка контентной фильтрации с помощью дополнительных функций антивирусных программ, интернет-браузеров или установки специального программного обеспечения, например, Родительского контроля в WindowsVista или средств Родительского контроля, встроенных в KasperskyInternetSecurity.

Если компьютером пользуются и взрослые, то для ребенка лучше создать отдельную учетную запись пользователя, в которой настраивается фильтрация и родительский контроль. При этом вы будете выполнять функции администратора (отдельная учетная запись): вы сможете контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера. Не забывайте создавать для работы надежные и защищенные пароли.

Нежелательную информацию можно получить и по электронной почте, поэтому важно настроить почтовый ящик ребенка с помощью фильтрации спама и таким образом предотвратить получение большей части нежелательных сообщений. Еще один безопасный, хотя и очень ограниченный способ использования электронной почты — это настроить параметры так, чтобы ребенок получал сообщения только от указанных адресов. Многие программы электронной почты позволяют блокировать сообщения, отправляемые с определенных адресов электронной почты.

Риск четвертый - контакты с незнакомыми людьми.С подобными рисками можно столкнуться при общении в чатах, онлайн-мессенджерах (ICQ, Skype, MSN и др.),

социальных сетях, на сайтах знакомств, форумах, блогах и т.д. Примерами таких коммуникационных рисков могут быть: кибербуллинг, незаконные контакты (например, груминг), знакомства в сети и встречи с интернет-знакомыми и др.

Для детей и молодежи Интернет главным образом является социальной средой, в которой можно не только встречаться с друзьями, но и с незнакомцами. В Интернете пользователя могут обидеть, запугать или даже оскорбить. С появлением киберпространства набирает обороты такое явление, как ***кибербуллинг*** (bullying,отbully – драчун, задира, грубиян, насильник), обозначающее запугивание, унижение, травлю, физический или психологический террор, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона и направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Запугивание в школе обычно заканчивается вместе с занятиями, но в Интернете обидчик может настигнуть свою жертву в любое время. Ведь запугивание или оскорбление в Интернете легко осуществимо с технической точки зрения: для отправки злонамеренного сообщения или публикации оскорбительного текста, доступного широкой аудитории, требуется несколько щелчков мышью. К тому же, в отличие от реального мира, виртуальность дает возможность анонимности и обеспечивает низкую вероятность наказания.

Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент.

И зачастую дети полагают, что если сообщить об этом родителям, это только усугубит ситуацию, что в итоге поддерживает ситуацию запугивания.

Даже если ребенок не сталкивался с оскорблениями в Интернете, но ему нравится общаться через Интернет, такие риски необходимо обсудить заранее и ему необходимо дать совет относительно действий, которые следует предпринять при причинении беспокойства. Прежде всего, ребенок должен понимать, что в Интернете, как и в реальной жизни, каждый человек имеет право на уважительное отношение, поэтому запрещается клеветать или оскорблять других пользователей. Объясните детям, что при общении в интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать. Некоторые действия, для которых потребовалось несколько щелчков мыши, очень сложно отменить, и дети могут не понять, насколько серьезной может стать ситуация. А ведь при необходимости анонимных пользователей можно отследить.

В случае если ваш ребенок лично столкнулся с "негативным собеседником", нужно объяснить, что общение можно прервать, закрыв чат, клиент электронной почты или даже выключив компьютер. Возможно стоит вообще покинуть данный ресурс, удали оттуда свою личную информацию, если не получается решить проблему мирным путем. Ребенок должен понять, что общение с подобными людьми нельзя продолжать (читать и отвечать на оскорбительные сообщения и письма), но тем не менее, если злонамеренные сообщения являются нарушением закона (преступлением против личности), то их необходимо сохранить и показать взрослым. Кроме того, можно настроить параметры программы работы с электронной почтой так, чтобы сообщения от определенного отправителя поступали в отдельную папку. В этом случае ребенку не придется их читать, а у вас будет достаточно материалов для дальнейших действий. Если же вы сами обнаружили материалы, оскорбляющие вас или ваших детей, обратитесь к администратору сайта (модератору чата), чтобы данную информацию удалили. Если же такового не произошло или администратор вам отказал в удалении, то сохраните скриншоты переписки с ним и всех страниц с оскорбительной информацией и обратитесь в полицию.

