МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования «Алтайский государственныйгуманитарно-педагогический университет имени В.М. Шукшина»
(АГГПУ им.В.М.Шукшина)

Институт естественных наук и профессионального образования
Кафедра математики, физики, информатики

Направление подготовки 44.03.01 Педагогическое образование
Профиль подготовки Информатика

Методические материалы по обучению безопасной работы в сети Интернет учащихся 7-9 классов

Выпускная квалификационная работа

Допустить к защите

Зав. кафедрой математики,

физики, информатики

«_____»_____20___г.

Захаров П.В.

_____

(подпись)

Выполнил студент

_____Ф-ZИ141группы

_____Чувьюрова_____

фамилия

_____Светлана Сергеевна____

имя, отчество

_____

подпись

Научный руководитель

канд. пед. наук, доцент_____

ученая степень, ученое звание

Старовикова И.В._____

фамилии, И.О.

_____

подпись

Оценка

_____

« ___»_____20___г.

_____

подпись председателя ГЭК

Бийск – 2019

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Алтайский государственный гуманитарно-педагогический университет имени В.М. Шукшина» (АГГПУ им.В.М.Шукшина)

АННОТАЦИЯ

на выпускную квалификационную работу бакалавра

студента Чувьюровой Светланы Сергеевны группыФ-ZИ141

Направление подготовки 44.03.01 Педагогическое образование

Профиль Информатика

Тема Методические метериалы по обучению безопасной работы в сети Интернет учащихся 7-9 классов.

Abstract: the paper is devoted to one of the urgent problems of teaching Informatics techniques - the formation of students ' knowledge and skills of safe work on the Internet in the basic course of Informatics and ICT.

Analysis of scientific and educational literature showed that currently there are several definitions of the concept of" information security "developed methods and tools to ensure the safe operation of the user on the Internet, offered various methods and techniques of formation of students' knowledge and skills for safe work on the network. Textbooks on Informatics and ICT for grades 7-9 present basic concepts on this topic and provide some recommendations for students.

The approach to solving this problem in the framework of teaching activities should include comprehensive measures: consideration of the problem in the organization of the term and extracurricular activities of students, the organization of interaction with parents of students. The paper presents methodological developments, including two extracurricular activities for students and parent-teacher meeting on this topic.

Keywords: information security, safe work of students on the Internet in the educational process in Informatics and ICT at school.

АвторВКР _____ Чувьюрова Светлана

Оглавление

Введение

В нашей жизни сеть Интернет настолько широко распространенна, что стали частью нашей жизни. Информационные технологии развиваются очень быстро. Появляются новые технологии, которые стремительно входят в нашу жизнь. Сейчас уже трудно представить всю нашу жизнь без мобильных телефонов, интересных и полезных сетевых приложений, электронной почты. Все в свободном доступе получаем любую информацию и в тоже время не задумываемся о том, насколько безопасна всемирная паутина. Даже в учебном процессе невозможно представить работу учителя и обучающихся без применения различных интернет технологий. Компьютерные технологии обязательно предполагают работу в социальных сетях. На сегодняшний день проблема обеспечения безопасной работы в сети Интернет является не новой, однако, на практике учителя часто сталкиваются с небезопасным контентом, представляемым некоторыми даже рекомендованными сайтами. Причинами этому могут служить, как различного рода атаки на сайты, так и вирусная активность на компьютере. Последний пример является очень распространенным, поскольку компьютеры в школе являются общедоступными. Но и это еще не все угрозы, которые могут ожидать учителей и учащихся, как во время образовательного процесса, так и в домашних условиях. Значительно быстро увеличивающийся информационный поток в школьных и внешкольных источниках и неспособность усвоения ее человеком в период школьного обучения представляет перед нами задачу, сформировать у учащихся умение выбирать из различных источников необходимую информацию, для этого нужно разработать методические материалы по работе безопасной сети Интернет. В современном информационном обществе сознание обучающимися важности обеспечения безопасности детей в Интернете и ее решения для будущего социума и образования нужно формировать, как отмечают многие исследователи данной проблемы, в образовательной деятельности школьных

предметов, включая курс “Информатика и ИКТ”, с использованием всех возможных педагогических технологий и применять различные формы и методы во внеурочной деятельности. В дидактике и частных методиках исследованию проблемы уделено особое внимание, однако полностью все ее аспекты не проработаны, что обуславливает актуальность исследования.

Объектом исследования является обеспечение пользователям возможности безопасной работы в сети интернет.

Предметом исследования является развитие у учащихся 7-9 классов навыков по безопасной работе в сети Интернет в рамках дисциплины «Информатика и ИКТ».

Целью исследования является разработка методических материалов для учащихся 7-9 классов по обеспечению безопасной работы в сети Интернет.

Для этого необходимо выполнить несколько **задач**:

1. проанализировать научную и методическую литературу по данной проблеме;
2. провести анализ содержания учебников для учащихся 7-9 классов по информатике и ИКТ;
3. разработать методические материалы для учащихся с 7-9 класс по обеспечению безопасной работе в сети Интернет в дополнение к базовому курсу информатики;
4. разработать рекомендации для родителей учащихся.

Методы исследования: анализ научной и учебно-методической литературы.

Практическая значимость: применение разработанных материалов будет полезно использовать в практической работе учителям информатики средних школ.

Глава 1 . Проблема обеспечения безопасной работы учащихся в сети Интернет как одна из актуальных проблем учебного процесса школы

1.1. Понятие информационной безопасности учащихся

Интернет – гигантская всемирная компьютерная сеть, объединяющая десятки тысяч сетей всего мира. Её назначение — обеспечить любому желающему постоянный доступ к любой информации. Интернет предлагает практически неограниченные информационные ресурсы, полезные сведения, учёбу, развлечения, возможность общения с компетентными людьми, услуги удалённого доступа, передачи файлов, электронной почты и многое другое. Интернет обеспечивает принципиально новый способ общения людей, не имеющий аналогов в мире [5]. Однако, как показала практика, используя сеть интернет необходимо заботиться о безопасности работы. Понятие информационной безопасности появилось относительно недавно. Существует несколько определений данного понятия.

Информационная безопасность – состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной среде. Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации [5].

Понятие информационной безопасности представляется нам в различных источниках - словарях, статья, учебниках. Автор статьи Склямина М.Ю. «Обеспечение информационной безопасности учащихся в системе общего образования», дает такое определение: «информационная безопасность – жизненно необходимое условие обеспечения интересов человека, общества и государства. И начинается эта безопасность со стен общеобразовательных учреждений. Взращивать компетентность учащегося в мире опасностей и способах защиты от них – необходимое условие безопасности жизнедеятельности на уроках и во внеурочной деятельности самими педагогами» [32].

Понятие «Информационная безопасность» сегодня трактуется как в широком, так и в узком смысле. В широком смысле данное понятие трактуется как состояние общества, при котором обеспечена надёжная и всесторонняя защита личности, общества и государства от воздействия на них особого вида угроз, выступающих в форме организованных информационных потоков и направленных на деформацию общественного и индивидуального сознания. В узком смысле это состояние безопасности информации и каналов передачи и приёма, а также организация защиты от применения противником информационного оружия в ходе боевых действий. Примечательно, что понятие в узком смысле трактуется с технической точки зрения, и является организационным средством обеспечения информационной безопасности в широком смысле. Необходимо рассматривать понятие информационной безопасности как информационную безопасность личности, которая включает в себя два этапа: безопасности формирующейся личности (информационную безопасность детей и учеников школы) и безопасность сформированной личности. Возможно также расширение состава информационной безопасности за счёт межгосударственной информационной безопасности [5].

