Методические рекомендации по организации урока информационной безопасности в основной школе

Анализ УМК по информатике и ИКТ для основной школы на предмет изучения информационной безопасности позволяет сделать вывод о том, что на уровне основного общего образования в рамках предмета «Информатика» акцент в соответствии с требованиями ФГОС делается на формировании навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

УМК «Информатика» 7 - 9 класс (ФГОС), автор Угринович Н. Д.

Тема «Информационное общество и информационная безопасность». Всего 3 часа: 1 час в 7 кл. и 2 часа в 9 кл. Содержание темы: Информационное общество. Информационная культура. Перспективы развития информационных и коммуникационных технологий. Правовая охрана программ и данных. Защита информации. Правовая охрана информации. Лицензионные, условно бесплатные и свободно распространяемые программы.

УМК «Информатика» 7 - 9 класс (ФГОС), авторы Семакин И.Г. и др.

Аспекты информационной безопасности рассматриваются в 7 и 9 классах в рамках тем «Компьютер: устройство и программное обеспечение» (содержание темы: правила техники безопасности и эргономики при работе за компьютером, использование антивирусных программ) и «Информационные технологии и общество» (содержание темы: проблемы безопасности информации, этические и правовые нормы в информационной сфере).

УМК «Информатика» 5-9 класс (ФГОС), автор Босова Л.Л.

Предметные результаты «Формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права» формируются в 5 классе при изучении темы «Передача информации», в 7 классе при изучении тем «Всемирная паутина» и «Программное обеспечение компьютера», в 9 классе при изучении темы «Информационные ресурсы и сервисы Интернета».

УМК «Информатика» 7-9 класс, (ФГОС), авторы Горячев А.В.

Некоторые аспекты информационной безопасности рассматриваются в 7 классе при изучении темы «Общение в сети Интернет». Содержание темы: Как вести себя и чего опасаться в сети Интернет. Ваша личная территория в

сети Интернет. Личное и публичное общение в Интернете. Как правильно спорить в Интернете.

УМК «Информатика» 7-9 класс, (ФГОС), авторы Гейн А.Г, Юнерман Н.А. и др.

В 9 классе в рамках темы «Правовые вопросы Интернета. Безопасность и этика Интернета. Защита информации» рассматриваются вопросы информационной безопасности в сети Интернет.

Таким образом, все авторские коллективы уделяют внимание вопросам информационной безопасности, в основном аспектам безопасного поведения в Интернете и защите от компьютерных вирусов. В основном такие уроки запланированы авторами в начале 7 класса и в конце 9 класса. При этом, с учетом потери уроков в праздничные дни и подготовкой к ОГЭ в конце 9 класса, учителя информатики часто предлагают данные темы на самостоятельное изучение обучающимся. А в 5, 6, 8 классах эта тема в явном виде вообще отсутствует. Однако именно в подростковом возрасте дети становятся участниками сетевых сообществ, ведут активную деятельность в Интернете. Конечно же, на этом этапе необходимо рассказать им о защите персональных данных, о признаках компьютерной зависимости и синдрома информационной усталости, о мошенничестве, связанном с использованием мобильных устройств. Поэтому совершенно необходимо дополнительное проведение занятий информационной безопасности. Это могут быть классные часы или внеурочные занятия, проектная деятельность.

Вместе с переходом в возрастную категорию «подросток» проблемы, связанные с Интернетом, становятся действительно острыми и глобальными. Дополнительная психологическая и социальная проблема детей подросткового возраста заключается в возрастном становлении характера и скептическом и недоверчивом отношении к замечаниям и рекомендациям родителей и учителей. А техническая подготовленность к использованию возможностей сети Интернет уже достаточна высока на фоне несформировавшейся психики и неустойчивого социального поведения школьников средней школы.

Учителю, чтобы усилить воспитательные меры работы с учениками важно показать, что вы такой же регулярный пользователь в сети, и сетевых сервисов: социальных сетей, чатов, форумов профессиональной направленности или связанных с личными увлечениями. Можно наладить с ними виртуальное общение по электронной почте, по skype, задавать задания, связанные с необходимостью налаживания такого рода общения.

Например, преподаватель биологии может попросить своих учеников, посадивших семена огородных растений дома для домашнего наблюдения за их ростом, присылать фотографии стадий роста растений по электронной почте. Таким образом, отрабатываются не только домашние задания непосредственно по программе курса и имеет место внедрение ИКТ в

образовательный процесс, но и формируется элемент электронной учебной коммуникации с преподавателем, повышающий авторитет учителя и заставляющий ученика осознанно работать с образовательными возможностями [11].

Как включить в образовательный процесс мероприятия, повышающие информационную культуру школьника основной школы? Какие методы, формы при этом использовать?