Особенно опасным риском является ***груминг*** – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации.

Для защиты детей от подобного риска необходимо соблюсти некоторые правила:

- Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе, с кем ребенок общается в сети. Обратите внимание, кого ребенок добавляет к себе «в друзья», с кем предпочитает общаться в сети – с ровесниками или людьми старше себя.
- Объясните ребенку, что нельзя разглашать в интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т. д.), а также пересылать виртуальным знакомым свои фотографии или видео.
- Объясните ребенку, что при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), лучше не использовать реальное имя. Помогите ему выбрать ник, не содержащий никакой личной информации.
- Объясните ребенку опасность встречи с незнакомыми людьми из интернета. В сети человек может представиться кем угодно, поэтому на реальную встречу с интернет-другом надо обязательно ходить в сопровождении взрослых.
- Детскийпознавательный интерес к теме сексуальных отношений между мужчиной и женщиной может активно эксплуатироваться злоумышленниками в интернете. Постарайтесь сами поговорить с ребенком на эту тему. Объясните ему, что нормальные отношения между людьми связаны с доверием, ответственностью и заботой, но в интернете тема любви часто представляется в неправильной, вульгарной форме.
- Важно, чтобы ребенок был вовлечен в любимое дело, увлекался занятиями, соответствующими его возрасту, которым он может посвящать свободное время.

Риск пятый - 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. Необходимо объяснить ребенку, что любые покупки, совершаемые в Интернете или по мобильному телефону, должны осуществляться взрослым, либо осуществляться с его разрешения. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в интернете.

Кроме того, по незнанию, неопытности, под воздействием рекламы ребенок может совершить покупки с помощью счета сотовой связи, поэтому в сотрудничестве с оператором установите необходимые блокировки для телефона, сообщений SMS или ограничения расходов в мобильном телефоне ребенка.

И, конечно же, не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки.

Риск шестой - интернет-зависимость. Интернет-зависимость – навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн. Выделяют:

- Навязчивый веб-серфинг – бесконечные путешествия по всемирной паутине, поиск информации;
- Пристрастие к виртуальному общению и виртуальным знакомствам (большие объемы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети);
- Игровая зависимость – навязчивое увлечение компьютерными играми по сети;
- Навязчивое желание потратить деньги – игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянное участие в интернет-аукционах;
- Пристрастие к просмотру фильмов через интернет;
- Киберсексуальная зависимость – навязчивое влечение к посещению порносайтов и занятию киберсексом.

Практически каждый пятый ребенок в России безуспешно пытается уменьшить проводимое в интернете время, часами блуждает в интернете без особой цели и чувствует себя дискомфортно, когда не имеет к нему доступа. В 10% случаев дети пренебрегают семьей, друзьями или школой, не спят или не едят из-за интернета.

Исследование стратегий родительского контроля выявило неутешительные закономерности: интернет-зависимость лишь немного ниже у тех, кому родители запрещают что-то делать в интернете и не зависит от объяснений, контроля и знания родителей о том, что ребенок делает в интернете. Заметим, что действия родителей гораздо сильнее влияют на частоту пользовательской активности ребенка: дети значительно меньше проводят времени в интернете, если родители запрещают им это, и несколько меньше - если родители объясняют и контролируют их.

Что же делать? В первую очередь, необходимо обратить внимание на возможные признаки интернет-зависимости у вашего ребенка.

