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.
- 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 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 учителей совместно с родителями.

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.

Работа с обучающимися должна вестись в зависимости от возрастных особенностей: начальное звено (2-4 класс), среднее (5-9 класс) и старшее (10-11 класс). На каждом этапе необходимы специальные формы и методы обучения в соответствии с возрастными особенностями. Формирование навыков информационной безопасности и культуры должно осуществляться не только на уроках информатики, но и на других предметах (например, обществознания, права, ОБЖ и т.д.), а также и во внеурочной деятельности.

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.

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).

Проведение компьютерной игры для младших школьников

В рамках классного часа или урока информатики (окружающего мира) обучающимся 2-4 классов целесообразно предложить компьютерную игру о правилах поведения в сети Интернет «Прогулка через ИнтерНетЛес» http://www.wildwebwoods.org/popup.php?lang=ru), где в игровой форме показано какие опасности могут встречаться при работе в сети Интернет, рассказано о сетевом взаимодействии и об этикете, а также о защите прав

детей.

Проведение тематического классного часа

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

Задачи:

1) информирование учащихся 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 учащихся 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 детей и 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 учащихся интернет-зависимости и игровой зависимости (игромании, гэмблинга);

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

Ожидаемые результаты:

В ходе проведения классного часа дети 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 учащихся, 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 учащихся 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 с 1 по 11 классы 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 в современной школе»;
- «Интернет и мое здоровье» и т.д.

Освоение медиабезопасностью наиболее эффективно в совместной деятельности со взрослыми. Поэтому желательно привлечь родителей, представителей органов исполнительной власти, правоохранительных органов, общественных организаций.

При проведении урока в начальных классах 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, а также в разделе «Тесты» (можно организовать on-line тестирование школьников 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/335).

При проведении урока в 5-9 классах 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 11-16 лет, а также в разделе «Тесты» (можно организовать on-line тестирование школьников 11-14 лет);
- 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».

При проведении урока в 10-11 классах 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 11-16 лет, а также в разделе «Тесты» (можно организовать on-line тестирование школьников 11-14 лет);

- на сайте (http://www.onlandia.org.ua/ru-RU/) On-ляндия. Безопасная веб-страна в разделе «Для подростков» советы по безопасному общению и работе в режиме on-line; 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» - «Старшие 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».

Дополнительные Интернет ресурсы для проведения классного часа:

- 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_k_deti_06.pdf)
- Материалы III ежегодного Форума Безопасного Интернета (http://safor.ru/prezentacii11.php)
- Сайт «Дети России Онлайн» (http://detionline.com/)

Проведение родительского собрания

Родительские собрания целесообразно проводить по ступеням возрастного развития обучающихся (начальная ступень образования, основная ступень образования, старшая ступень образования).

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 (с учетом возрастных особенностей) (Приложение 5).

В конце родительского собрания всем родителям предлагается памятка по безопасности детей в сети Интернет при помощи программных средств.

Урок «Интернет-безопасность»

(на всех образовательных ступенях)

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 детей и подростков правилам ответственного ибезопасного 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 детей, 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.

В рамках ***урока «Интернет-безопасность» в начальных классах*** целесообразно ознакомить обучающихся:

– с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;

– как критически относиться к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

– 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://1dnevnik.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 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_rooma.html - молодѐжная история с элементами интерактива;

2) http://content-filtering.ru/aboutus - информационно-аналитический ресурс «Ваш личный Интернет»;

3) www.icensor.ru – Интернет-фильтр.

В рамках ***урока «Интернет-безопасность» в старших классах*** целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве (см. рекомендации для проведения урока Интернет–безопасности в среднем звене).

Необходимо обратить внимание обучающихся на классификацию вредоносных информационных ресурсов:

информация, причиняющая вред здоровью и (или) развитию детей;

информация, запрещенная для распространения среди детей;

информация, ограниченная для распространения среди детей определенных возрастных категорий.

На уроке необходимо затронуть следующие аспекты:

перечень рисков, подстерегающих ребенка в сети Интернет;

рекомендации по грамотному использованию электронной почты;

технологии безопасного общения в средах мгновенного обмена сообщениями.

Необходимо обеспечить обучающихся инструкциями по безопасному общению в чатах; советами по профилактике и преодолению Интернет-зависимости; общими правилами по безопасности детей в сети Интернет.

Также рекомендуется рассмотреть следующие объекты, являющиеся опасными в Интернете: нежелательные программы; защита личных данных; мошенничество; виртуальные “друзья”; пиратство; on-line-игры; этика; критический подход к информации.

Обеспечить обучающихся информацией о программном обеспечении, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации.

