Министерство образования и молодежной политики Свердловской области
Государственное автономное образовательное учреждение
дополнительного профессионального образования Свердловской области
«Институт развития образования»

Проведение Единого урока безопасности в сети «Интернет»

Методические рекомендации для педагогов общеобразовательных организаций

Екатеринбург
2019

ББК 74.200я81
П 79

Авторы - составители:
О. А. Богословская, кандидат сельскохозяйственных наук, заведующий учебно-методическим кабинетом ГАОУ ДПО СО «ИРО»;
М. А. Герасимова, кандидат педагогических наук, заведующий кафедрой педагогики профессионального образования ГАОУ ДПО СО «ИРО».

П 79 Проведение Единого урока безопасности в сети «Интернет»: методические рекомендации / Министерство образования и молодежной политики Свердловской области, Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования»; авт.-сост. О. А. Богословская, М. А. Герасимова. – Екатеринбург: ГАОУ ДПО СО «ИРО», 2019. – 27 с.

Данное издание включает рекомендации педагогам по проведению ежегодного Единого урока безопасности в информационно-телекоммуникационной сети Интернет, проводимого в рамках плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы. В издании использованы материалы ГАОУ ДПО СО «ИРО» по формированию информационно-безопасной среды в образовательных организациях, разработанные для педагогов Свердловской области и используемые в процессе реализации дополнительных профессиональных программ.

ББК 74.200я81

Содержание

Введение 3

Нормативно-правовые основания предотвращения угроз безопасности детей в современной информационной среде 4

Деятельность педагогов по обеспечению информационной безопасности 9

Организация уроков информационной безопасности в школе 14

Особенности организации урока информационной безопасности в начальной школе 16

Методические рекомендации по организации урока информационной безопасности в основной школе 19

Методические рекомендации по организации урока информационной безопасности для старшеклассников 23

Библиографический список 26

Введение

В соответствии с решениями парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», прошедшими 17 апреля 2017 года в Совете Федерации, и планом мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы, утверждённого приказом Минкомсвязи России №88 от 27.02.2018, в образовательных и воспитательных организациях Российской Федерации ежегодно с 2014 года осенью проводится Единый урок по безопасности в сети «Интернет».

Единый урок представляет собой цикл мероприятий для детей, обучающихся с участием педагогов, родителей, социальных партнеров, направленных на повышение уровня их информационной безопасности, а также на привлечение внимания родительской и педагогической общественности к проблеме обеспечения безопасности и развития детей в информационном пространстве.

Именно формирование информационной и цифровой грамотности детей и подростков является одним из важнейших факторов обеспечения их информационной безопасности. Информационная безопасность детей, подростков, молодежи является основой не только в сохранении информационного суверенитета нашей страны и формирования всех сфер информационного общества, но и обеспечения развития цифровой экономики.

Единый урок, включая его мероприятия и информационно-методический контент по его проведению, ориентирован на возраст детей и подростков с 5 до 19 лет, что позволяет организовать обучение информационной безопасности и цифровой грамотности детей разного возраста. Единый урок направлен на участие в нем детей старшего дошкольного возраста, младших школьников, обучающихся основной школы, старшей школы и обучающихся по программам среднего профессионального образования в профессиональных образовательных организациях.

Единый урок является одним из крупнейших мероприятий в сфере детства. Благодаря его систематическому проведению, а также реализации других программ по повышению уровня знаний школьников в сфере информационной безопасности информационная культура и цифровая грамотность российских детей растет с каждым годом [1].

При подготовке методических рекомендаций были использованы материалы ГАОУ ДПО СО «ИРО», разработанные для педагогов Свердловской области и используемые в процессе реализации дополнительных профессиональных программ (авт. Л. И. Долинер, Г. А. Бутакова, Е. В. Ахлестина, Т. А. Сундукова, Д. Е. Щипанова, Н.В. Шпарута, Н. Ю. Сероштанова,), а также материалы И. А. Волковой И.А. (МАОУ Лицей № 130, г. Екатеринбург).

Нормативно-правовые основания предотвращения угроз безопасности детей в современной информационной среде

Согласно Федеральному закону, информационная безопасность детей – состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию [2]. Кроме того информационная безопасность детей в рамках Концепции рассматривается в двух направлениях:

– защита ребенка от дестабилизирующего воздействия информационной продукции;

– создание условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия [3].

Угрозу информационной безопасности обучающихся в Интернете, прежде всего, представляет информация, не предназначенная для детей. В Интернете, как и в реальной жизни, учащихся подстерегают опасности: доступность нежелательного контента в социальных сетях, обман и вымогательство денег, платные СМС на короткие номера, пропаганда насилия и экстремизма, игромания и интернет-зависимость, склонение к суициду и т.п.

Довольно распространенной угрозой для обучающихся является общение в Интернете с незнакомыми людьми. Очевидно, что обучающиеся пренебрегают своей безопасностью в этой сфере. Согласно опросам некоторые дети регулярно переносят виртуальные контакты в реальную жизнь. Таким образом, встречи с интернет-знакомыми представляют для школьников определенный риск. В наибольшей степени это характерно для старшеклассников.

Ряд угроз в равной степени актуален для подростков любого возраста, у них взламывают страницы в социальных сетях, они также часто сталкиваются с оскорблениями, угрозами, распространением персональных данных без их согласия. Несмотря на то, что практически все школьники встречались в Интернете с определенными рисками, большинство из них, вне зависимости от возраста, рассматривают интернет-пространство как безопасное для себя.