Следовательно, в составляющие информационной безопасности включена информационная безопасность детей, (сформировавшейся) личности, общества, государства и международная безопасность. Учитывая данные составляющие, необходимо предложить методические рекомендации и разработки по обучению в системе непрерывного образования с целью обеспечения информационной безопасности.

1.2. Основные риски и угрозы информационной безопасности в сети Интернет

Как показывают исследования, учащиеся пользуются социальными сетями не придавая значение серьезности и опасности использования ресурсов Интернет, устанавливают слабый к взлому пароль, заполняю все

поля, запрашиваемые системой, указывают свои конфиденциальные сведения и сведения о своих родных, открывают доступ своей страницы всем пользователям Интернета. Все приводит к тому, что учащиеся становятся уязвимыми и могут подвергаться различным угрозам. В своей работе Герасименко В.А. [16] выделяет несколько категорий угроз, к первой угрозе относятся финансовые махинации. При работе в сети Интернет, есть возможность столкнуться с различными опасностями. Опасность может возникнуть по причине деятельности сетевых мошенников. Основные цели мошенников могут заключаться в том, чтобы завладеть личной информацией пользователей сети Интернет. Заведомо зная о том, какие действия могут предпринять мошенники, есть возможность сократить к минимуму опасность быть обманутым ими. Популярной операцией мошенников является незаконное завладение денежными средствами пользователей сети Интернет. В основном, у мошенников есть возможность завладеть деньгами, которые хранятся на счетах в электронных платёжных системах или на банковских картах. Для проведения данной махинации, мошеннику необходимо завладеть ключевыми данными для доступа к личным счетам пользователя. К ключевым данным относятся логины и пароли для входа в личный кабинет платёжных систем, данные банковских карт, требуемые для выполнения платежей. Кроме хищения денежных средств мошенники зачастую создают подставные Интернет-магазины, которые предлагают купить определённые товары, стоимость которых определённо завышена. Покупатель, который приобрел такой товар, обычно не получает то, на что рассчитывал. В подставных Интернет-магазинах и на мошеннических порталах, посетителю рекомендуют купить какой-либо товар, совершить оплату посредством отправки SMS-сообщения. Чётко узнать сумму, списанную с мобильного телефона можно или из описания, которое было сделано продавцом, или после того, как будет произведено списание денежных средств со счёта. В Сети Интернет существует возможность столкнуться с множеством предложений, которые обещают получение большого дохода без вложений

или же с минимальными капиталовложениями. Нередко эти предложения относятся к рискованным способам дохода, при которых высока возможность потери инвестированных средств и минимальна вероятность получения дохода. Периодически такие предложения скрывают за собой обманные схемы. Ко второй угрозе относится кража данных учетных записей**.** Учётные записи пользователей Интернета также являются ценностями. Например, наиболее ценными можно назвать учётные записи от электронной почты. В большинстве случаев адреса электронных почт применяются для того, чтобы произвести подтверждения регистрации на других электронных сайтах. Многие сайты, которые предусматривают регистрацию, также поддерживают функцию восстановления пароля. При утрате пароля пользователь может воспользоваться возможностью восстановления пароля: на электронную почту, которую пользователь указал при регистрации, приходит письмо со старым паролем или со ссылкой на создание нового пароля. Если взломщик имеет доступ к почтовому ящику, то он может овладеть и другими учётными записями. В таких случаях у него есть определённые цели: воровство денег пользователя (учётные записи платёжных систем), и рассылка рекламы каких-либо товаров и услуг (учётные записи социальных сетей). К примеру, если взломщик будет иметь доступ к учётной записи в социальной сети, то у него будет возможность делать рассылку рекламы от имени пользователя. Чаще всего такая деятельность, спустя немного времени подавляется администраторами социальной сети. Во многих случаях другие пользователи замечают вредоносную рассылку и обращаются в администрацию социальной сети. Чтобы достигнуть своих целей, злоумышленники применяют вредоносные программы. Третья угроза - вредоносные программы. Согласно ст. 273 УК РФ [21] создание, применение и распространение вредоносных компьютерных программ уголовно наказуемо. Но по причине того, что злоумышленники действуют анонимно, остановить их очень сложно. Вредоносные программы применяются для воровства данных и денежных

средств пользователей. Также программы используют для вымогательства денег, для скрытого управления компьютером, для нарушения работы компьютерных систем. В Сети Интернет действует множество путей распространения этих программ. Например, мошенники делают сайты, после перехода на которые, на компьютер, не защищённый особым ПО, устанавливается вредоносная программа. Действия данной программы основываются на логике, предусмотренной её создателем. К примеру, программа имеет возможность просмотра файлов пользователя и отправки данных, содержащих информацию о паролях. Также, она имеет способность уничтожения данных, без которых работа компьютера невозможна. Программа способствует передаче тех текстов мошеннику, которые пользователь вводит с клавиатуры, а также и пароли. Подобная программа имеет способность блокировки ПК, при которой работа компьютера будет невозможна. При такой блокировке на экране компьютера выводится окно с предложением отправить платное SMS для разблокировки компьютера. Такой вид вымогательства денежных средств является самым классическим примером. Сайты мошенников часто имеют адреса, схожие с адресами популярных веб-сайтов – к примеру, адреса поисковых систем. Web-дизайн этих сайтов аналогично может быть похож на сайты, за которые они себя выдают. Если ошибиться при наборе адреса сайта, то можно случайно попасть на сайт мошенников. При работе в сети Интернет, всегда можно увидеть рекламу, призывающую пользователей нажать на неё. К примеру, рекламное изображение может иметь текстовое сообщение, в котором говорится о заражении компьютера пользователя вирусами, и чтобы излечить вирус, нужно пройти по рекламной ссылке. К такой рекламе нужно относиться с внимательностью, так как рекламные ссылки могут способствовать установке вредоносных программ на ваш компьютер. Зачастую программы злоумышленников применяются с помощью электронной почты или программ для общения пользователей друг с другом (Skype). Текстовые сообщения могут содержать вредоносную программу,

которая содержится в виде файла или же, содержать ссылку на страницу, при переходе по которой ПК будет заражён. В современном мире сайты и программы для обмена сообщений между пользователями являются основными методами распространения вредоносных программ. Но, важно то, что не надо забывать о том, что некоторые вредоносные программы применяются и другими способами – например, с помощью заражения файлов на переносных носителях информации. В особенности, опасными являются компьютеры общего пользования. Четвертая угроза - неосторожность пользователя. Некоторые пользователи, пренебрегающие правилами безопасности защищённости компьютерных данных, создают конкретную угрозу безопасности собственных данных и денежных средств. Часто они полагают, что их данные не представляют интереса для злоумышленников. Вследствие того, что пользователи не уделяют внимания безопасности, они подвергают опасности свои данные. Невнимательность пользователей сети нередко является причиной неисправности компьютеров. Перегрев является главной опасностью для компьютеров и ноутбуков. ПК нагреваются вследствие перекрытия или засорения пылью вентиляционных отверстий. Приходим к выводу, что наиболее частыми угрозами в сети являются завладение личной информацией, финансовые махинации, и реклама, при нажатии на всплывающее окно, мы автоматически переходим на другой неизвестный сайт, который может быть вирусом. В данном случае помогут установленные на компьютер антивирусные программы и родительский контроль [18].

