Методические рекомендации по повышению информационной грамотности педагогических работников.

Введение

Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

В современных условиях развития общества компьютер стал для ребенка и «другом» и «помощником» и даже «воспитателем», «учителем». Всеобщая информатизация и доступный, высокоскоростной Интернет уравнял жителей больших городов и малых деревень в возможности получить качественное образование.

Между тем существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу.

В связи с этим необходимо направить все усилия на защиту детей от информации, причиняющей вред их здоровью и развитию. Просвещение подрастающего поколения, знание ребенком элементарных правил отбора информации, а также умение ею пользоваться способствует развитию системы защиты прав детей.

«Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны - теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и как их избежать» (П.А.Астахов, уполномоченный при Президенте Российской Федерации по правам ребенка).

Медиаграмотность определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг.

Согласно российскому законодательству ***информационная безопасность детей*** – это состояние защищенности детей, при котором отсутствует риск,

связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому,
психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ
"О защите детей от информации, причиняющей вред их здоровью и развитию").

Преодолеть нежелательное воздействие компьютера возможно 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, так как темпы информатизации оказались столь быстрыми, что и семья и школа оказались не готовы к угрозам нового типа, методы борьбы с которыми еще только разрабатываются.

Какие же опасности ждут школьника в сети Интернет? Прежде всего можно выделить следующие:

- суицид-сайты, на которых дети получают информацию о «способах» расстаться с жизнью;
- сайты-форумы потенциальных самоубийц;
- наркосайты. Интернет пестрит новостями о "пользе" употребления марихуаны, рецептами и советами изготовления "зелья";
- сайты, разжигающие национальную рознь и расовое неприятие: экстремизм, национализм, фашизм;
- сайты порнографической направленности;
- сайты знакомств. Виртуальное общение разрушает способность к общению реальному, "убивает" коммуникативные навыки подростка;
- секты. Виртуальный собеседник не схватит за руку, но ему вполне по силам "проникнуть в мысли" и повлиять на взгляды на мир.

Это далеко не весь список угроз сети Интернет. Любой школьник может попасть на такие сайты случайно: кликнув по всплывшему баннеру или перейдя по ссылке. Есть дети, которые ищут подобную информацию специально, и естественно, находят. Кроме этого, появились психологические отклонения, такие как компьютерная и Интернет-зависимость, игромания (зависимость от компьютерных игр). Для преодоления негативного воздействия сети Интернет на детей, в образовательном учреждении должна проводиться целенаправленная воспитательная работа педагогов совместно с родителями. Образовательному учреждению необходимо выработать единую стратегию безопасности совместными усилиями педагогических работников, родителей и обучающихся.

Обучение педагогических работников может проводиться в форме семинаров, мастер - классов, круглых столов, в рамках которых должны рассматриваться проблемы информационной безопасности личности в сети Интернет, нежелательный контент и меры борьбы с ним, виды и формы информационно - психологического воздействия и методы защиты от него,

правила и нормы сетевого этикета, причины возникновения девиантной формы поведения детей и методы работы по их профилактике и устранению.
Необходимую информацию можно найти на сайтах: «Школьный сектор. Права и дети в Интернете» (schoolsectorp.wordpress.com), «Безопасность» (http://sos-ru.info), «Безопасный Интернет» (http://www.saferinternet.ru) и т.д.

Достичь высоких результатов в воспитании невозможно без привлечения родителей. Очень часто родители не понимают и недооценивают угрозы, которым подвергается школьник, находящийся в сети Интернет. Некоторые из них считают, что ненормированное «сидение» ребенка в сети лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, между тем «выпуская» его в Интернет не представляют себе, что точно также нужно обучить его основам безопасности в сети. Ребенок абсолютно беззащитен перед потоком информации, сваливающейся на него из сети. Наша задача выработать в нем критическое мышление.
С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательного учреждения. Формы работы с родителями могут быть разнообразны: выступления на родительских собраниях, индивидуальные беседы, информация на сайте школы, встречи со специалистами, семинарские занятия. Должны быть разработаны специальные методические рекомендации для родителей по обеспечению информационной безопасности в сети Интернет. Они должны содержать классификацию Интернет угроз, рекомендации по обеспечению безопасности ребенка в сети Интернет дома (в зоне ответственности родителей).
Комплексное решение поставленной задачи со стороны семьи и школы позволит значительно сократить риски причинения различного рода ущерба ребенку со стороны сети Интернет. Обеспечение информационной безопасности и воспитание информационной культуры должно стать приоритетным направлением работы современного образовательного учреждения.
Неделя безопасного Интернета проводится в целях привлечения внимания к проблеме безопасности детей и взрослых в сети Интернет.
Предметная неделя как форма методической, учебной и внеклассной работы в школе представляет собой комплекс взаимосвязанных мероприятий, предлагает разнообразные формы деятельности, способствует личностному развитию обучающихся. Для более детальной проработки представленного материала нами разработан примерный план мероприятий, который может быть рекомендован для организации и проведения в образовательных учреждениях недели «Безопасность Интернет».