Интернет становится неотъемлемой частью жизни современных подростков, они воспринимают его как естественное пространство общения и жизнедеятельности и, возможно, поэтому могут недооценивать риски, проявлять рискованное поведение.

При этом чем старше подростки, тем более они уверены в собственной безопасности в Интернете, что, вероятно, обусловлено уверенностью в своих навыках использования Интернета и самоидентификацией со взрослыми пользователями. Таким образом, представляется, что рискованное поведение подростков в Интернете может быть обусловлено излишней уверенностью в своих силах и стремлением проявить свою самостоятельность.

Чем более активными пользователями являются подростки, чем больше времени они проводят в Интернете, тем в большей степени они подвержены действию различных интернет-угроз. Важно акцентировать внимание школьников, особенно старшего подросткового возраста, что в интернет-пространстве, как и в реальной жизни, существуют угрозы, которым в равной степени подвержены и взрослые, и дети.

При возникновении различных сложных, опасных ситуаций в Интернете важно, чтобы подростки знали, как следует вести себя, и к кому они могут обратиться за помощью. Вместе с тем при возникновении подобных ситуаций школьники предпочитают справляться с ними самостоятельно, особенно это характерно для старшеклассников [4].

Доступ несовершеннолетних к сайтам в сети «Интернет» дает им возможность изучать образовательный контент, общаться с ровесниками, самостоятельно обучаться, узнавать о проводимых конкурсах, олимпиадах, принимая в них участие, и использовать сеть «Интернет» в качестве источника для собственного развития.

Однако использование интернета вместе с возможностями несет и риски. Прежде всего, это:

– издевательство ровесниками и незнакомцами в сети над ребенком, травля (буллинг);

– воровство его аккаунтов, денег и личных данных;

– втягивание ребенка в асоциальную деятельность (группы смерти, группы с рекламой наркотиков и т.д.);

– прочтение детьми информации, вредящей их мировоззрению и психотическому состоянию [5].

В целях ограничения доступа к сайтам в сети «Интернет», содержащим информацию, распространение которой в Российской Федерации запрещено, создана единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (далее - реестр).

В него включаются доменные имена и (или) указатели страниц сайтов в сети «Интернет», содержащих информацию, распространение которой в Российской Федерации запрещено; сетевые адреса, позволяющие идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

Основаниями для включения в реестр сведений по состоянию на сентябрь 2019 г. являются:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети "Интернет":

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года N 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона от 11 ноября 2003 года N 138-ФЗ "О лотереях" о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети «Интернет» и иных средств связи;

е) информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции;

ж) информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц;

2) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети «Интернет», информацией, распространение которой в Российской Федерации запрещено;

3) постановление судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети «Интернет», порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица [6].

Федеральный закон от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» определяет перечень запрещенной для детей информации, возрастные категории детей и виды информации, разрешенной для той или иной категории, а также требования к обороту информационной продукции.

К информации, запрещенной для распространения среди детей, относится информация:

1. побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
2. способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
3. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4. отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

5. оправдывающая противоправное поведение;

6. содержащая нецензурную брань;

7. содержащая информацию порнографического характера;

8. о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

Оборот такой информации не допускается среди детей в местах, доступных для детей, без применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от такой информации.

Особая категория информации, к которой доступ ограничен для определенных возрастных категорий:

1. представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

2. вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Распространение вышеуказанных категорий информации допускается среди детей определенных возрастных групп при соблюдении обладателем информации установленного законом порядка доступа детей к информации (в частности, при условии, что в информационной продукции содержится идея торжества добра над злом, сострадание к жертве насилия, осуждение насилия, а изображение и описание насилия, жестокости, антиобщественных действий носит ненатуралистический, кратковременный или эпизодический характер и т.п.).

Законом также закреплена обязанность классификации информации по пяти возрастным категориям:

1. информационная продукция для детей, не достигших возраста шести лет;

2. информационная продукция для детей, достигших возраста шести лет;

3. информационная продукция для детей, достигших возраста двенадцати лет;

4. информационная продукция для детей, достигших возраста шестнадцати лет;

5. информационная продукция, запрещенная для детей [2].

Деятельность педагогов по обеспечению информационной безопасности

Задача педагогов в связи с имеющимися рисками состоит в том, чтобы воспитать у детей, обучающихся культуру безопасного использования Интернет, в том числе, педагогу необходимо:

– указать на риски необдуманного использования Интернет детям, родителям;

– сформировать у детей осознанное отношение к использованию ресурсов Интернет, предостеречь обучающихся от необдуманных поступков, сформировать у учащихся навыки критического отношения к получаемой в Интернете информации;

– формировать культуру общения в сети Интернет.

Со стороны всех учителей необходима пропаганда информационной культуры по использованию ресурсов Интернета для всех субъектов образовательного процесса, всех участников образовательных отношений. От каждого педагога зависит актуализация вопросов использования программного обеспечения родительского контроля, ограничения времени доступа детей к Интернету.

Формирование информационной безопасности обучающихся будет эффективным, если педагогическая деятельность будет основана на следующих положениях:

- информационно-личностная безопасность учащегося рассматривается как компонент информационной компетенции, и каждый педагог в рамках своей деятельности функционально обеспечивает управление информационными угрозами;
- в содержание образовательных программ включается дидактический компонент; в учебных программах содержится учебный материал об информационных угрозах, признаках негативного воздействия на личность, правила работы с информацией, приемы проблемного обучения и развития критического мышления и т.п.