1.3. Проблема обеспечения безопасности при работе в сети Интернет как одна из насущных проблем системы образования

В настоящий момент проблеме безопасности является основной и решается на протяжении многих лет. Безопасность использования интернета и информационных и коммуникационных технологий одна из актуальнейших и важнейших тем современности. Не только в нашей стране, но и в странах

СНГ уже более десяти лет решают эту проблему. Даже США и Европейский Союз вплотную столкнулись с необходимостью решения всего спектра проблем: как регулировать доступ детей в Интернет и контролировать их пребывание там? Сегодня в мире уже возникло устойчивое понимание, что проблема детской безопасности в Интернете – это предмет, требующий скоординированного решения на всех уровнях: от семейного и муниципального до регионального и международного. В решении этой проблемы необходимо использовать правовые регуляторы, нормы обычаев и морали, а также технические и технологические возможности. Механизмом решения этой проблемы должно стать формирование информационной культуры личности – родителей, детей и учителей. Например, в ЕС была разработана программа «Безопасный Интернет», цель этой программы – поддержка и защита детей и молодых людей в режиме «Горячей линии» путем реализации инициатив повышения осведомленности и борьбы с незаконным и деструктивным контентом и поведением в Сети. В России же была утверждена Лига безопасного Интернета, целью которого является полное искоренение опасного контента в сети Интернет как мера, позволяющая избежать введение цензуры. Также в России был принят закон «О защите детей от информации, причиняющей вред их здоровью и развитию», целью которого является обеспечение информационной безопасности несовершеннолетних путем введения законодательных гарантий и организационно-правовых механизмов защиты детей. Данная проблема не только реально существует, но и по мере увеличение детской аудитории Интернета в России будет становиться все более острой.

Анализируя исследование Хохловой Н.И. [27] можно сделать вывод, что борьба за безопасный интернет охватила многие страны, и каждый разрабатывает свои методы борьбы с нежелательным контентом. Автор разрабатывает отдельные уроки по правилам поведения в сети Интернет, которые применяет на уроках информатики и во внеурочной деятельности.

Предлагает воспользоваться зарубежным опытом в вопросе обеспечения безопасности детей в сети Интернет.

На сегодняшний день в России и за рубежом возрастает подростковая жестокость и детская смертность. Дети большую часть своего времени проводят за компьютером и что они там смотрят никто не знает, а ведь именно там и показывают и рассказывают о жестоком отношении к друг другу, о самоубийстве. Мы хотим, что бы не только дети и их родители обращали на это внимание, но и школа, и государство имело огромное влияние на эту сферу жизни. Таким образом мы видим, что нужны более современные способы защиты от несанкционированного доступа к сетевым ресурсам. Об этом говорится в работе Р.Д Абрарова и Д.А Курязова [1].Они отмечают, что все-таки может быть и такое, что такая защита становится уязвимой и не срабатывает программные продукты для защиты информации. Поэтому возникает проблемы необходимости в создании дополнительных аппаратных и программных средств защиты сетевых ресурсов от несанкционированного доступа или подключения.

К аппаратным средствам защиты относятся различные брандмауэры, сетевые экраны, фильтры, антивирусные программы, устройства шифрования протокола и т. д. К программным средствам защиты можно отнести: слежения сетевых подключений (мониторинг сети); средства архивации данных; антивирусные программы; криптографические средства; средства идентификации и аутентификации пользователей; средства управления доступом; протоколирование и аудит. При создание крупномасштабных (локальных, корпоративных и т. д.) компьютерных сетей возникает проблема обеспечения взаимодействия большого числа компьютеров, серверов, подсетей и сетей т. е. проблема поиска и выбора оптимальной топологий становится главной задачей. Известно, что в компьютерных сетях для обеспечения безопасности информации и сети подлежит обработке критическая информация. Под термином «критическая информация» подразумеваются определенные факты относительно

намерений, способностей и действий, жизненно необходимых для эффективного управления и деятельности критически важных структур. С точки зрения безопасности компьютерные сети обладают следующими недостатками: недостаточный контроль над клиентскими компьютерами; отсутствие механизма настраиваемого доступа нескольких пользователей к разным ресурсам на одном компьютере; необходимость подготовленности пользователя к разным административным мерам — обновлению антивирусной базы, архивированию данных, определению механизмов доступа к раздаваемым ресурсам и т. д.; разделение ресурсов и загрузка распределяются по различным узлам сети, многие пользователи имеют потенциальную возможность доступа к сети как к единой компьютерной системе; операционная система, представляющая сложный комплекс взаимодействующих программ. В силу этого обстоятельство трудно сформулировать четкие требования безопасности, особенно к общецелевым сетям, разрабатывавшимся без учета безопасности; неопределенная периферия сильно влияет невозможность определения, в большинстве случаев, точных пределов сети. Один и тот же узел может одновременно работать в нескольких сетях, и, следовательно, ресурсы одной сети вполне могут использоваться с узлов, входящих в другую сеть. Такое широкомасштабное разделение ресурсов, несомненно, преимущество; множественность точек атаки компьютерной системе, можно контролировать доступ к системе пользователей, поскольку этот доступ осуществляется с терминалов компьютерной системы.

На основе анализа угрозы безопасности компьютерных сетей можно сделать выводы о свойствах и функциях, которыми должна обладать система обеспечения безопасности локальных и корпоративный сетей (КС). 1. Идентификация защищаемых ресурсов, т. е. при подключение компьютерным сетям присвоение защищаемым ресурсам, по которым в дальнейшем система производит аутентификацию. 2. Аутентификация защищаемых ресурсов. 3. Применение парольной защиты ресурсов во —

всей части компьютерной сети. 4. Регистрация всех действий: вход пользователя в сеть, выход из сети, нарушение прав доступа к защищаемым ресурсам и т. д. 5. Обеспечение защиты информации при проведении сканирования сети от вредоносных программ и ремонтно-профилактических работ.

Также очень важно рассмотреть решение проблемы со стороны школы, педагогов, родителей и учащихся. Проблему обучения школьников безопасному использованию средств ИКТ рассматривают авторы статьи Анурьева М.С, Королева Н.Л, Остапчук К.И [7]. Они исследует проблему обучения школьников безопасному использованию средств ИКТ. На основании содержания школьных учебников по информатике, можно сказать, что недостаточно формируется компетентная база личной информационной безопасности школьника, что негативно сказывается на психологическом и нравственном здоровье учащихся. Во всех рассматриваемых авторских учебниках не представлены вопросы, связанные с умением фильтрации нежелательного контента из всей массы информации в Интерете, а также профилактике интернет-зависимости у детей. В статье описывается, что необходимо провести многоплановую работу с обучающимися по прививанию навыков безопасного поведения в виртуальной среде, также необходимо проводить дополнительные занятия со школьниками с целью развития компетентности безопасного применения ИКТ. Ими сделан вывод, что необходимо разработать комплекс мероприятий с учащимися и их родителями по обеспечению безопасной работе в сети Интернет в урочной и внеурочной деятельности. Также проводить групповые и индивидуальные беседы с родителями и учащимися по правилам безопасного использования Интернет ресурсов.

Также для просвещения подрастающего поколения, знание учащимися элементарных правил поведения и отбора нужно информации в сети Интернет рассказывается в работе исследователя И.А Желтова [12]. Автор делает акцент на воспитание сетевой культуры и информационной

грамотности школьника, которая способствует обеспечению безопасности детей в Интернет - пространстве. Автор выделяет основные опасности в сети Интернет:

1. Сайты порнографической направленности.

2. Сайты, разжигающие национальную рознь и расовое неприятие.

3. Депрессивные молодежные течения. Обучающийся может поверить, что шрамы - лучшее украшение, а суицид - всего лишь способ избавления от проблем.

4. Наркотики. Интернет пестрит новостями о «пользе» употребления марихуаны, разнообразными рецептами и советами изготовления.

5. Сайты знакомств. Виртуальное общение разрушает способность к общению реальному, разрушает коммуникативные навыки подростка.

6. Секты. Виртуальный собеседник не схватит за руку, но ему вполне по силам «проникнуть в мысли» и повлиять на взгляды на мир.