Ознакомить обучающихся с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможные формы проведения урока в 9-11 классах – лекция, деловая игра, урок-презентация проектов, мозговой штурм «Интернет-безопасность», дискуссия, дебаты, встреча со специалистами медиа-сферы, системными администраторами и т.д.

Полезные ссылки:

1) http://www.kaspersky.ru – антивирус «Лаборатория Касперского»;

2) http://www.onlandia.org.ua/rus/ - безопасная web-зона;

3)http://www.interneshka.net – международный онлайн-конкурс по безопасному использованию Интернета;

4)http://www.saferinternet.ru – портал Российского Оргкомитета по безопасному использованию Интернета;

5) http://content-filtering.ru – Интернет СМИ «Ваш личный Интернет»;

6) http://www.rgdb.ru – Российская государственная детская библиотека.

Примерный план-конспект урока на тему «БезОпасный Интернет»приведён в Приложении 7.

По итогам проведения уроков проводится итоговое анкетирование по теме «Безопасный интернет» (Приложение 8).

Проведение внеклассного мероприятия «Сказка о золотых правилах безопасности в сети Интернет»

Сказку целесообразно подготовить силами обучающихся 5-6 классов и представить ее обучающимся начальной школы.

При разработке сценария внеклассного мероприятия «Сказка о золотых правилах безопасности в сети Интернет» значимую роль играет сам педагог, так как именно от него зависит своевременность и актуальность представленного материала.

Обсуждение сказки позволит младшим школьникам определить собственную позицию организации работы в сети Интернет. Примерный сценарий сказки приведен в Приложении 9.

По окончании внеклассного мероприятия обучающимся раздаются памятки с семью золотыми правилами работы в сети Интернет.

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

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, пришедших в российскую школу в последние десятилетия. Среди ИТ, внедряемых в сфере образования, можно выделить следующие: обучающие, тренажеры, справочные, единые информационными образовательные пространства (сайт школы, дистанционное обучение, электронные дневники), техническое обеспечение кабинетов и др.

скорее положительно

скорее отрицательно (не вижу необходимости)

Другое:_____

3. ***Информационные технологии и обучение в школе.*** 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 школы, рекомендуемые учителем 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 учащегося, которые выставляют учителя 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 Школьного сайта***

часто посещаем (в том числе раздел Новости)

очень редко посещаем

не посещаем

Другое:_____

6***. Школьный сайт.*** Напишите, пожалуйста, что бы Вы хотели 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 детям 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?

Приложение 5

Рекомендации для родителей (законных представителей) детей различных возрастных категорий

Возраст от 7 до 8 лет

Находясь в Интернете, ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям (законным представителям) особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).

В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок.

Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернету. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку. Запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как Kaspersky Internet Security версии 7.0 со встроенным родительским контролем.

Советы по безопасности в сети Интернет:

Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернет с помощью средств Родительского контроля.

Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM).

Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.

Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.

Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

Научите детей не загружать файлы, программы или музыку без вашего согласия.

Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.

Подробнее о таких фильтрах

http://www.microsoft.com/rus/athome/security/email/fightspam.mspx.

Не разрешайте детям использовать службы мгновенного обмена сообщениями.

В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.

Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах.

Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте:

Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

Не забывайте беседовать с детьми об их друзьях в Интернет.

Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.

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 Интернете.

Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.

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 о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Расскажите детям о порнографии в Интернет.

Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст от 13 до 17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернете 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 Интернете. 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.

Что посоветовать в этом возрасте?

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 сети Интернет должен находиться в общей комнате.

Не забывайте беседовать с детьми об их друзьях в Интернете, 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 сети 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 Интернете.

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 Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, 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 закону.

Приложение 7

План - конспект урока на тему «БезОпасный Интернет»

(9 – 11 класс)

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

Задачи:

- изучение информированности пользователей о безопасной работе в сети Интернет;
- знакомство с правилами безопасной работы в сети Интернет;
- ориентироваться в информационном пространстве; способствовать ответственному использованию online-технологий;
- формирование информационной культуры обучающихся, умения самостоятельно находить нужную информацию, пользуясь web-ресурсами;
- воспитание дисциплинированности при работе в сети.

Обучающиеся должны знать:

перечень информационных услуг сети Интернет;

правилами безопасной работы в сети Интернет;

опасности глобальной компьютерной сети.

Обучающиеся должны уметь:

ответственно относиться к использованию on-line-технологий;

работать с Web-браузером;

пользоваться информационными ресурсами;

искать информацию в сети Интернет.

Тип урока: урок изучения нового материала.