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ МЕРОПРИЯТИЙ

Анкетирование обучающихся

Для изучения проблемы безопасности в сети Интернет и отношения к ней подростков

разрабатываются анкеты, позволяющие проанализировать современную ситуацию в образовательной среде.

Анкетирование предполагается проводить в форме анонимного опроса как на бумажных носителях, так и в электронном виде. Примерные формы анкет представлены в Приложении 1 и Приложении 2.

Проведение круглого стола «Основы безопасности в сети Интернет»

Цель: формирование устойчивых жизненных навыков при работе в сети Интернет.

Работе круглого стола предшествует предварительная подготовка обучающихся по предложенной тематике. Перечень вопросов для обсуждения выявляется в результате анкетирования обучающихся. Примерные вопросы для обсуждения:

1. Для чего нужен Интернет?
2. Какие существуют риски при пользовании интернетом, и как их можно снизить?
3. Какие виды мошенничества существуют в сети Интернет?
4. Как защититься от мошенничества в сети Интернет?
5. Что такое безопасный чат?
6. Виртуальный собеседник предлагает встретиться, как следует поступить?
7. Как вы можете обезопасить себя при пользовании службами мгновенных сообщений?

При подведении итогов круглого стола обучающимся можно предложить правила поведения в сети Интернет (Приложение 3).

Освоение медиа-безопасности наиболее эффективно в совместной деятельности со взрослыми. Поэтому желательно *привлечь* родителей, представителей органов исполнительной власти, правоохранительных органов, общественных организаций. При проведении урока для детей начальных классов рекомендуется использовать материалы, размещённые:

- на сайте интерактивного курса по Интерент-безопасности (http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu.htm) в разделе «Для учащихся» рассказы для детей 7-10 лет.
- на сайте (http://www.onlandia. org. ua/ru-RU/) On-ляндия. Безопасная веб-страна в разделе «Для детей 7-10 лет» рассказы в картинках, задания и вопросы;
- на сайте (http://content-filtering.ru/aboutus/) Информационно- аналитический ресурс «Ваш личный Интернет» в разделе «Юным пользователям» - «Дошкольники и младшие классы» подсказки и советы по безопасному поведению в сети Интернет;
- на сайте http: //stopfraud.megafon.ru/ федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах «Виды мошенничества» и «Наши рекомендации», а также советы родителям;
- на портале «Безопасный интернет» (http: //www.saferinternet.ru/) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме «Безопасный интернет».

В качестве видео заставки для классного часа или урока можно использовать

http://youtu.be/789j0eDglZQ мультфильм «Безопасный интернет», который разработала студия Mozga.ru.
- на сайте «Началка.ком» материалы по безопасному интернету (http: //www.nachalka.com/taxonomy/term/33
- на сайте (http://www.onlandia.org.ua/ru-RU/) On-ляндия. Безопасная веб-страна в разделе «Для детей 11-14 лет» рассказы в картинках, задания и вопросы; в разделе «Для учителей» опасности в сети и поведение в сети;
- на сайте (http://content-filtering.ru/aboutus/) Информационно- аналитический ресурс «Ваш личный Интернет» в разделе «Юным пользователям» - «Средние классы» подсказки и советы по безопасному поведению в сети Интернет, а также при использовании онлайн-игр и мобильного телефона;
- на сайте http: //stopfraud.megafon.ru/ федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах «Виды мошенничества» и «Наши рекомендации», а также советы родителям;
- на портале «Безопасный интернет» (http: //www.saferinternet.ru/) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме «Безопасный интернет».
- Справочник по детской безопасности в Интернет от Google (http://www.google.ru/familysafety/)
- Сайт советов по работе на компьютере (http: //shperk.ru/sovety/kaksdelat-internet-dlya-detej-bolee-bezopasnym.html)
- Сайт «Компьютерная безопасность. Безопасность жизни» (http://blog.chljahsoft.net/3167)
- Сайт «Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт» (http://i-deti.org/)
- Буклет «Безопасный интернет детям» Министерства внутренних дел РФ (http://www.mvd.ru/userfiles/liflets)
- Материалы III ежегодного Форума Безопасного Интернета (http://safor.ru/prezentacii11 .php)
- Сайт «Дети России Онлайн» (http://detionline.com/)
- как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывания в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Рекомендуется продемонстрировать возможности детских поисковых систем http: //kids. quintura.ru, http://agakids.ru и детского браузера http://www.gogul.tv, а также познакомить с детскими социальными сетями: http: //cyberpapa.ru/, http: //interneshka.net/, http://kinderonline. ru/detskiy portal.html, http://1 dnevnik.ru/, http://www.detkino.ru.