Деятельность классных руководителей и учителей-предметников

Наиболее распространенной формой работы по обеспечению информационной безопасности в Интернете классных руководителей с обучающимися является проведение тематических уроков, классных часов и индивидуальных бесед по вопросам информационной безопасности обучающихся в Интернете.

Чаще всего классные руководители для обеспечения информационной безопасности в Интернете рассказывают обучающимся о правонарушениях в Интернете, обучают распознавать мошеннические сообщения, разговаривают с учениками о том, что следует делать в случае столкновения с трудными/неприятными ситуациями в Интернете (оскорблениями, шантажом, правонарушениями, травлей и т. д.), а также рассказывают о возможностях Интернета для обучения, общения, показывают полезные сайты.

Современные подростки располагают достаточно полной информацией о том, как защититься от таких угроз, как вирус, спам, навязчивая реклама. Очень многие из них зачастую лучше, чем взрослые, разбираются в технической стороне вопроса.

Вместе с тем, дети не готовы противостоять угрозам, исходящим от реальных людей и связанным с оскорблениями и унижениями. У них отсутствуют четкие установки, не сформированы определенные стереотипы поведения в подобных ситуациях. У многих учащихся отсутствует также представление о том, что деятельность, которая осуществляется в Интернете, становится одной из сторон реальной жизни современного человека, на которую распространяются нормы поведения, принятые в обществе.

Именно на эти вопросы предлагается обратить внимание и классных руководителей, и других специалистов, занимающихся вопросами воспитания в целом и информационной безопасности обучающихся в частности.

Главными направлениями работы педагогов и родителей по обеспечению информационной безопасности обучающихся являются обеспечение безопасности информационной среды для обучающихся и развитие личностных установок и навыков безопасного поведения обучающихся в Интернете.

В школе создаются условия для организации возможности использования Интернет ресурсов на уроках и во внеурочное время. Информационная политика учебных учреждений, как правило, жестко регламентируется. То есть учителя не имеют возможности самостоятельно устанавливать на школьные компьютеры различные программы и производить настройки. Вместе с тем, учителя-предметники должны иметь представление о безопасном использовании Интернета для возможного изменения информационной политики своей образовательной организации и для рекомендаций при общении с родителями учеников. В общеобразовательных организациях должен реализовываться комплекс мероприятий по обеспечению исключения доступа обучающихся к ресурсам Интернета, содержащим информацию, несовместимую с задачами образования и воспитания, в том числе и с личных устройств.

Рекомендации по работе с обучающимися начальных классов

1. Перед первым выходом вашего ученика в Интернет как можно четче оговорите правила пользования сетью. Обсудите с ребенком, куда ему можно заходить (возможно, на первых порах стоит составить список сайтов), что можно и что нельзя делать, сколько времени можно находиться в Интернете.
2. Сообщите ему о том контроле, который Вы намерены осуществлять: проверка посещенных ребенком страниц, контроль времени, проведенного в Сети, проверка адресов электронной почты. Объясните ребенку, что вы доверяете ему и заботитесь о его безопасности.
3. Договоритесь с ребёнком о соблюдении им следующих правил:

- сообщить родителям свое регистрационное имя и пароль; если ребенку разрешено участвовать в чатах или блогах, то e-mail адрес и пароль почтового ящика;
- никому, кроме родителей, эти сведения сообщать категорически нельзя;
- не сообщать без разрешения родителей для каждого отдельного случая личную информацию (домашний адрес, номер телефона, номер школы, место работы родителей);
- не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через Интернет;
- сразу обратиться к родителям, если ребенок увидит нечто неприятное, тревожащее, угрожающее на сайте или в электронной почте;
- не соглашаться лично встретиться с человеком, с которым ребенок познакомился в сети;
- если кто-то предлагает ребенку какой-то необычный «секрет» - тут же сообщить об этом родителям;
- не скачивать, не устанавливать, не копировать ничего с дисков или из Интернета без разрешения родителей на каждый отдельный случай;
- не делать без разрешения родителей в Интернете ничего, что требует оплаты;

– проявлять уважение к собеседникам в Интернете, вести себя так, чтобы не обидеть и не рассердить человека.

4. В течение некоторого времени сопровождайте ребенка в его путешествиях по сети для того, чтобы убедиться, что ребенок соблюдает ваш уговор.

5. Периодически проверяйте в браузере журнал посещённых ребёнком Интернет-страниц. Конечно, журнал можно очищать, но не всякий ребёнок умеет это делать.

Большое значение для эффективности мероприятий по Интернет-безопасности имеет не только содержание, но и форма его проведения.

Для обучающихся начальной школы целесообразно использовать следующие формы: урок-путешествие, урок-викторину, урок-соревнование, урок-игру, беседу, можно организовать решение проектной задачи по данному вопросу.

Учителю начальных классов для обучения своих воспитанников организации безопасной работы в сети Интернет нужно:

– знать, какие опасности подстерегают ребенка в Интернете и его интересы в соответствии с возрастными особенностями,
– иметь каталог качественных дидактических сетевых или локальных электронных материалов по теме изучения,
– организовать интересную деятельность по освоению новых знаний и формированию умений безопасной работы в сети Интернет на уроке и во внеурочное время,
– обращать внимание родителей на проблему безопасности ребенка в сети Интернет.