Информационная безопасность в Интернете может обсуждаться во время уроков информатики, социологии, ОБЖ, гражданского права и др. В образовательном учреждении рекомендуется проводить неделю, день, уроки Интернет-безопасности, внеклассные мероприятия.

Мероприятия можно приурочит к профессиональным праздникам:

Международный день защиты информации – 30 ноября. Праздник начал существовать в 1998 году (с праздника есть даже сайт) т.к. в 1988 г. была зафиксирована первая массовая эпидемия червя, получившего название по имени своего «творца» – Морриса. Праздник существует и признан международным благодаря американской Ассоциация компьютерного оборудования. Цель этого Дня — напомнить всем о необходимости защиты компьютерной информации, а также обратить внимание производителей и пользователей аппаратных и программных средств на проблемы безопасности.

Международный день безопасного Интернета – второй вторник февраля (введен в 2004 году). Сайт международного дня безопасности Интернета www.saferinternetday.org

Во время мероприятий по медиабезопасности следует ознакомить обучающихся:

- с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;
- с информацией о необходимости критического отношения к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, признаках отличия достоверных сведений от недостоверных, способах нейтрализации вредной и опасной для детей информации, распознавания признаков злоупотребления доверчивостью;
- с правилами общения в социальных сетях (сетевой этикет).

В рекомендациях «Безопасный Интернет» [14] предлагается следующая тематика проведения школьных мероприятий по медиабезопасности:

- Противозаконная, неэтичная и вредоносная информация в Интернете: как ее избежать.
- Достоверность информации в Интернете, проблемы и способы проверки информации на достоверность и полноту.
- Этика сетевого общения.

- Личная информация: нужна ли она в Интернете, как защитить личную информацию в блогах, социальных сетях и пр.
- Социальные сети: как общаться в сети и не попасть в сети мошенников и злоумышленников.
- Что такое хакерство? Почему хакеров считают преступниками.
- Интернет- зависимость: угрозы, реальность, проблемы, решения.
- Web -серфинг: как не потерять себя и свое время в Интернете.
- Как распознать кибермошенничество и не стать жертвой.
- Нигерийские письма: предложения в письмах и как не попасться на удочку мошенников.
- Что такое киберхулиганство: как не стать жертвой и киберхулиганом.
- Как защитить свою почту от спама и не стать спамером.
- Компьютерные вирусы и методы борьбы с ними.
- Законодательство России о киберпреступлениях.
- Безопасность в коммерческих Интернет-сервисах: Интернет-магазины, услуги различных фирм и др.,
- Компьютерные игры, как не стать игроманом.
- Азартные игры в Интернете – поле чудес для….?
- Мобильные угрозы в современном мире.
- Как правильно вести себя с киберхулиганами и защититься от нежелательного общения.

Одним из эффективных способов изучения любого учебного материала и в частности вопросов по информационной безопасности является метод высокотехнологичных учебных проектов. Учителю любой дисциплины важно инициировать большие и малые телекоммуникационные учебные проекты.

В методических рекомендации по проведению уроков «Безопасность в Интернете» в начальной и средней школе [11] *учебный телекоммуникационный проект* рассматривается как совместная учебно-познавательная, творческая или игровая деятельность учащихся-партнеров, организованная на основе компьютерной телекоммуникации, имеющая общую цель, согласованные способы деятельности, направленная на достижение общего результата деятельности.

Так, например, можно участвовать в сетевых проектах для школьников организованных дистанционно или организовать собственный учебный проект.

Школьной проектной деятельностью учитель решает сразу несколько проблем [11]: во-первых, учащиеся приобретают навык практического применения полученных теоретических знаний по использованию компьютеров, компьютерных технологий и Интернета и связанные с этим вопросы безопасности; во-вторых, и это самое главное, школьник начинает видеть в компьютере и Интернете не только игрушку и поток непотребных

ресурсов, но инструмент создания нового, интересного и нужного не только ему, но и окружающим его в школе и дома людям, пространства. И в этом пространстве ребёнок подобен творцу: каким он его создаст, таким его мир и будет.

Лучше всего инициировать глобальный (на один или несколько классов) проект, связанный с усиленной необходимостью коммуникации. То есть каждый школьник выполняет часть работы по общему учебному телекоммуникационному проекту. Чем глобальнее и трудозатратнее проект, тем лучше. Надо добиваться того, чтобы школьнику просто некогда было бы заниматься в Интернете чем-то иным, кроме работы по реализации проекта. Для этого проект должен быть:

а) интересен самим детям и, желательно, и предложен же ими, чтобы они позднее не могли отказаться от того, что сами же и предложили;

б) очень высокотехнологичным, чтобы для его реализации школьнику было необходимо полностью проявить свою компьютерную «продвинутость», да ещё и подучиться разным сложным технологиям, общаясь со своими виртуальными друзьями: здесь пройдёт естественный отсев пустопорожних коммуникаций в социальных сетях: человеку творческому некогда и не о чем разговаривать на уровне междометий о несущественных пустяках;

в) долгосрочным и предусматривающим дальнейшее коммуникативное дополнение. После размещения его в сети у детей, гордящихся проделанной работой, должен быть стимул общаться в Интернете на тему своего проекта и постоянно дополнять и дорабатывать его. Для этого необходимо устраивать публичные показы проектов школьников на классных часах, на предметных уроках, в рамках программы которых сделаны эти проекты.