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частично-поисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Ссылки на web-ресурсы:

1) http://www.kaspersky.ru – антивирус «Лаборатория Касперского»;

2) http://www.onlandia.org.ua/rus/ - безопасная web-зона;

3)http://www.interneshka.net – международный онлайн-конкурс по безопасному использованию Интернета;

4)http://www.saferinternet.ru – портал Российского Оргкомитета по безопасному использованию Интернета;

5) http://content-filtering.ru – Интернет СМИ «Ваш личный Интернет»;

6) http://www.rgdb.ru – Российская государственная детская библиотека.

Этапы урока:

1. Организация начала урока. Постановка цели урока.

Просмотр видеоролика

http://video.mail.ru/mail/illari.sochi/_myvideo/1.html.

Постановка темы и главного вопроса урока.

2. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения обучающихся).

3. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденному материалу.

4. Закрепление изученного материала. Рекомендации по правилам безопасной работы. Тестирование.

5. Подведение итогов урока. Оценка работы группы. Домашнее задание.

Ход урока

1. Организация начала урока. Постановка цели урока.

Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но с другой стороны, миллионы компьютеров получили доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И ни когда-то, а прямо сейчас.

(Просмотр видеоролика «Дети и Интернет» – 1 мин. (по выбору))32 (http://www.youtube.com/watch?v=HbVgg6-3EWo&feature=autoplay&list=PLD70B32DF5C50A1D7&playnext=1 Как оставаться в безопасности на YouTube http://www.youtube.com/watch?v=3Ap1rKr0RCE&feature=relmfu Развлечения и безопасность в Интернете http://www.youtube.com/watch?v=AMCsvZXCd9w&feature=BFa&list=PLD70B32DF5C50A1D7&lf=autoplay

Остерегайся мошенничества в Интернетеhttp://www.youtube.com/watch?v=xRSnLKveMpY&feature=relmfu Мир глазами Gmail - ЗАЩИТА ОТ СПАМА)

Как не стать жертвой сети Интернет? Тема нашего урока - «Безопасный Интернет».

Главный вопрос урока: Как сделать работу в сети безопасной?

2. Изучение нового материала.

Игра «За или против».

Учитель предлагает игру «За или против». На слайде - несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

1. Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!

2. Интернет – это глобальный рекламный ресурс. И это хорошо!

3. Общение в Интернете – это плохо, потому что очень часто подменяет реальное общение виртуальному.

4. Интернет является мощным антидепрессантом.

5. В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Виртуальные грабли

Учитель предлагает обучающимся ответить на вопросы «Какие опасности подстерегают нас?», «Какие виртуальные грабли лежат у нас на пути?». (Целесообразно заранее нескольким обучающимся подготовить короткие сообщения по темам: «Интернет-зависимость», «Вредоносные и нежелательные программы», «Психологическое воздействие на человека через Интернет», «Материалы нежелательного содержания», «Интернет-мошенники»).

Физ. минутка «Собери рукопожатия».

Участникам предлагается в течение 10 секунд пожать руки как можно большего числа других людей.

Обсуждение.

- Кому сколько человек удалось поприветствовать? У кого-то возник психологический дискомфорт? Если – да, то чем он был вызван?

Анализ ситуации.

Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия? Однако,

очень важно знать, что есть рядом люди, готовые выслушать, оказать поддержку, помочь в трудную минуту.

Учитель предлагает ответить на главный вопрос урока – «Как сделать работу в сети безопасной?»

3. Практическая работа.

- Что можно? Что нельзя? К чему надо относиться осторожно?

Обучающимся предлагается посмотреть ресурсы http://content-filtering.ru/aboutus, http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_rooma.html, http://www.youtube.com/watch?v=y37Ax5TPc3s&feature=related.

Учитель спрашивает, что об этом можно прочитать на web-страницах и просит обучающихся сформулировать правила безопасной работы.

Резюме (обсуждение найденной информации). Какие правила безопасной работы выбрали обучающиеся, посещая web-сайты?

4. Закрепление изученного материала.

Интернет – это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен. Попробую сформулировать некоторые простые рекомендации, используя хорошо известные образы.

Современный Интернет – это не только обширная, но и настраиваемая среда обитания! В нем хорошо тому, кто может обустроить в нем собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео, включайте в друзья людей, которым вы доверяете. Тогда вместо

бессмысленного блуждания по сети ваше Интернет-общение будет приносить пользу.

Рефлексия. На данном этапе предлагается подвести итоги урока Интернет-безопасности: на столе лежат три смайлика, обучающимся необходимо выбрать и положить перед собой тот, который соответствует настроению школьника.

И помните, Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!

Оценивание обучающихся.

Информация о домашнем задании, инструкция о его выполнении:

1. Дать определение понятию «информационная безопасность».

2. Составить информационный лист «Моя безопасная сеть».