Рекомендации по работе с обучающимися старших классов

Какое содержание выбрать для проведения занятий со старшеклассниками? К 10 классу обучающиеся часто информационно более подкованы, чем некоторые учителя. В рамках уроков информатики они изучают уже не только нормы сетевой этики, но и методы защиты информации, законодательное регулирование в информационной области. То есть обучающиеся обладают необходимыми знаниями. Вопрос в том, насколько школьники используют данные знания в повседневной жизни.

Поэтому в первую очередь уроки информационной безопасности в данном возрасте должны носить не информирующий, а деятельностный характер. Причем организация деятельности старшеклассников должна носить продуктивный характер. Эффективно использование проектной технологии.

Например, это может быть проект «Проблемы информационной безопасности. Касаются ли они лично меня?» или «Мифы информационной безопасности».

Введение в проблему проекта можно реализовать с помощью он-лайн анкеты. Обучающимся предлагается ответить на вопросы анкеты Гугл, предложенной учителем http://bit.ly/U5wDxE.

Отметим, что при заполнении анкеты ребятам нужно лишь выбрать подходящий ответ из предложенных. После того, как все обучающиеся отправят свои ответы, автоматически сформируется отчет в виде диаграмм, доступный для просмотра. Эти диаграммы педагог предлагает обучающимся для обсуждения.

Цель обсуждения с детьми – вместе определить готовность к современным киберугрозам. Скорее всего, результатом беседы станет выявление соответствующей проблемы. После обсуждения вариантов ее решения целесообразно объединиться в группы для разработки рекомендаций (памятки) по безопасному поведению в сети на основе мифов информационной безопасности [7].

Итак, на что нужно обратить особое внимание обучающихся при рассмотрении вопроса об Интернет безопасности? Сформулируем правила для обучающихся основной школы, которые педагог должен включить в работу с обучающимися:

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. Остерегайся «подделок».

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.

4. Соблюдай правила вежливости.

Хотя Интернет – это среда для общения, в ней существуют определенные специфическая правила вежливости. Их сейчас широко обсуждают в Интернете, но, к сожалению, в целом культура общения в Интернет-сети 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.

Организация уроков информационной безопасности в школе

Единый урок безопасности для детей возможно провести в следующих формах, которые могут быть использованы как самостоятельные формы, так и на основе их интеграции. Это могут быть:

1. Проведение традиционного урока, классного часа, деловой игры на основе предоставленных методических материалов или видеоматериалов, или проведение видео-урока;
2. Проведение семинара или занятия с участием приглашенного эксперта;
3. Проведение акций (разработка совместно с детьми и распространение листовок, флайеров, распространение через дневники обучающихся тематических материалов и др.).

Содержание занятий должно охватывать: технические, правовые и психологические аспекты информационной безопасности.

Единый урок может быть организован и с использованием сети «Интернет»:

1. Для обучающихся организована Всероссийская контрольная работа по информационной безопасности на портале Единого урока www.Единыйурок.дети. В ходе контрольной работы обучающиеся смогут не только проверить свои знания в различных областях информационной безопасности, но и получить именной сертификат в электронной форме;
2. Организация участия детей в VI международном квесте (онлайн-конкурсе) по цифровой грамотности «Сетевичок» позволят организовать полноценное дистанционное обучение детей основам информационной безопасности в игровой форме. Квест включает тематические курсы и викторины, опросы и

другие онлайн активности, за участие в которых начисляются баллы. Победителям квеста станут обучающиеся, набравшие максимальное количество баллов на уровне района, субъекта и Федерации. Все участники получают именные дипломы, а победители специальные призы от спонсоров и партнеров конкурса. Квест проходит на сайте www.Сетевичок.рф.

Федеральный молодежный проект «Сетевичок» реализуется в соответствии со следующими целями и задачами:

- формирование у молодого поколения киберкультуры и киберграмотности;
- обучение детей методам борьбы с негативом в сети;
- повышение уровня вовлеченности школьников в социально-активную деятельность;
- создание и развитие позитивного контента в Рунете;
- воспитание духовно-нравственных и культурных ценностей;
- повышение медиаграмотности среди детей.

Реализация Проекта включена Министерством образования и науки РФ в качестве обязательного мероприятия для всех образовательных учреждений общего и среднего профессионального образования России в рамках Единого урока по безопасности в сети «Интернет».

Участниками квеста могут быть учащиеся учреждений образования Российской Федерации, реализующие программы начального, общего, среднего и высшего профессионального образования; дети-сироты и дети, оставшиеся без попечения родителей; дети сотрудников российских компаний, предприятий и государственных учреждений.

Квест проходит в онлайн-формате, то есть без привязки к месту и времени, пройти его можно с любого устройства, имеющего выход в интернет. Обучающихся будут участвовать в онлайн-курсах, викторинах, конкурсах рисунков и эссе, выполнять тестовые задания и различные опросы.

По окончании обучающийся должен уметь анализировать достоверность сетевой информации и умение использовать полученную в сети «Интернет» информацию; оценивать и анализировать свои и чужие поступки и действия в сети «Интернет»; работать с возможностями, функционалом и рисками в сети «Интернет»; использовать информацию, полученную из разных источников, для решения учебных и практических задач [8].

Цифровая и медиаграмотность предполагает формирование и развитие пользовательских умений и установок на эффективную работу с информационными ресурсами, а также ответственное отношение к собственному поведению, основанное на осознавании последствий своих действий в интернет-пространстве.

