

июнь, 2023 г.

Иванова Н.В., ведущий специалист-методист
Отдела образования Администрации
Краснохолмского муниципального округа

Методические рекомендации по теме:

Повышение информационной грамотности педагогических работников в области информационной безопасности

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», «преподавателем». Всеобщая информатизация и доступный, высокоскоростной Интернет уравнил 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 обучающихся, 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.

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 обучающихся.

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 ОУ оказались не готовы к угрозам нового типа, методы борьбы с которыми еще только разрабатываются.

Какие же опасности ждут обучающихся 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. 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 обучающийся 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 преподавателей 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: «Права и дети в Интернете» (schoolsectorp.wordpress.com), «Безопасность» (<http://sos-ru.info>), «Безопасный Интернет» (<http://www.saferinternet.ru>) и т.д.

Полезно создать в ОУ «Совет по Интернет - безопасности», в рамках которого обучающиеся будут изучать и создавать проекты по данной тематике,

проводить доклады и заседания, что позволит воспитать в обучающихся не только культуру общения в сети, но и привить нравственность, ответственность за использование и передачу информации.

Достичь высоких результатов в воспитании невозможно без привлечения родителей. Очень часто родители не понимают и недооценивают угрозы, которым подвергается обучающийся, 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 незащищен 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 ОУ, 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 ОУ 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 ОУ представляет собой комплекс взаимосвязанных мероприятий, предлагает разнообразные формы деятельности, способствует личностному развитию обучающихся. Для более детальной проработки представленного материала можно использовать 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 использовании интернета, 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 использовании службами мгновенных сообщений?

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

Проведение тематического классного часа

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.
Задачи:

- 1) информирование обучающихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;
- 2) информирование обучающихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);
- 3) обучение подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);
- 4) профилактика формирования у обучающихся интернет-зависимости и игровой зависимости (игромании, гэмблинга);
- 5) предупреждение совершения обучающимися правонарушений с использованием информационно-телекоммуникационных технологий.

Ожидаемые результаты.

В ходе проведения классного часа обучающимся должны научиться делать более безопасным и полезным свое общение в Интернете и иных информационно-телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;

- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;

- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;

- распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;

- распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;

- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;

- анализировать степень достоверности информации и подлинность ее источников;

- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях. При организации классного часа важно исходить из возрастных особенностей обучающихся, учесть уровень их знакомства с Интернетом. Организовать проведение классного часа необходимо таким образом, чтобы несовершеннолетние не только получили необходимый минимум знаний об информационной безопасности, но смогли высказать свою точку зрения на указанную проблему.

При определении содержания, форм и методики проведения единого классного часа важно учитывать:

- необходимость деятельностного подхода в учебной работе обучающихся в активном и интерактивном режиме;

- целесообразность использования методик учебного сотрудничества, различных вариантов работы в группах, кооперации, моделирования жизненных ситуаций. При определении тематики бесед для единого классного часа «Безопасный Интернет» необходимо исходить:

- из понимания важности и значимости для каждого человека основ медиакультуры;

- из возможности в доступных игровых ситуациях знакомить обучающихся с основами медиакультуры; из необходимости приобретения обучающимися первичного опыта регулирования медиаотношений;

- из необходимости получения обучающимися знаний и навыков использования конкретных правил и норм медиаобразования и первичного опыта разработки собственных правил медиакультуры. Темы бесед могут быть следующие:

- «Интернет среди нас»;

- «Я и мои виртуальные друзья»;

- «Интернет в моей семье»;

- «Мой Интернет»;

- «Интернет и природа»;
- «Мой социум в Интернете»;
- «Интернет и моя будущая профессия»;
- «Интернет и мое здоровье».

Проведение родительского собрания

В начале родительского собрания рекомендуется провести анонимное анкетирование, которое позволит выявить отношение родительской общественности к внедрению в образовательный процесс ИКТ. По результатам анкетирования будет определена дальнейшая стратегия работы ОУ по безопасности детей в сети Интернет.

Примерный перечень вопросов анкетирования в Приложении 4.

После анкетирования проводится беседа по проблеме доступа ребенка к сети Интернет, в которой поднимаются наиболее актуальные вопросы. Далее даются рекомендации родителям по работе детей в сети Интернет. В конце родительского собрания всем родителям предлагается памятка по безопасности детей в сети Интернет при помощи программных средств.