В качестве примера можно привести сетевую игру, организованную в МКОУ ГО Заречный «СОШ№4». 40 детей из 7 городов России в течение месяца рассказывали в сети друг другу о своем городе и градообразующем мероприятии в форме сетевых презентаций, видеороликов и сетевых газет, а затем с помощью созданных сетевых интерактивных заданий проверяли друг у друга приобретенные за это время знания. Времени детям хватало только на то, чтобы в сети создавать и творить собственные сетевые ресурсы, смотреть и анализировать работы других участников игры. Прогуливаться по различным сомнительным сайтам возможности не было. Сейчас ребята знают, чем можно заниматься в сети. В рамках учебной практики «Зачем WEB 2.0 школьнику?», организованной МКОУ ГО Заречный «СОШ№4» была разработана карта знаний http://www.mindmeister.com/ru/165370920 «Что можно делать школьнику в сети Интернет с помощью WEB 2.0 технологий». Разработанная схема представлена на рис 4.

Если ребенок с социально-значимым результатом побывал в сети, узнал, что в сети можно оформлять фото и видео материалы, создавать презентации, инструменты для проверки знаний, организовать личное

сетевое пространство, проводить информационные исследования, то вряд ли у него появится в дальнейшем желание вновь перейти к праздному лицезрению сетевых ресурсов.

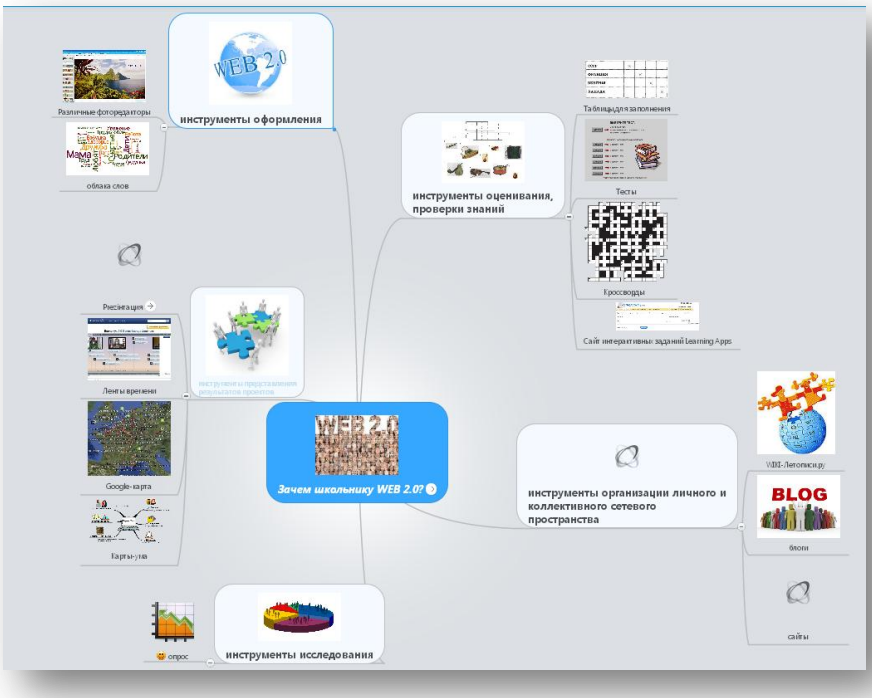

рис 4

Конкретным примером реализации проектной деятельности может стать WEB-квест. Для примера можно рассмотреть WEB-квест «Безопасный Интернет» http://www.web-kvest.pldetstva.edusite.ru/p1aa1.html

рис 5

Веб-квест - это игра, реализованная на сетевом ресурсе с заданиями над которыми работают учащиеся, выполняя ту или иную возложенную на них миссию – выбрав одну из ролей, предложенных учителем.

Особенностью образовательных веб-квестов является то, что часть или вся информация для самостоятельной или групповой работы учащихся с ним находится на различных веб-сайтах, ссылки на которые может предложить педагог, предварительно выбрав самые интересные и информативные по изучаемому вопросу. Кроме того, результатом работы с веб-квестом является публикация работ учащихся в виде веб-страниц и веб-сайтов (локально или в Интернет).