В этой статье указывается, что в рамках школьного и домашнего общения с компьютером имеется возможность использовать уже наработанные средства; некоторые хорошо известны и даже включены в различные программные средства. Так, существует множество программ, позволяющих ограничить время работы за компьютером, отфильтровать содержимое Интернета, обезопасить маленького пользователя. Они называются программами родительского контроля (в WindowsVista). Это дает возможность контролировать использование компьютера ребенка в четырех направлениях:

- ограничивать время, которое он проводит за экраном монитора;

- блокировать доступ к некоторым сайтам;

- блокировать доступ к другим интернет- сервисам;

- запрещать запуск некоторых программ.

Исследователи, занимающиеся данной проблемой, сходятся во мнении, что для предупреждения рисков и повышения психологической безопасности подростков в онлайн - среде необходимы следующие шаги:

- гласность, широкое обсуждение проблемы онлайн-безопасности подростков в СМИ и на государственном уровне;

- объединение усилий всех пользователей интернет - сообщества, как создателей сервисов и разработчиков программных продуктов, так и простых пользователей;

- разработка и внедрение программ по формированию навыков безопасного поведения в Сети для школьников;

- продолжение научных исследований по проблеме.

Автором сделан вывод, что комплексное решение поставленной задачи со стороны семьи, школы, государства позволит значительно сократить риски причинения разного рода ущерба ребенку со стороны средств ИКТ и воспитать информационно грамотное, умеющее безопасно действовать в Интернете подрастающее поколение. Поэтому обеспечение информационной безопасности и воспитание сетевой культуры должно стать приоритетным направлением работы современной школы. И не только школы, здесь необходимо привлекать родителей к данному процессу. Постоянный контроль родителей усилить меры безопасности ребенка в Сети. Также совместное время проведение не только за компьютером, позволить развить навыки вашего ребенка и в других направлениях.

Также рассматривается вопрос об увеличении численности несовершенолетних школьников в Интернете. Авторы статьи Беленов Н.В, Самосонов О.С. [10] выделяют путь разрешения проблемы информационной безопасности – это обучение школьника восприятию и оценке информации, ее осмыслению на основе нравственных и культурных ценностей. Обеспечение информационной безопасности в условиях школьного образования рассматривается как совокупность деятельности по недопущению вреда психике и сознанию ребёнка. К опасностям информационной безопасности можно отнести доступность, присутствие в интернете элементов, нарушающих психику ребенка, а также элементов, не соответствующих возрастным особенностям обучающихся. Авторы приходят

к такому выводу, что проведение игр, круглого стола, беседа, анкетирование, классный час, собрание родителей, тематические уроки по безопасности в интернете, внеклассных мероприятий – это очень эффективные формы, помогающие учителю формировать навыки информационной безопасности у школьников. Особое значение для воспитания обучающихся имеют рекомендации, которые раскрывают психологические, интеллектуальные и коммуникативные особенности каждого ребенка, которые готовят человека к безопасной жизнедеятельности в информационном обществе. Также необходимо проводить индивидуальные беседы с ребенком, если он попал в трудную ситуацию в сети, необходимо понять проблему и найти пути ее решения. Возможно это будет психологическая атака на ребенка, угрозы в сети, домогательства, все это может привести к психологической травме у ребенка. Этого не надо допускать, все это может привести к жестокости в школе или дома, поэтому необходимо проводить профилактические меры по правилам поведения в сети как в школе, так и дома.

Неустоев А.А согласен с решением данной проблемы и в своей статье [11] посвященной проблеме информационной безопасности учащихся раскрывает еще один способ решения проблемы информационной безопасности – это научить ребенка критическому пониманию информации, ее адекватному восприятию и оценке. Школьникам и родителям необходимо знать о том, что в виртуальном мире существует целый свод правил, которые необходимо соблюдать при общении в сетях. Некорректное поведение, которое подростки демонстрируют в виртуальном пространстве, а так же совершают правонарушения в сфере ИКТ, говорит о незнании и неумении использовать основные правила поведения. Учитель должен иметь представление о классических методах защиты информации, и в равной мере о современных технологиях информационной безопасности. Он должен уделять большое внимание учебно-воспитательной работе с обучающимися, направленной на борьбу с негативным влиянием информационного пространства. В учебных программах, учебниках, методических пособиях по

информатике для школ РФ в различной степени нашли место следующие аспекты проблемы безопасности:

- техника безопасности при работе с компьютером;
- защита данных и Интернет сфере;
- правовая охрана программ, проектов и информации;
- проблема недостоверной информации;
- свобода слова и цензура в Интернет;
- надежность и безопасность работы компьютера;
- зависимость общества и человека от компьютера;
- качество ПО.

Такого рода материалы раскрывают вопросы безопасности использования компьютерной техники, информационных ресурсов, защиты интересов общества, но не отвечают на вопрос, как обеспечить собственную безопасность в информационном обществе. Тем не менее, информационная культура не сводится к информационным технологиям, она включает нравственный, психологический и другие гуманитарные компоненты. Поэтому необходимо более тщательно раскрывать все аспекты данной проблемы и находить пути ее решения. Необходимо раскрывать не только технические аспекты безопасной работы, а также психологические и нравственные компоненты.

В своих рекомендациях «Безопасность школьников в сети Интернет» Е.А. Багрова, И.В Лысакова [2] раскрывают проблему защиты несовершеннолетних пользователей от различных опасностей, подстерегающих их во всемирной паутине. Образовательное учреждение – это территория для развития личности обучающихся, а школа – это стартовая площадка для вступления выпускников во взрослую жизнь и успешного становления личности в современном обществе. Дети очень редко используют Интернет как образовательный ресурс, все чаще делают упор на игры и развлечения. Но мы все знаем, что интернет таит в себе много опасностей. Большинство родителей знакомо с данной проблемой, но лишь

немногие знают, как правильно защитить своего ребенка. Целью является разработать первоочередные шаги для обеспечения безопасности. Безопасность детей одна из главных задач цивилизованного общества. Необходимо проводить с детьми профилактические работы, она должна быть организованна с учетом возрастных особенностей. Потому что, не все советы которые мы дает во взрослой жизни, подходят детям дошкольного возраста. Необходимо проводить мероприятия, беседы, классные часы, тренинги, участвовать в конкурсах, различных проектах, выпуске стенгазет. Также представлены рекомендуемые направления работы: разъяснительная работа, направленная на убеждающий эффект; применение методов противодействия идеологии экстремизма; приемы и способы воздействия на отдельных учеников, на целевые аудитории; приемы, направленные на нейтрализацию замечаний; приемы, направленные на нейтрализацию технологий информационного воздействия. Профилактическая работа с родителями – родительские собрания, индивидуальные беседы, лекции.