- Прежде всего, оцените, сколько времени ваш ребенок проводит в сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.
- Поговорите с ребенком о том, чем он занимается в интернете. Социальные сети создают иллюзию полной занятости – чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить – ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните, поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в сети и не заменяет ли оно реальное общение с друзьями.
- Понаблюдайте за сменой настроения и поведения вашего ребенка после выхода из интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить: головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и другие.
- Поговорите со школьным психологом и классным руководителем о поведении вашего ребенка, его успеваемости и отношениях с другими учениками. Настораживающими факторами являются замкнутость, скрытность, нежелание идти на контакт. Узнайте, нет ли у вашего ребенка навязчивого стремления выйти в интернет с помощью телефона или иных мобильных устройств во время урока.

Если вы обнаружили возможные симптомы интернет-зависимости у своего ребенка, необходимо придерживаться следующего алгоритма действий:

1. Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т.д.
2. Не запрещайте ребенку пользоваться интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и пр.). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в сети.
3. Ограничьте возможность доступа к интернету только своим компьютером или компьютером, находящимся в общей комнате – это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает Ваш ребенок.
4. Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в интернете. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий – например, от бездумного обновления странички в ожидании новых сообщений.
5. Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть

всей семьей или с друзьями – при этом общаясь друг с другом «вживую». Важно, чтобы у ребенка были не связанные с интернетом увлечения, которым он мог бы посвящать свое свободное время.

6. Дети с интернет-зависимостью субъективно ощущают невозможность обходиться без сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без интернета. Важно, чтобы ребенок понял – ничего не произойдет, если он на некоторое время «выпадет» из жизни интернет-сообщества.
7. В случае серьезных проблем обратитесь за помощью к специалисту.

Подводя итог, можно придти к **общим рекомендациям**, как обезопасить своего ребенка при пользовании Интернетом:

1. ***Установите компьютер в общей для всей семьи комнате***

   В этом случае разговор об Интернете и наблюдение за его использованием станет естественным в повседневной жизни. Обсуждение проблем может стать проще, если компьютер находится в общей комнате. Кроме того, Интернетом можно пользоваться вместе.
2. ***Обсуждайте Интернет***

   Проявляйте интерес к действиям ребенка и его друзей как в Интернете, так и в реальной жизни. Расскажите ребенку о прекрасных и увлекательных вещах, которые возможны в Интернете, а также о трудностях, с которыми можно столкнуться. Обсудите с ребенком действия, которые необходимо предпринять, если чувствуется неловкость в какой-либо ситуации в Интернете.
3. ***Узнайте больше об использовании компьютера***

   Если вы сами являетесь пользователем Интернета, вам будет проще определить правильную тактику для детей и помочь им найти в Интернете полезный материал. И тем не менее, постоянно повышайте собственный уровень компьютерной грамотности, чтобы знать, как обеспечить безопасность детей (например, посещение курсов, чтение специальной литературы, консультации с экспертами). И регулярно знакомьте всех членов вашей семьи с базовыми принципами безопасной работы на компьютере и в Интернете.
4. ***Используйте Интернет вместе***

   Найдите сайты, которые подходят для детей, или узнайте о способах поиска полезной информации: запланируйте совместную туристическую поездку, просмотрите образовательные сайты для помощи в школьных заданиях или найдите информацию об увлечениях детей. Просматривая веб-сайты в Интернете вместе, можно также помочь ребенку оценить значимость найденной информации. Можно добавить любимые сайты в папку «Избранное», чтобы совместно просмотренные ранее веб-сайты можно было открыть одним щелчком мыши.
5. ***Договаривайтесь с ребенком о способе и времени использования Интернета***

   Может оказаться полезным согласовать с ребенком время, которое он проводит за компьютером, а также список веб-сайтов, которые он может посещать. Это необходимо обсудить с детьми и прийти к определенному решению, которое всех устраивает.
6. ***Установите доверительные отношения с ребенком***

   Это поможет избежать последствий столкновения ребенка с негативным опытом в Интернете. Положительный эмоциональный контакт ребенка с родителями поможет расположить его к трудному разговору о том, что произошло. Ребенок должен вам доверять и понимать, что вы тоже обеспокоены и хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.

Надеюсь, информация поможет вам чувствовать себя в безопасности на просторах интернета и поможет вашим детям избегать неприятностей в киберпространстве.

Спасибо за внимание!