При продумывании методов организации урока и внеурочной деятельности важно помнить об особенностях мышления современной молодежи - «клиповом», которое не отличается глубиной проникновения в информацию, но зато отличается большими скоростями пропускания через себя информации. Дети сегодня не умеют анализировать текстовую информацию, не обладают навыками функциональной грамотности чтения. Для формирования данной грамотности, важно учить детей сворачивать и разворачивать информацию, представлять ее в различных формах. Решением проблемы может стать задания по преобразованию одного вида информации в другой вид. Например, можно предложить информацию из видео или текст перевести в графику – плакат, комикс, инфографику или, наоборот, по картинке, плакату, комиксу, инфографике составить рассказ, объясняющий вопросы безопасности информации. Результаты деятельности важно предоставить общественности – опубликовать в Интернете, повесить в тематических уголок школы, выпустить газету для школы с результатами деятельности, выступить перед младшими школьниками.

Идея такой формы работы была предложна на странице сайта Мастер класс «Урок информационной безопасности» (рис 6)

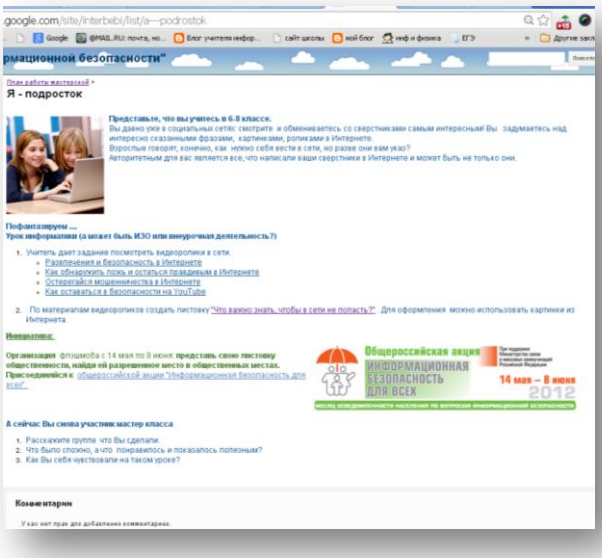

рис.6

На уроке ребятам предлагается посмотреть ролики

- Развлечения и безопасность в Интернете
- Как обнаружить ложь и остаться правдивым в Интернете
- Остерегайся мошенничества в Интернете
- Как оставаться в безопасности на YouTube

По материалам видеороликов создать в группах тематические листовки, используя сетевые технологии совместного редактирования Google.

Лучшие листовки повесить в *уголок безопасности*, который должен быть в каждой школе.

Итак, резюмируем, на что нужно обратить особое внимание при рассмотрении вопроса об Интернет безопасности детей основной школы:

1. Относись к информации осторожно. То, что веб-сайт эффектно выглядит, еще ни о чем не говорит. Спроси себя: для чего этот сайт сделан? В чем меня хотят убедить его создатели? Чего этому сайту не достает? Узнай об авторах сайта: зайди в раздел «О нас» или нажми на похожие ссылки на странице. Узнай, кто разместил информацию. Если источник надежный, например, университет, то, вполне возможно, что информации на сайте можно доверять.
2. Часто в Сети можно столкнуться с подделками под известные сайты социальных сетей или почтовых сервисов, так называемым «фишингом». После неосторожного ввода имени пользователя и пароля на страницах не настоящих, поддельных сайтов, злоумышленники используют пароли в своих целях на реальных сайтах. Например, для рассылки спама от имени владельца почтового ящика или злоумышленного обращения в социальных сетях от имени владельца аккаунта. Каждый сайт в Интернете имеет свой уникальный адрес. Необходимо проверять именно адрес страницы, не доверяя внешнему оформлению, которое может быть скопировано с оригинального.
3. Используя информацию из Интернета в своей работе, следуй правилу трех источников. Организуй поиск и сравни три разных источника информации, прежде чем решить, каким источникам можно доверять. Не забывай, что факты, о которых ты узнаешь в Интернете, нужно очень хорошо проверить, если ты будешь использовать их в своей работе.

Хотя Интернет – специфическая среда для общения, в ней существуют определенные правила вежливости, которые широко обсуждаются в Интернете, но, к сожалению, культура общения остается на низком уровне. В сети нередко можно наблюдать грубость, речевую агрессию, нетерпимость к чужим мнениям. Важно сохранять правила человеческого общения даже в случае анонимной коммуникации. На эмоциональное послание лучше отвечать не мгновенно, а через некоторое время, дабы не плодить излишний негатив в общении. Основные правила общения в сети описаны в приложении «*Сетевой этикет»*.