Для достижения положительного результатов необходимо проводить комплексную работу семьи и школы. На смену «знаниевому» подходу пришел «компетентностный». И в своей статье В.В. Обухович «Интернет-безопасность» [25] описывает, что сейчас происходит замена «компетентностного» на «адаптационный». Адаптивный подход – любые принимаемые человеком решения, основываются на опыте взаимодействия индивидума с окружающей средой.[25] «Адаптивный» подход делает «акцент на формировании способности учащихся адекватно реагировать на вызовы современной культуры и применять полученные знания и навыки в процессе социализации и инкультурации». В федеральном образовательном стандарте второго поколения заявлен компетентностный подход. Данный подход подразумевает результатом образовательной деятельности является не набор знаний, а определенный уровень компетентности: «Интегрированным результатом освоения основных общеобразовательных программ является уровень компетентности выпускника». Под

компетентностью понимается следующее: «ключевые компетентности, имеющие универсальное значение для различных видов деятельности (обобщенные способы решения учебных задач; исследовательские, коммуникативные и информационные умения), умение работать с разными источниками информации. Информационная компетентность является одной из базовых компетентностей, на которую направлена система образования. Информационная безопасность и информационная компетентность взаимосвязаны. Информационная безопасность – состояние защищенности жизненно важных интересов личности, проявляющихся в умении выявлять и идентифицировать угрозы информационного воздействия». Понятие «информационная компетентность» не сводится к аспектам связанным, с компьютеризацией, является более широким, интернет-безопасность является частью информационной компетентности и одной из наиболее актуальных сегодня тем. Именно этой проблеме посвящена его статья. Интернет не только приносит пользу, но он является сильным искушением для учащихся. Надо научить школьников распределять свое время, не только развлекаться, но и получать знания. Уметь отличать авторитетные источники от сомнительных. Педагогика основана на общении человека с человеком, а если сократить роль учителя и сделать шаг к компьютеризации, то это будет опасное положение. В числе сайтов содержащих небезопасную информацию: посвященные какой-либо незаконной деятельности, с рекламой табака и алкоголя, пропагандирующие насилие и девиантное поведение, содержащие информацию о сектах и террористических организациях, посвященные продаже запрещенных товаров. Опасность таких ресурсов состоит в возможности нарушения нормального развития ребенка, неправильного формирования нравственных ценностей, знакомстве с людьми с преступными намерениями, заражения компьютера вредоносными программами. Важно отметить, что сами школьники не понимают данную опасность, которую могут встретить в интернете. В связи с этим, путем развития информационной безопасности является просветительская

деятельность. Одной из проблем является отсутствие уроков медиабезопасности, часто школьники даже не понимают этого термина. Знания о медиабезопасности необходимы в связи с тем, что вредоносные сайты устроены таким образом, что находятся в поисковых системах при безопасных запросах. Представляется, что отказ от вредной информации должен быть осознанным выбором ребёнка, сформированным под влиянием просветительской деятельности, медиабезопасности. Специалисты предлагают ряд решений проблемы медиабезопасности: например, посещение детьми определённого перечня безопасных сайтов, интернет-фильтр. Однако все указанные меры не должны быть скрытыми от школьника. Так, психолог А. Березников [9] отмечает: «Чтобы запреты не вызвали негативного отклика (особенно когда речь идет о подростках), нужно все ограничения проговаривать в устной беседе с ребенком». Важно отметить, что запрет не является решением проблемы. Так, психологи выделяют три типа школьников, использующих интернет: «ботаники» (интересуются только полезной информацией), «потребители онлайн контента» (ищут общения, наиболее часто используемые ими ресурсы — это социальные сети и всевозможные чаты), а также «универсалы» (совмещают все виды сетевой активности). Запреты действуют лишь на первую группу, но ей они и не нужны. У остальных же радикальные меры вызывают противоречие и подрывают доверие к взрослым. В этом отношении неэффективным и неэтичным считается метод программ-шпионов, которые просто позволяют видеть все действия ребёнка в сети.

Важно отметить, что специалистами предлагается и такой вариант, как список определённых правил пользования интернетом для ребёнка. Один из них приводит В. В. Гафнер [9], его список состоит из следующих положений: «1. Контролировать расписание, время подключения и способ использования им Интернета. 2. Ребёнок должен понять, что его виртуальный собеседник может выдавать себя за другого. 3. Не разрешать ребенку предоставлять личную информацию через Интернет. 4. Оградить ребёнка от ненадлежащего

веб-содержимого. 5. Установить на компьютер антивирусную программу». Кроме того, важным представляется знакомство учащихся с полезными сайтами. Так, многих учащихся могут заинтересовать сайты вузов, в которые они планируют поступать. Сегодня в условиях развития информационных технологий сайты вузов приобретают особое значение. Они становятся таким же источником информации, как дни открытых дверей, или информация, полученная от официальных лиц. Можно смело утверждать, что сегодня сайт — это неотъемлемая часть вуза .

Важно отметить, что интернет-безопасность должна была частью образования не только детей, но и родителей. Зачастую родители не знают об опасностях, которые ребёнок может встретить в интернете, не следят за временем и деятельностью детей в сети, не знают о программах родительского контроля и фильтрации. Часто родители считают, что интернет-образованием должна заниматься школа, однако это не так. Каждая семья должна продумать собственную стратегию родительской помощи в интернете, состоящую из следующих элементов: правила и ограничения, личный контроль, использование технических средств защиты, личное активное участие в виртуальной жизни детей. Таким образом, интернет-безопасность школьников должна занимать важное место, воспитывая личность, не только защищённую от негативной интернет-информации, но и способную делать собственный выбор. Можно сказать, что данная статья раскрывает новое понятие «информационная компетентность», которое взаимосвязано с информационной безопасностью. Автор [9] отмечает отсутствие уроков по медиабезопасности, которые необходимы для нашего образования. Также отмечает, что и семья должна играть немало важную роль в осуществлении родительского контроля в интернете. Автор указывает на важную роль педагога, потому что он является первым, кто может познакомить учащихся с сетью Интернет и правилами поведения. В обязанность учителя входит грамотно предоставить учащимся информацию о о безопасности в сети Интернет.

Вопрос о необходимости формирования компетентности педагогов в области информационной безопасности личности учащихся раскрывается в работе О.Б. Голубева, О.Ю. Никифорова [17]. Учителям необходимо формировать у учащихся навыки информационной безопасности и медиаграмотности, которые позволят самостоятельно оценивать уровни опасности и противостоять угрозам и рискам в сети Интернет. Они предлагают разработать практические рекомендации для учащихся и их родителей. Государство со своей стороны требует описать все аспекты безопасного взаимодействия школьника с Интернет-средой с учетом всех региональных особенностей. К таким аспектам отнесем: модель угроз информационной безопасности детей в глобальной сети Интернет, психологические риски, модель организации информационной безопасности в образовательном учреждении. Для разработки всех теоретических и практических основ информационной безопасности школьников необходимо: разработать комплексную модель школьника в сети Интернет. Модель должна содержать совокупность взаимосвязанных профилей школьника для доступа к различным сервисам сети Интернет. Анализ подобной модели позволит сделать обоснованные выводы об интересах школьника во всемирной паутине, получить представление о его предпочтениях и мотивах. Модель школьника в сети Интернет необходимо дополнить загружаемым, скачиваемым и порождаемым им контентом, который может включать в себя текстовые, графические, аудио и видео материалы; выполнить анализ угроз информационной безопасности обучающихся в сети Интернет. В ходе анализа будут выявлены основания для классификации и описание всех угроз, имеющих значение в рамках изучения данной проблемы, в разрезе выделенных классификационных оснований; подробно изучить существующие проблемы интернет-зависимости школьников во всех аспектах. Здесь можно выделить актуальные примеры интернет-зависимости: от социальных сетей, от сайтов развлекательной направленности, от социальных сетей, от видеохостингов,

от онлайн-игр; исследовать главные принципы организации защиты детей от вредной информации в сети Интернет. Изучить позитивный и негативный опыт в России и в зарубежных странах; изучить рынок современных аппаратных и программных средств обеспечения информационной безопасности детей в сети Интернет. Выполнить их сравнение и провести анализ эффективности использования; выявить региональные аспекты информационной безопасности в сети Интернет школьников дома и в образовательном учреждении. Проанализировать и определить текущее состояние проблемы; описать концепцию системы контентной фильтрации в образовательных учреждениях как центрального элемента системы обеспечения информационной безопасности школьников в сети Интернет. Провести анализ ее эффективности и определить текущий уровень развития. Данная статья дает развернутый ответ, на то какие задачи необходимо решить, чтобы двигаться в правильном направление в решении проблем обеспечения безопасной работы в сети Интернет. Дает определенный план по которому необходимо действовать в решении данной проблемы, выявляя различные проблемы и пути их решения. Также рассматривает все стороны и аспекты данной проблемы и путем анализа дает правильные решения.