Урок «Интернет-безопасность»

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

1) информирование обучающихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2) информирование обучающихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

3) ознакомление обучающихся с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;

4) обучение подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику обучающихся, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

5) предупреждение совершения обучающимися правонарушений с использованием информационно-телекоммуникационных технологий.

В ходе уроков Интернет - безопасности обучающиеся должны научиться делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно-телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;

- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;

- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации; распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;

- распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;

- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;

- анализировать степень достоверности информации и подлинность ее источников; применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

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.

Приложение 4

Материалы для проведения родительского собрания.

Анкета для родителей

Уважаемые родители!

В ОУ информационные технологии применяются в различных направлениях: учебная деятельность (урочная и внеклассная), воспитательная (классные часы и различные мероприятия), ИКТ являются основой единого информационного пространства школы (администрация, преподаватель, обучающийся, родитель) - сайт ОУ, работа "Электронного журнала", учебно-материальная база ОУ, цифровые образовательные ресурсы и т.п. В том числе, информационные технологии прочно вошли в деятельность и досуг обучающихся. Просим Вас ответить на несколько вопросов. (Все вопросы не являются обязательными для ответа. Если Вы выбираете "другое" - не забудьте поставить напротив галочку).

1. В каком классе учится Ваш ребенок?

2. Отношение к внедрению ИТ в образование.

Внедрение информационных технологий (ИТ) в образование относится к числу крупномасштабных инноваций. Среди ИТ, внедряемых в сфере образования, можно выделить следующие: обучающие, тренажеры, справочные, единые информационными образовательные пространства (сайт ОУ, дистанционное обучение, электронные дневники), техническое обеспечение кабинетов и др.

- скорее положительно

- скорее отрицательно (не вижу необходимости)

- Другое:

3. Информационные технологии и обучение в ОУ проводятся различные мероприятия с применением информационных технологий (проектная деятельность, уроки, классные часы и родительские собрания).

- урок, с применением новых информационных технологий более популярен у моего ребенка (более интересен, понятен и т.п. - со слов ребенка)
 - ребенок с интересом и удовольствием выполняет проекты (рефераты, доклады), используя компьютер
 - ребенок готовится к уроку, используя компьютер (Интернет, полезные ссылки на сайте ОУ, рекомендуемые преподавателем сайты и т.п.)
 - классный руководитель проводит родительские собрания с использованием компьютера
 - Другое:
-

4. Работа "Электронного журнала". Одной из возможностей ресурса является просмотр на страницах этого ресурса в Интернете оценок обучающегося, которые выставляют преподаватели на уроках и их комментарии, домашнее задание... (пароль доступа индивидуален для каждого пользователя)

- в нашем классе есть "Электронный журнал", его работа очень важна для нас
 - в нашем классе есть "Электронный журнал", но в его работе нет необходимости
 - возможности "Электронного журнала" очень важные, но в нашем классе он не работает
 - в нашем классе он не работает и думаю, что нет в нем необходимости
 - Другое:
-

5. Посещение сайта ОУ

- часто посещаем (в том числе раздел Новости)
 - очень редко посещаем - не посещаем
 - Другое:
-

6. Сайт ОУ. Напишите, пожалуйста, что бы Вы хотели бы изменить в работе сайта. Ваши предложения и рекомендации Вы можете написать в этом разделе! _____

7. Есть ли у Вас дома компьютер?

- да (один)
 - да (несколько)
 - нет
 - Другое:
-

8. Кто пользуется компьютером у Вас дома?

- только родители
- только ребенок
- все члены семьи (родители и дети)

*Примерный список вопросов, которые планируется обсудить на
родительском собрании*

1. В каком возрасте следует разрешить детям посещение интернета?
2. Следует ли разрешать обучающимся иметь собственные учетные записи электронной почты?
3. Какими внутрисемейными правилами следует руководствоваться при использовании интернета?
4. Как дети могут обезопасить себя при пользовании службами мгновенных сообщений?
5. Могу ли я ознакомиться с записью разговоров моего ребенка в программе обмена мгновенными сообщениями (MSN Messenger, ICQ, Mail Agent)?
6. Могут ли дети стать интернет-зависимыми?
7. Что должны знать дети о компьютерных вирусах?
8. Как проследить какие сайты посещают дети в интернете?
9. Что следует предпринять, если моего ребенка преследуют в интернете?
10. Помогает ли фильтрующее программное обеспечение?
11. На какие положения политики конфиденциальности детского сайта нужно обращать внимание?
12. Какие угрозы встречаются наиболее часто?
13. Как научить детей отличать правду ото лжи в Интернет?