Для отбора содержания урока могут быть использованы материалы сайта www.detionline.com (видеоматериалы, материалы электронного журнала «Дети в информационном
обществе», материалы Линии помощи), а также материалы других сайтов, содержащих
информацию по безопасному использованию сети Интернет.
Большое значение для эффективности урока Интернет-безопасности имеет не только содержание, но и форма его проведения. Целесообразно использовать для детей 1-4 классов - урок-путешествие, урок-викторину, урок-соревнование, урок-игру, беседу. Полезные ссылки:
1) http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/loputon metsa.html - о правилах безопасного поведения в сети Интернет с элементами интерактива;
2) http://www.nachalka.com/node/948 - учебное видео «Как обнаружить ложь и остаться правдивым в Интернете»;
3) http://content-filtering.ru/aboutus/ - информационно-аналитический ресурс «Ваш личный Интернет».
В ходе урока «Интернет-безопасность» в среднем звене
целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве:
Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации,
причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищённости, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому,
психическому, духовному и нравственному развитию.); № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребёнке порочные наклонности, сформировать у ребёнка искажённую картину мира и неправильные жизненные установки.)
Ознакомить обучающихся с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015). Возможны следующие формы проведения урока: урок - пресс-конференция, урок-викторина, урок-соревнование, урок-презентация проектов, урок-практикум, урок-встреча с системными
администраторами и т.д.
Полезные ссылки:
1) http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma ro oma.html -

молодёжная история с элементами интерактива;
2) http://content-filtering.ru/aboutus - информационно-аналитический ресурс «Ваш личный
Интернет»;
3) www.icensor.ru - Интернет-фильтр.

Приложения

Приложение 1

Анкета №1 «Осторожно, вирус!»
Что является основным каналом распространения компьютерных вирусов?
1. Веб-страницы
2. Электронная почта
3. Флеш-накопители (флешки)
Для предотвращения заражения компьютера вирусами следует:
1. Не пользоваться Интернетом
2. Устанавливать и обновлять антивирусные средства
3. Не чихать и не кашлять рядом с компьютером Если вирус обнаружен, следует:
1. Удалить его и предотвратить дальнейшее заражение
2. Удалить его и предотвратить дальнейшее заражение
3. Удалить его и предотвратить дальнейшее заражение
4. Установить какую разновидность имеет вирус
5. Установить какую разновидность имеет вирус
6. Установить какую разновидность имеет вирус
7. Выяснить как он попал на компьютер
Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
1. Применение брандмауэра
2. Обновления операционной системы
3. Антивирусная программа
Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
1. Уничтожение компьютерных вирусов
2. Создание и распространение компьютерных вирусов и вредоносных программ
3. Установка программного обеспечения для защиты компьютера.

Приложение 2

Анкета №2 «Осторожно, Интернет!»
1. Какую информацию нельзя разглашать в Интернете?
1. Свои увлечения
2. Свой псевдоним
3. Домашний адрес

2. Чем опасны социальные сети?
1. Личная информация может быть использована кем угодно в разных целях
2. При просмотре неопознанных ссылок компьютер может быть взломан
3. Все вышеперечисленное верно

3. Виртуальный собеседник предлагает встретиться, как следует поступить?
1. Посоветоваться с родителями и ничего не предпринимать без их согласия
2. Пойти на встречу одному
3. Пригласить с собой друга

4. Что в Интернете запрещено законом?
1. Размещать информацию о себе
2. Размещать информацию других без их согласия
3. Копировать файлы для личного использования

5. Действуют ли правила этикета в Интернете?
1. Интернет - пространство свободное от правил
2. В особых случаях
3. Да, как и в реальной жизни.

Приложение 3

Круглый стол «Основы безопасности в сети Интернет»
Правила работы в сети Интернет
1. Не входите на незнакомые сайты.
2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
4. Никогда не посылайте никому свой пароль.
5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
6. При общении в Интернет не указывать свои личные данные, а использовать псевдоним (ник)
7. Без контроля взрослых ни в коем случае не встречаться с людьми, с которыми познакомились в сети Интернет.
8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.
9. В настоящее время существует множество программ, которые производят фильтрацию содержимого сайтов. Между членами семьи должны быть доверительные отношения, чтобы вместе просматривать содержимое сайтов.
10. Не всей той информации, которая размещена в Интернете, можно верить.
11. Не оставляйте без присмотра компьютер с важными сведениям на экране.
12. Опасайтесь подглядывания через плечо.
13. Не сохраняйте важные сведения на общедоступном компьютере.