Приложение 8

Примерные материалы итогового анкетирования обучающихся по теме "Безопасный Интернет"

1. Укажите свой возраст_____
2. Что такое Интернет?_____
3. Какие опасности существуют в Интернете?_____

_____

_____

4. Использование Интернета является безопасным, если: * выберите один или несколько вариантов из списка ответов

a) защитить свой компьютер, защитить себя в Интернете, соблюдать правила

b) разглашать личную информацию, заботиться об остальных, регулярно обновлять операционную систему

c) защитить компьютер, создавать резервные копии документов, закону надо подчиняться даже в Интернете

5. Как защитить себя в Интернете? * выберите один или несколько вариантов из списка ответов

a) защитить свой компьютер, расширять круг знакомств с неизвестными людьми

b) стараться давать как можно меньше информации о себе

c) размещать фотографии свои, друзей и родственников

6. Как обезопасить свой компьютер? * выберите один вариант из списка ответов

a) выключить и спрятать в шкаф

b) установить антивирусную программу

7. Что надо делать, чтобы антивирусная программа была эффективной *выберите один или несколько вариантов из списка ответов

a) лучше не иметь антивирусную программу

b) обновлять антивирусную базу

c) не посещать сайты, где нет достоверности, что сайт находится под защитой

8. Кто создаёт опасные программы? * выберите один или несколько вариантов из списка ответов

a) чёрный властелин

b) хакеры

c) шпионы

d) пожиратели смерти

9. Перечислите правила поведения в Интернете * если вы не знаете ответа на этот вопрос, то напишите "Без ответа"_____

_____

10.А что для вас является "Безопасным Интернетом?" * если вы не знаете ответа на этот вопрос, то напишите "Без ответа"_____

_____

Приложение 9

Сказка о золотых правилах безопасности в Интернет

В некотором царстве, Интернет- осударстве жил-был Смайл-царевич-Тьютор-Королевич, который правил славным городом СоцОБРАЗом. И была у него невеста– прекрасная Смайл-царевна-Он-лайн-Королевна, день и ночь проводившая в виртуальных забавах. Сколько раз предупреждал её царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл-царевич, возводя город СоцОБРАЗ, заботился об охране своих границ и обучал жителей города основам безопасности жизнедеятельности в Интернет-государстве. И не заметил он, как Интернет-паутина всё-таки затянула Смайл-царевну в свои коварные сети. Погоревал –

да делать нечего: надо спасать невесту. Собрал он рать королевскую-СоцОбразову – дружину дистанционную и организовал "Регату" премудрую.

Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они «Семь золотых правил безопасного поведения в Интернете», сложили их в котомку Смайл-царевичу, и отправился он невесту искать. Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: порно-сообщества Змея-искусителя-Горыныча, стрелялки-убивалки Соловья-разбойника, товары заморские купцов шоповских, сети знакомств-зазывалок русалочьих…

Как же найти-отыскать Смайл-царевну? Крепко задумался Тьютор-королевич, надел щит

антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную. Долго бродил он, отбиваясь от реклам шоповских зазывающих и спамов завлекающих. И остановился на распутье игрища молодецкого трёхуровневого, стал читать надпись на камне, мохом заросшим: на первый уровень попадёшь – времени счёт потеряешь, до второго уровня доберёшься – от родных-близких отвернёшься, а на третий пойдёшь - имя своё забудешь. И понял Смайл-царевич, что здесь надо искать невесту.

Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей разомкнувшихся Смайл - царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято

соблюдай наказы безопасные!»

Всегда помни своё Интернет-королевское имя (E-mail, логин, пароли) и не кланяйся всем подряд (не регистрируйся везде без надобности)!

Не поддавайся ярким рекламам-указателям и не ходи тропками путанными на подозрительные сайты: утопнуть в трясине можно!

Если пришло письмо о крупном выигрыше – это «Лохотрон-грамота»: просто так выиграть невозможно, а если хочешь зарабатывать пиастры, нужно участвовать в полезных обучающих проектах – в «Регате…», например!

Чтобы не забыть тропинку назад и вернуться вовремя, бери с собой Клубок волшебный (заводи себе будильник, садясь за компьютер)!

Если хочешь дружить с другими царствами-государствами, изучай полезные социальные сервисы Web 2.0: они помогут тебе построить «Мой королевский мир», свой царский блог, форум для глашатаев важных – друзей званных.

Не забывай обновлять антивирусную программу – иначе вирус Серый Волк съест весь твой компьютер!

Не скачивай нелицензионные программные продукты – иначе пираты потопят твой корабль в бурных волнах Интернета!

Залилась совестливыми слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего СоцОБРАЗа, сама начнёт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой.

И зажили они дружно и счастливо с мечтою расширить границы образовательные.