Учитывая возрастные и психологические особенности обучающихся разных возрастных групп можно предложить следующие рекомендации по по проведению Единого урока безопасности в сети «Интернет».

Работа педагогов с родителями

В работе педагогов важное место занимает работа с родителями.

Предлагаем примерную содержательную структуру серии занятий, семинаров для педагогов (родителей) для развития цифровой компетентности

обучающихся, основанная на материалах методических пособий «Фонда Развития Интернет»:

Модуль 1. Технические аспекты использования Интернета
Тема 1. Цифровой образ жизни
Тема 2. Безопасное подключение
Тема 3. Надежные пароли
Тема 4. Вирусы в Интернете
Тема 5. Искусственный интеллект

Модуль 2. Информация в Интернете
Тема 1. Информация в Интернете: возможности и риски
Тема 2. Возможности поиска в Интернете
Тема 3. Достоверность информации в Интернете
Тема 4. Авторское право в Интернете

Модуль 3. Коммуникация в Интернете
Тема 1. Самопрезентация
Тема 2. Социальные сети
Тема 3. Друзья или френды
Тема 4. Агрессия в Интернете

Модуль 4. Цифровое потребление
Тема 1. Цифровое потребление
Тема 2. Реклама в Интернете
Тема 3. Мошенничество в Сети
Тема 4. Люди, которые играют в игры [9].

Особенности организации урока информационной безопасности в начальной школе

Реализация программы формирования УУД в начальной школе – ключевая задача внедрения нового образовательного стандарта. Отличительной особенностью начала обучения является то, что наряду с традиционным письмом ребенок сразу начинает осваивать клавиатурный набор текста. Ряд дисциплин начального образования позволяют привлекать использование Интернета для осуществления учебной деятельности. Изучение искусства предполагает изучение современных видов искусства наравне с традиционными, в частности, цифровой фотографии, видеофильма, мультипликации. В контексте изучения всех предметов должны широко использоваться различные источники информации, в том числе, в доступном Интернете.

В современной школе широко применяется проектный метод. Средства ИКТ являются наиболее перспективным средством реализации проектной методики обучения, а работа в Интернете позволяет ускорить и расширить процесс поиска информации.

Необходимо также учитывать психологические особенности ребенка этого возраста (7-8 лет). Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут делать без разрешения родителей. Поэтому, находясь в сети Интернет, ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Стоит учитывать, что дети в таком 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.

С 9 лет дети, как правило, уже имеют представление о том, какая информация есть в Интернете. Абсолютно нормально, что они хотят увидеть ее, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств родительского контроля.

По поводу использования электронной почты хотелось бы заметить, что детям такого возраста не рекомендуется иметь собственный электронный почтовый ящик, – они должны пользоваться семейным, чтобы родители могли контролировать переписку.

Дети этого возраста должны выходить в Интернет первоначально только под присмотром учителей или родителей на сайты, которые соответствуют возрасту и культурному развитию ребенка.

Важно настаивать, чтобы дети никогда не соглашались на личные встречи с друзьями из Интернета. Приучите детей не загружать программы без вашего разрешения, объяснив им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

Приведем описание некоторых интересных идей для реализации уроков и форм организации внеурочной деятельности по рассматриваемой теме.

Организовать проектную деятельность во внеурочное время можно участвуя вместе с обучающимися в сетевых проектах на сайте http://www.nachalka.com/. В разделе «Сетевые проекты» данного сайта описан план работы по проектам на очередной учебный год.

Под сетевым проектом на сайте понимают такую организацию проектной деятельности, которая подразумевает удаленное взаимодействие детей из разных уголков страны, объединенных общей темой, целью, формами работы, методами исследования.

Начиная такое взаимодействие, учитель обязательно должен зарегистрироваться вместе с детьми на сетевом ресурсе, в этом могут помочь родители. При регистрации на ресурсе уже в деятельности можно проговорить правила создания паролей в сети (понятие надежного пароля) и значения учетной записи для организации безопасной сетевой деятельности (зарегистрированный пользователь несет ответственность за созданный им контент). В процессе работы над проектом, общаясь в сети с ровесниками, обучающиеся понимают не на словах, а на деле важность и необходимость сетевого этикета.

Таким образом, работая по сетевым проектам можно не только получить опыт проектной деятельности, организовать площадку для совместной деятельности ребенка и родителя, получить новые предметные знания по предложенной в проекте теме, но и изучить не в теории, а на практике вопросы безопасности в Интернет.

В Интернете много тематических интересных видео, сетевых интерактивных ресурсов, игр, тестов. С помощью перечисленных ниже ресурсов в интересной форме можно организовать целенаправленную деятельность

учащихся на уроках и во внеурочное время по формированию полезных навыков безопасной работы в сети:

1. Интернет-игра по информационной безопасности http://igra-internet.ru/game. Много разных игр для всех возрастов. Требуется бесплатная регистрация.
2. Игра для детей 7-10 лет "Через Web джунгли". http://www.wildwebwoods.org/popup.php?lang=ru
3. «Основы безопасности детей и молодежи в Интернете» - интерактивный курс по Интернет-безопасности. http://laste.arvutikaitse.ee/rus/html/etusivu.htm.
4. Сказка о Колобке и Интернет-безопасность. Данный ресурс представляет WIKI-рассказ о безопасности в Интернете со вставленными анимационными картинками. В интересном формате ребенок может познакомиться с опасностями и способами защиты в сети.
5. Образовательный проект МТС «Дети в Интернете» http://detionline.com/mts/about в разделе «Уроки» предлагает дидактический материал для проведения урока - видео, презентацию, методическое пособие, брошюру для родителей, онлайн игру.
6. Правила Интернет-этикета для школьников http://chitalia.blogspot.com/2009/12/blog-post_6152.html.
7. На сайте Центра безопасности Google *в разделе «Ресурсы»* http://www.google.ru/intl/ru/safetycenter/ можно найти большой список полезных Интернет-ресурсов по данной теме
8. Проект «Разбираем Интернет» http://www.razbiraeminternet.ru/ рассказывает об устройстве электронного мозга сетевого пространства, дети узнают, как получить доступ к знаниям, находить нужную информацию, критически оценивать контент, создавать собственные Интернет-проекты, общаться — и делать все это, соблюдая простые правила безопасности.
9. Детский портал «Смешарики» www.smeshariki.ru, представляет цельную игровую развивающую среду, Детская социальная сеть Смешариков – Шарарам http://www.smeshariki.ru/auth.aspx представляет собой интерактивное образовательное пространство, где дети могут общаться друг с другом и получать полезные навыки, в том числе и в части правил безопасности в Интернете.
10. Твиди Интернет-портал для детей и подростков 6-16 лет http://www.tvidi.ru/ –онлайн-игры, виртуальные миры, форумы, конструктор комиксов, новости, чаты, социальная сеть, онлайн-кинотеатр, сервисы хранения фото-, видео- и аудиофайлов. Портал содержит советы и рекомендации по безопасному использованию Интернета.

Представим идею использования ресурса №4 предложенного выше списка - Сказка о Колобке и Интернет-безопасность на уроке или при организации внеурочного времени.

Дети знакомятся с отрицательными и положительными героями сказки, которые в сказке представлены анимированными картинками. Далее читают рассказ о приключениях героев.

После прочтения дети получают задание заполнить таблицу совместного редактирования, где классифицируют рассмотренные понятия и определяют роль каждого героя в сказке.

Таблица 1

Заполни таблицу В первой колонке представь всех героев сказки. А во второй колонке то, что Колобок тебе о них рассказал, а может что-то ты уже знал? Красным цветом окрась опасности, зеленым защиту, а синим нейтральные понятия	
Слова	Что и кто это Что делают для информационной безопасности

Итак, подведем итоги.

Учителю начальных классов для обучения своих воспитанников организации безопасной работы в сети Интернет нужно:

– знать какие опасности подстерегают ребенка в Интернете и его интересы в соответствии с возрастными особенностями,

– иметь каталог качественных дидактических сетевых или локальных электронных материалов по теме изучения,

– организовать интересную деятельность по освоению новых знаний и формированию умений безопасной работы в сети Интернет на уроке и во внеурочное время,

– обращать внимание родителей на проблему безопасности ребенка в сети Интернет.

Методические рекомендации по организации урока информационной безопасности в основной школе

Учитывая возрастные особенности аудитории необходимо уделять 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.

Проблемы подростка, 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, учитель 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 [10].

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» [11] предлагается следующая тематика проведения школьных мероприятий по медиабезопасности:

- Про вредные программы и Интернет-жуликов;
- «Вредные советы» в Сети;
- Как защититься от «охотника на детей»?;
- Про «вредные зелья»;
- Если в Интернете обижают…;
- Опасности общения в Сети;
- Полезный и безопасный Интернет;
- Угрозы компьютеру и деньгам;
- «Промывание мозгов» в Интернете;
- «Про это»: как не стать жертвой;
- «Игла» в Интернете;
- Киберунижение;
- Позитивный Интернет;

– Опасные программы и Интернет-мошенники;
– Экстремистская и террористическая пропаганда, секты;
– Сексуальная эксплуатация детей;
– Наркотики в Сети.

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 рекомендациях по проведению уроков «Безопасность в Интернете» в начальной и средней школе 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 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 разной информации, но инструмент создания нового, интересного и нужного не только ему, но и окружающим его в школе и дома людям, пространства. И в этом пространстве ребенок 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 ими же, 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 презентации проектов школьников как на классных часах, так и на уроках, в рамках программы которых выполнены эти проекты.

Если ребенок имеет опыт презентации проекта в сети, узнал, 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.

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, поместить в тематический 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».

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 поместить 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.

4. 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».

Методические рекомендации по организации урока информационной безопасности для старшеклассников

При изучении предмета «Информатика» на базовом уровне в общеобразовательных организация уделяют достаточное время для изучения правовых аспектов защиты информации. На углубленном уровне изучаются также современные методы защиты информации. Следует отметить, что некоторые школьники уже в старших классах начинают вести экономическую и профессиональную деятельность в сети Интернет, делая он-лайн покупки, оказывая информационные услуги. Они хранят «в облаке» свои файлы и данные, регистрируются на сайтах госуслуг, записываются на прием к врачу через Интернет, создают свои группы в сетевых сообществах. При этом информационные технологии развиваются очень быстро, а вместе с развитием технологий растет и количество угроз. И, конечно, ни один учебник информатики не успевает обновляться с такой же скоростью, что и информационная сфера. Поэтому совершенно необходимо дополнительное проведение занятий по информационной безопасности для старшеклассников. Это могут быть классные часы, внеурочные занятия, уроки проектной деятельности в рамках недели информационной безопасности.