Эти предложения поддерживает Неустроев А.А. [13]. Он раскрывает актуальность профилактической воспитательной работы с современными учащимися по обеспечению безопасности детей в сети Интернет. Главная мысль статьи заключается в том, что ученик школы XXI века должен научиться пользоваться всеми возможностями и особенностями информационной сферы, владеть культурной этикой и правилами поведения в сети Интернет. Автор выделяет самые основные проблемы, с которыми встречаются обучающиеся:

— анонимность, отсутствие настроек безопасности;

— шантаж, вымогательство, манипулирование, оскорбления и нападки со стороны других;

— взаимосвязь между количеством проведенного онлайн времени и психоэмоциональным состоянием школьников;

— долгое пребывание детей и подростков за компьютером влечет за собой значительный вред здоровью, они могут стать потенциальными потребителями негативного интернет-контента (экстремистских материалов различного характера, разрушительного поведения и зависимостей). Чтобы при работе учащиеся обладали навыками грамотного и безопасного использования Интернета. В целях контроля информационной безопасности детей необходим постоянный мониторинг действующих законов и правовой практики исходя, из реальной эффективности принятых в интересах детей мер и управленческих решений. Необходим регулярный контроль информационной деятельности обучающихся.

Необходимо рассмотреть какие задачи стоят перед школой, государством, семьей. В методических рекомендациях педагогического работника Баскаковой Н.И. [4] разработаны рекомендации руководящим и педагогическим работника, родителям обучающихся и детям разного возраста. Выявлена одна из важных и первостепенных проблем – это защита несовершеннолетних от противоправных действий с использованием сети Интернет. Перед государством стоит задача поддержания эффективного комплекса мер по профилактике, предотвращению и преодолению последствий вредоносных действий в отношении несовершеннолетних, совершаемых с применением Интернета. Образовательное учреждение играет ключевую роль в обеспечении мер по Интернет-безопасности. Решение этой проблемы требует комплексного подхода. В образовательном учреждении должен быть сформирован пакет нормативно – правовой документации: документы по контентной фильтрации, по обработке персональной информации, положения и регламенты по работе в сети Интернет, различные положения об организации профилактической работы по медиабезопасности, о формах профилактической работы с детьми и родителями по Интернет - безопасности. В организационном плане должен

выполняться ряд мер технико - технологической направленности – это установка антивирусных программ, программ – фильтров, лицензионное программное обеспечение. Также к внутришкольным мероприятиям относится реализация правил Инетернет-безопасности с привлечением всех работников образовательного учреждения. Для профилактической работы с детьми и родителями педагогические работники должны знать риски и опасности в сети, должны быть готовы дать необходимые рекомендации по решению этой проблемы. Для профилактических мер необходимо постоянно проводить мониторинг, диагностику проблем по Интернет-безопасности. В программно-методическом обеспечение должен быть разработан модуль, в который должны быть включены темы по медиабезопасности и безопасном поведении в сети. Также рекомендуется проводить классные часы, внеклассные мероприятия на которых знакомить детей и родителей с правилами поведения в сети Интернет. Разнообразна может быть и тематика школьных мероприятий например: достоверность информации в сети, этика сетевого общения, интернет – зависимость, компьютерные вирусы, азартные игры в сети, кибермошенничество, как защитить личную информацию в сети, как защититься от нежелательного общения. Для каждого класса можно использовать свою форму урока: 1-4 классы – урок–путешествие, урок-викторину, урок-игру и т.п., 5-8 классы – урок-презентация проектов, урок – пресс-конференция, урок- практикум, урок – встреча со специалистами и т.д., 9-11 классы – деловая игра, дискуссия, дебаты, день медиабезопасности, встреча со специалистами. Так что же необходимо знать педагогу в этом вопросе. Необходимо знать виды Интернет угроз, уметь и распознавать и предотвратить. Для этого необходимо вместе с детьми анализировать полезную информацию в сети Интернет. Необходимо научить детей правильно реагировать на агрессию в сети, рассказать, куда необходимо обратиться в подобных случаях. Зачастую дети и подростки в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться. Сделать их пребывание в Интернете самая главная задача для педагогов и

родителей. Приведены самые распространенные риски в сети Интернет. Контентные риски – это различные информационные ресурсы, содержащие противозаконную, неэтичную и опасную информацию. Как мы знаем распространение различной противозаконной информации преследуется законодательно. Неэтичный контент не запрещен к распространению и не попадает под действие уголовного кодекса – это онлайн-игры, порнография, азартные игры, различные способы самоубийства, пропаганда нездорового образа жизни, нецензурная брань, оскорбления. Коммуникационные риски взаимосвязаны с общение во всемирной паутине и межличностными отношениями различных интернет - пользователей. Предположим, что это знакомство и различного рода встречи в сети, интернет-хулиганство, кибербуллинг, незаконные контакты и др. Кибербуллинг, преследование с использованием цифровых информационных технологий, в большей мере воздействуют на детей и подростков независимо от возраста. В первую очередь это происходит на различных сайтах и может продолжаться достаточно долгое время. Субъектов кибербуллинга в России в два раза больше, чем в среднем по европейским странам. Электронные риски – программное обеспечение, которое может принести вред вашему компьютеру. Потребительские риски – значительное превышение в Интернете правами пользователя. Чаще всего происходит хищение доступной личной информации – это хищение банковских данных, всевозможных паролей, номеров кредитных карточек и т.д. Хищение личных данных называется фишингом. Рассматривается такое понятие как интернет-зависимость, которая начинается во всемирной паутине, где дети проводят большую часть времени. Так родители потеря контроль над своими детьми, поэтому необходимо найти равновесие между разумным использованием интернета и различными играми. Интернет – зависимость это навязчивое желание посетить Интернет и неспособность выйти из него. Исходя из данного исследования проблемы, можно выделить самое главное – это создание комплекса мер по решению данной проблемы. Ведь именно

совместными усилиями можно продвинуться в решении этой проблемы. Также необходимо провести совместную работу учащихся и родителей по освоению правил безопасного поведения в сети Интернет. Разработать пособия по обучению безопасной работы детей в сети.

В научной работе учителя информатика Юдиной Т.М. [6] проводится теоретический анализ научной и методической литературы и раскрывается проблема увеличения потребности в обеспечении эффективного использования информационных научно-образовательных ресурсов. Раскрывается тема о способах защиты отинтернет угроз при работе за компьютером дома. Описываются все возможные риски при работе в сети, также раскрываются принципы интернет – зависимости, которая в наше время стала очень распространенна. Подробно автор рассматривает способы защиты, распространенные программные фильтры. Также описаны рекомендации для детей и их родителей по безопасному использованию интернета и предложены общие правила при работе в сети. В ходе работы было проведено тестирование учащихся на сайте «Единый урок.дети». Результаты показали, что 50% учащихся плохо знакомы с безопасностью в сети, 35% хорошо знакомы, 15% не только знакомы, но и соблюдают правила безопасного пользованию сетью Интернет. В данной статье описываются все возможные риски при работе в сети, раскрываются принципы интернет-зависимости, описываются распространенные программные фильтры. Также предложены рекомендации для детей и родителей по безопасной работе в сети дома.

Выводы по главе 1

В информатике введено понятие информационной безопасноти. Это понятие имеет ряд определений. К настоящему времени выделены основные риски и угрозы информационной безопасности в сети Интернет.