Какое содержание выбрать для проведения занятий со старшеклассниками? К 10 классу обучающиеся часто информационно более подкованы, чем некоторые учителя. В рамках уроков информатики они изучают уже не только нормы сетевой этики, но и методы защиты информации, законодательное регулирование в информационной области. Т.е. обучающиеся обладают необходимыми знаниями. Вопрос в том, насколько школьники используют данные знания в повседневной жизни. Поэтому в первую очередь уроки информационной безопасности в данном возрасте должны носить не информирующий, а деятельностный характер. Например, это может быть проект «Проблемы информационной безопасности. Касаются ли они лично меня?» или «Мифы информационной безопасности».

Введение в проблему проекта можно реализовать с помощью он-лайн анкеты. Обучающимся предлагается ответить на вопросы анкеты Гугл, предложенной учителем http://bit.ly/U5wDxE.

Вопрос 1. Вам пришло письмо (далее идет текст письма, в ответ на которое убедительно требуют написать логин и пароль электронной почты) Каковы Ваши действия в ответ на это письмо?

Вопрос 2. Для чего, на Ваш взгляд, нужны зоны свободного доступа к Интернету (Free Wi-Fi)?

Вопрос 3. Установлена ли на Вашем смартфоне (планшете) антивирусная программа?

Вопрос 4. Являетесь ли Вы участником одной из соцсетей?

Вопрос 5. Какую информацию о Вас можно найти на Вашей странице в соцсети?

Необходимо отметить, что при заполнении анкеты ребятам нужно лишь выбрать подходящий ответ из предложенных. После того, как все обучающиеся отправят свои ответы, автоматически сформируется отчет в виде диаграмм, доступный для просмотра. Эти диаграммы педагог предлагает обучающимся для обсуждения. Цель обсуждения – определить нашу готовность к современным киберугрозам. К сожалению, на сегодняшний день уделяется недостаточно внимания информационной безопасности, поэтому скорее всего результатом беседы станет выявление соответствующей проблемы. После обсуждения вариантов ее решения целесообразно распределиться на группы для разработки рекомендаций (памятки) по безопасному поведению в сети на основе мифов информационной безопасности.

Обучающимся предлагается подтвердить или развенчать мифы информационной безопасности.

Миф 1. В сети я абсолютно анонимен...

– Вопросы: Возможна ли анонимность в сети? Что можно узнать обо мне, имея лишь ip-адрес? Какую информацию обо мне можно получить из Интернета?

– Материалы для изучения: «Система технических средств для обеспечения функций оперативно-розыскных мероприятий» http://ru.wikipedia.org/СОРМ, «Whois-сервисы» http://ru.wikipedia.org/wiki/WHOIS, http://ipgeobase.ru/, «Методы анонимности в сети», http://habrahabr.ru/post/190396/

Миф 2. Я не нарушаю закон.

– Вопросы: Что мне будет за нарушение авторских прав? Что нелицензионного есть на «моём» компьютере? Каковы могут причины проверки моего компьютера специальными органами?

– Материалы для изучения: «Новости по тегу «пиратство» от SecurityLab» http://link.ac/37a6, «Авторские права. Ответственность за нарушение авторских прав», http://bit.ly/U5fpk7, «Законодательство о пиратстве», http://bit.ly/1iDiXzB, «Антипиратский закон» http://ru.wikipedia.org/wiki/Федеральный закон от 2 июля 2013 года № 187-ФЗ.

Миф 3. Социальные сети - место общения.

– Вопросы: Что нельзя делать в социальных сетях и почему? Что нужно делать, если мою учётную запись «взломали»? Чем опасны социальные сети?

– Материалы для изучения: «Сайт «Одноклассники.ру» несет угрозу безопасности России» http://bit.ly/1pDUxO8, «Социальную сеть «ВКонтакте» признали пиратским сайтом», http://bit.ly/UHrIU6, «Социальные сети, психология, криминал и шпионаж. Что связывает?», http://bit.ly/1vynivz.

Миф 4. Я защищён антивирусом.

– Вопросы: Как выбрать антивирус? Как часто нужно обновлять антивирус? Можно ли отключать антивирус, если программа установки просит это сделать и почему? Достаточно ли просто удалить вирус? Кто еще, кроме меня может пострадать от моего «зараженного» компьютера?

– Материалы для изучения: «Securelist. Угрозы», http://www.securelist.com/ru/threats, «Качество антивирусной защиты и проблемы антивирусных программ», http://bit.ly/1n8tOD8, «Для чего используют ботнеты?», http://bit.ly/1vyDfCf, «Финансовые киберугрозы», http://bit.ly/1uzY7Xb.

Миф 5. Реклама - двигатель торговли.

– Вопросы: Нужно ли запретить рекламу? Нужно ли намеренно защищаться от рекламы и почему? Как защититься от скрытой рекламы и НЛП? Можно ли утверждать, что информация, размещенная на надежном сайте, является истинной?

– Материалы для изучения: «НЛП в действии», http://bit.ly/1lw6r4V, «Скрытая реклама - способ управления сознанием», http://re-port.ru/articles/36369/, «Информационная война», http://ru.wikipedia.org/Информационная война, «Информационные войны: правила и примеры», http://www.echo.msk.ru/blog/apopova/1273448-echo/

Вопросы для всех: Достаточно ли только технического обеспечения информационной безопасности? Зачем меня кому-то взламывать?

Результатом проекта может стать презентация или видеоролик, содержащий ответы на вопросы, а также правила безопасного поведения в информационной среде.