Анализ научно-методической литературы по проблеме исследования показал, что школа и педагогические работники уделяет внимание решению проблемы обеспечения безопасной работе учащихся в сети интернет. Обозначена необходимость комплексного взаимодействия образовательных учреждений, государства, семьи. Это будет способствовать повышению уровня безопасности учащихся как в школе, так и дома. Разработаны различные формы и методы, которые успешно используются в учебно-воспитательном процессе. Среди них можно назвать беседы, круглые столы, дебаты, дискуссии, проведение родительских собраний.

Глава 2. Разработка рекомендаций для учащихся 7-9 классов по обеспечению безопасной работы в сети Интернет

2.1. Анализ содержания действующих учебников по информатике и ИКТ

Рассмотрим наличие материала по теме «Безопасность в сети Интернет» в действующих учебниках по информатике и ИКТ. Данные представим в таблице 1.

Таблица 1

Наличие материала по теме исследования в действующих учебниках по информатике и ИКТ

Учебник (класс)	**Тема урока**	**Рассматриваемая проблема**	**Количество часов**
Л.Л Босова, А.ЮБосова, 2014 г (8 класс)	нет	нет	нет
Л.Л Босова, А.ЮБосова, 2013 г (9 класс)	Глава 4.2 «Всемирная компьютерная сеть Интернет» Глава 4.3 «Информационные ресурсы и сервисы Интернета»	Глава 4.2 Понятие Интернет. IP-адрес, DNS. Глава 4.3 Понятие: файловый архив, электронная почта, основные формы коллективного взаимодействия(чаты,форумысоц.сети), логин и пароль .	2 часа
Л.Л Босова, А.ЮБосова, 2013 г (7 класс)	Глава 1.3 «Всемирная паутина».	Глава 1.3 Понятие WWW или Всемирная паутина, web-страницы, web-браузеры, поисковые системы, поисковые запросы, полезные адреса Всемирной паутины.	2 часа
И.Г Семакин, Л.В	Глава 25	Глава 25.	3 часа

Шестакова 2015 (9 класс)	«Информационные ресурсы современного общества». Глава 26 «Проблемы формирования информационного общества». Глава 27 «Информационная безопасность».	Понятие информационные ресурсы, национальные информационные ресурсы и их виды. Глава 26 Понятие: информатизация и ее задачи, информационное общество. Глава 27 Информационные преступления, программно - технические способы защиты информации, понятие компьютерный вирус, правовая защита информации, опасности соц.сетей.	
И.Г Семакин, Л.В Шестакова 2012 г (7класс)	нет	нет	нет
И.Г Семакин, Л.В Шестакова 2015 (8 класс)	Глава 1. «Передача информации в компьютерных сетях». Глава 2. «Электронная почта и другие услуги компьютерных сетей». Глава 3. «Аппаратное и программное	Глава 1. Компьютер и локальная сеть, глобальная сеть,интернет. Глава 2. Электронная почта, почтовый ящик, электронный адрес, телеконференция, форум, файловые архивы и другие сетевые сервисы, коллективные проекты. Глава 3. Технические средства глобальной сети, протоколы,	5 часов

	обеспечение сети». Глава 4. «Интернет и всемирная паутина». Глава 5. «Способы поиска в Интернете».	сервер-программа электронной почты. Глава 4. Интернет, что такое WWW, web-сервер, web-сайт, web-страница, проблема поиска информации в сети. Глава 5. Три способа поиска в Интернете, поисковые серверы, язык запросов поисковой системы. Система основных понятий Главы 1.	
Н.Д Угринович (8 класс) 2015 г	Глава 6. «Коммуникационные технологии и разработка web – сайтов» Глава 6.2 «Локальные компьютерные сети» Глава 6.3 «Глобальная компьютерная сеть Интернет» Глава 6.4 «Web-страницы, web-сайты»	Глава 6 Передача информации. Глава 6.2 Сетевые ресурсы, аппаратное и программное обеспечение проводных и беспроводных сетей. Глава 6.3 Интернет, подключение к интернету, адресация в интернете, маршрутизация и транспортировка данных по компьютерным сетям. Глава 6.4 Web-сайты, структура web-страницы, форматирование текста, вставка изображений, гиперссылки, интерактивные формы списки на web-странице.	4 часа

		Практические работы «Коммуникационные технологии и разработка webсайтов»	
Н.Д Угринович (9 класс)	Глава 6. «Информатизация общества» «Информационное общество» «Информационная культура» «Перспективы развития ИКТ»	Глава6. Информационное общество, население, занятое в информационной сфере, информационная культура, коммуникативная культура.	3 часа

В таблице представлены школьные учебники, в которых отражена тема по безопасной работе в сети Интернет. В учебнике Босовой Л.Л. [15] 7 класс – всего 1 глава, 9 класс – 2-е главы и 8 класс - отсутствует. В учебниках Семакина Л.В. [29] 9 класс – 3 главы, 8 класс – 5 глав и 7 класс - отсутствует. В учебниках Угриновича Н.Д. [35] в 9 классе – 1 глава, 8 классе – 4 главы и 7 класс - отсутствует. В учебнике Босовой Л.Л. [14] для 9 класса кратко представлены правила сетевого этикета, где указывается на необходимость уважать своих партнеров по Сети. Описывается понятие фишинг, контакты с незнакомыми детьми, угроза заражения вирусом, азартные игры, также описаны сайты с ненужной и опасной информацией, представлены несколько правил личной информации. Отмечается, что необходимо быть внимательнее при работе в Интернете, необходимо нести ответственность за свои данные. В учебнике Босовой Л.Л. [15] для 7 класса есть только одна глава «Всемирная паутина». Отмечается, что это мощное информационное хранилище, которое содержит разнообразную информацию, точнее можно

сказать, что содержит абсолютно всю информацию. Информация представлена на страницах (www), также могут на сайтах быть представлены гиперссылки. Можно сказать, что Всемирная паутину представляет собой определенную библиотеку. Также описывается как найти нужную информацию, существует множество поисковых систем. Представлены полезные сайты Всемирной паутины.

Анализ действующих учебников показал, что материал по рассматриваемой проблеме содержит основные понятия и некоторые указания для учащихся при работе в сети интернет. Выявляется необходимость обращения к решению проблемы во внеурочной деятельности учащихся. На наш взгляд это могут быть методические материалы. Методические материлы разработаны с целью обеспечения реализации образовательными организациями системы мероприятий, направлен ных на обучение учащихся правилам безопасного поведения в интернет-пространстве, профилактику интернет-зависимости, националистических проявлений в молодежной среде и устранение риска вовлечения подростков в противоправную деятельность. Материалы разработаны на основании письма Министерства образования и науки от 12.12.2014 №17-02/9115-ИК «О методическом обеспечении деятельности по противодействию экстремизму среди обучающихся и профилактике интернет-зависимости». 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»).

Предлагаемые нами материалы представлены в следующем параграфе.

2.2. Методические материалы по обучению безопасной работе в сети Интернет учащихся 7-9 классов

Родительское собрание «Интернет – опасности для детей»

Цель: оказание помощи родителям в обеспечении безопасной работы детей в Интернете

Задачи родительского собрания:

- обсудить с родителями проблему о зависимости детей от Интернета;
- познакомить родителей с опасностями, с которыми дети могут встретиться в Интернете.
- совместно найти пути решения данной проблемы;
- познакомить родителей с советами специалистов по общению ребят с интернетом;
- научить некоторым правилам и способам, облегчающим общение с подростком;
- побудить родителей к полноценному общению с собственными детьми;
- расширить объем знаний родителей о нормах и способах решения образующихся проблем с детьми.

Форма проведения: беседа.

Оснащение: компьютер; мультимедийный проектор.