Предложенные материалы также допустимо использовать для организации дискуссий на основе предложенных педагогом материалов.

Полезные ссылки для подготовки урока информационной безопасности.

– Интернет-игра по информационной безопасности http://igra-internet.ru/game. Много разных игр для всех возрастов. Требуется бесплатная регистрация.

– «Основы безопасности детей и молодежи в Интернете» — интерактивный курс по Интерент-безопасности. http://laste.arvutikaitse.ee/rus/html/etusivu.htm

– «Лаборатория Касперского» для образования http://academy.kaspersky.ru.

– Securelist (современные угрозы, аналитика, статистика, глассарий, описания и блог от «Лаборатории Касперского») http://www.securelist.com/ru.

– VirusTotal (https://www.virustotal.com/) - бесплатный сервис, анализирует подозрительные файлы и веб-сайты и облегчает быстрое обнаружение вирусов, червей, троянов и всех видов вредоносных программ.

– Всероссийский конкурс социальной рекламы в форме видеороликов и плакатов «Безопасный Интернет - детям». Работы победителей. http://www.fid.su/projects/saferinternet/year/photovideo.

– Все о безопасном Интернете (очень много ссылок на полезные ресурсы) на Информационном портале школьных библиотек России http://www.rusla.ru/rsba/technology/safety.

– Сайт фонда развития Интернет - Дети России Онлайн http://www.detionline.com.

- сайт Фонда Развития Интернет http://www.fid.su/projects/deti-v-internete
- Лига безопасного Интернета http://www.ligainternet.ru/
- сайт Центра безопасности Майкрософт http://www.microsoft.com/ru-ru/security/default.aspx
- сайт Ростелеком «Безопасноть детей в Интернете, библиотека с материалами, памятками, рекомендациями по возрастам http://www.safe-internet.ru/
- онлайн интернет-игра «Изучи Интернет – управляй им» http://www.igra-internet.ru/ [7].

Материалы по информационной безопасности также разработаны и представлены на сайте ГАОУ ДПО СО «ИРО» на сайтах кафедры информационных технологий (irro.ru/index.php?cid=148) и кафедры воспитания и дополнительного образования (irro.ru/index.php?cid=352).

Библиографический список

1. Онлайн-площадка для проведения Единых уроков [Электронный ресурс] / Режим доступа: https://www.единыйурок.рф/index.php/proekty/urok (дата обращения: 23.09.2019)
2. «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс]: федеральный закон от 29.12.2010 № 436-ФЗ // Официальный сайт компании «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 24.09.2019)

3. «Об утверждении Концепции информационной безопасности детей» [Электронный ресурс]: распоряжение Правительства РФ от 02.12.2015 N 2471-р // Официальный сайт компании «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_190009/ (дата обращения: 24.09.2019)
4. Методические рекомендации для педагогов и родителей по повышению уровня информационной безопасности детей по итогам социологического исследования проблемы «Деятельность подростков в сети Интернет: динамика, риски, реакция родителей» [Текст]: метод. рекомендации / Л. И. Долинер [и др.]; М-во образования и молодежной политики Свердловской области; Гос. автоном. образоват. учреждение доп. проф. образования Свердловской области «Институт развития образования». – Екатеринбург: ГАОУ ДПО СО «ИРО», 2019. – 55 с.
5. Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учетом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности [Электронный ресурс]: методические рекомендации // Онлайн-площадка для проведения Единых уроков. – Режим доступа: https://www.единыйурок.рф/images/doc/metod/cyber.pdf (дата обращения: 24.09.2019)
6. «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]: федеральный закон от 27.07.2006 г. № 149-ФЗ (с изменениями и дополнениями) // Информационно-правовой портал «Гарант.ру».– Режим доступа: http://base.garant.ru/12148555/87f87c00c1712306229db52e8e9eb87b/#ixzz60QbLJm9I (дата обращения: 24.09.2019)
7. Информационная безопасность обучающихся в современной информационной среде [Текст]: метод. рекомендации / Н. В. Шпарута [и др.]; М-во общего и профессионального образования Свердловской области; Гос. автоном. образоват. учреждение доп. проф. образования Свердловской области «Институт развития образования». – Екатеринбург: ГАОУ ДПО СО «ИРО», 2017. – 67 с.
8. Международный квест (онлайн-конкурс) по цифровой и медиа-грамотности для детей и подростков «Сетевичок» [Электронный курс] // Официальный сайт. – Режим доступа: http://сетевичок.рф/index.php (дата обращения: 24.09.2019)
9. Интернет: возможности, компетенции, безопасность: метод. пособие для работников системы общего образования [Электронный ресурс] / Г. Солдатова [и др]. – М.: Google, 2013. – 165 с. – Режим доступа: http://www.razbiraeminternet.ru/files/book_theory.pdf (дата обращения: 24.09.2019)
10. Методические рекомендации по проведению уроков «Безопасность в интернете» в начальной и средней школе [Электронный ресурс]: метод. рекомендации / Н. И. Комарова. – Режим доступа: http://liceum165nn.ru/DswMedia/metodichkadlyaprovedeniyaurokapobezopasnogointerneta.pdf (дата обращения: 26.09.2019)

11. Центр безопасного Интернета [Электронный ресурс]: Интернет-СМИ «Национальный узел Интернет-безопасности. – Режим доступа: http://www.saferunet.ru (дата обращения: 24.09.2019)