Участники: родители обучающихся, классный руководитель.

Ход родительского собрания

Добрый день, уважаемые родители! Тема нашего разговора сегодня «Профилактика интернет-рисков и борьба с ними»

Если ваши дети пользуются Интернетом, вы, без сомнения, должны волноваться о том, как уберечь их от проблем, которые могут подстерегать их в путешествии по этому океану информации.

Какие существую интернет-риски и какие меры по профилактике нужно знать и применять родители.

Сейчас на нашем собрании вы найдете для себя ответ на данный вопрос.

Выступление классного руководителя

Сейчас все больше и больше компьютеров подключаются к работе в сети Интернет. При этом большое распространение получает подключение по скоростным каналам, как на работе, так и дома. Все больше численность детей получает возможность работать в Интернет. Но совместно с тем все острее возникает проблема обеспечивания безопасности наших детей в сети. Так как изначально Интернет развивался вне какого-либо контроля, то теперь он представляет собой огромное количество информации, причем далеко не всегда безопасной. В связи с этим и с тем, что возраст, в котором человек начинает работать с Интернет, становится все моложе, возникает проблема обеспечения безопасности детей. А кто им может в этом помочь, если не их родители и окружающие взрослые?

Следует понимать, что подключаясь к сети Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как к выходу в Интернет.

- Дети опережают взрослых по количеству времени, которое они проводят в Интернете. В возрасте между 8 и 13 годами дети составляют половину общего числа пользователей Интернета
- 44 % детей, регулярно использующих Интернет, хоть один раз подвергались сексуальным домогательствам при виртуальном общении, 11 % подверглись этому несколько раз.
- 14.5 % ребят назначали встречи с незнакомцами через Интернет, 10 % из них ходили на встречи в одиночку, а 7 % никому не сообщили, что с кем-то встречаются.
- 19 % ребят иногда посещают порносайты, еще 9 % проделывают это регулярно, 26% детей принимают участие в чатах о сексе

- 38% детей просматривают страницы о насилии
- 16% детей просматривают страницы с расистским содержимым

По сведениям МВД РФ, в Интернете сегодня действуют до 40 русских вебсайтов, содержащих материалы экстремистского и террористического характера. Причём любой четвертый подобный сайт находится на ресурсах отечественных провайдеров.

Хотя наиболее серьезные угрозы подстерегают наших детей за пределами мониторов, есть много серьезных опасностей, с которыми дети сталкиваются онлайн. К примеру, получая доступ к неуместной информации на сайтах, посвященных преступной деятельности или заходя на вебсайты, подвергающие риску их конфиденциальность. Хотя нашу озабоченность, в первую очередь, вызывает порнографический и иной сексуальный контент, существуют другие виды неприемлемой доступной информации, которая имеет возможность быть настолько же вредоносной для наших детей.

Как научить детей отличать правду ото лжи в Интернет?

Следует объяснить детям, что нужно критически относиться к полученным из Интернет материалам, ведь опубликовать информацию в Интернет может абсолютно любой человек. Объясните ребенку, что сегодня буквально любой человек имеет возможность создать свой личный вебсайт и при этом никто не станет держать его под контролем, насколько правдива помещенная там информация. Научите ребенка проверять все то, собственно, что он видит в Интернет.Как это объяснить ребенку? Существует памятка для родителей.

На примере решений Google, призванных гарантировать безопасность детей и в Интернете вы можете ставить фильтры для ненужных вебсайтов.

Подведение итогов

Я полагаю, что сейчас у нас была дружелюбная обстановка. Вам было комфортно, это видно из обсуждений различных вопросов. И в заключении ответьте на вопросы письменно. Желали бы вы продолжить обсуждать эту тему на родительских собраниях? Изменилось ли ваше отношение к

использованию детьми сети Интернет? Завершая наше родительское собрание, я раздаю вам памятки и призываю к сотрудничеству: давайте вместе любить наших детей, вместе заботиться об их здоровье, создавать успешное настоящее и счастливое будущее!

Исходя из принципа комплексного подхода к решению проблемы, нами следующие разработыны внеклассное мероприятия для учащихся.

Внеклассное мероприятие «Интернет вокруг нас»

(для учащихся 8класса)

Цель: оказание помощи учащимся и их родителям в безопасной работе в сети Интернет.

Задачи:

-выявить способы борьбы с интернет угрозами;

-познакомить родителей и учащихся с правилами поведения в сети;

-побудить родителей к полноценному общению со своими детьми;

- расширить объем знаний о безопасной работе в сети Интернет.

Форма проведения: игра, беседа.

Участники: классный руководитель, обучающиеся и их родители.

Ход мероприятия

Я вас всех приветствую на нашем мероприятии посвященный теме Интернет риски и борьба с ними. Интернет всегда и везде с нами, мы большое количество времени проводим в социальных сетях, и должны беспокоиться о том, как обезопасить себя и своего ребенка от различных угроз в Интернет паутине.

Присутствующие делятся на две команды «Родители» и «Ученики». Команде «Ученики» необходимо создать свое интернет сообщество и определить в нем чем правила поведения участников. Команда «Родители» должна придумать все возможные Интернет риски. Далее команда «Родители» по одному называют угрозы, а команда «Ученики» должны посоветоваться между собой и принять решение как они будут противостоять данной угрозе, и так далее со всеми остальными угрозами.

Далее проводим **Обсуждение.**

Зачем в Интернет сообществе нужны обязанности и запреты?

Какие бывают Интернет угрозы? Как с ними бороться?

Подводим итоги

Я думаю, что сегодня у нас была дружелюбная обстановка. Нам всем было комфортно, это видно из нашей беседы. Сегодня мы с вами узнали как бороться со все возможными угрозами в сети. Это было очень полезно для нас всех. Хотели бы вы продолжить обсуждение на данную тему? Изменилось ли ваше отношение к использованию ваших детей Интернета? Завершая наше мероприятие я раздаю вам памятки и призываю: давайте вместе заботиться о здоровье наших детей.

Внеклассное мероприятие по правилам поведения в Интернете

«Кодекс цифрового мира»

(для учащихся7класса)

Задачи:

• выделение правил интернет-сообществ;

• обсуждение интернет-этикета и правил общения с другими людьми в Интернете;

• создание кодекса цифрового мира. Необходимые материалы: листы ватмана или флип-чарт, маркеры, клейкие листочки для голосования, примеры кодексов.

Рекомендуемый возраст: 7–9 класс.

Процедура проведения

Упражнение проводится с целью формирования у школьников представлений о важности этических правил и норм поведения в Сети. Результатом упражнения должен стать универсальный кодекс поведения в Сети. Ведущий демонстрирует участникам логотипы четырех социальных сетей и спрашивает, знают ли они, что это за соц. сети, кто их создал и в каком году. Выслушав ответы, ведущий по необходимости их дополняет. Далее ведущий спрашивает, в чем отличие сообществ Facebook

и «ВКонтакте» от сообществ YouTube и Flickr. Выслушав ответы, ведущий обобщает, что первые два сосредоточены вокруг профилей пользователей, а последние два — вокруг контента, которые размещают пользователи (видео и фото). Ведущий спрашивает участников, что, на их взгляд, позволяет пользователям социальных сетей взаимодействовать так, чтобы их сообщество развивалось и не распадалось. Ведущий выслушивает несколько ответов и резюмирует их. Ведущий может подчеркнуть, что большинство современных интернет-сообществ живет и работает по правилам, которые организаторы вырабатывают для себя и для будущих участников сами. Свод правил, содержащий основные принципы поведения, называется кодексом. Ведущий спрашивает участников, какие кодексы им известны. Выслушав ответы нескольких участников, ведущий может привести в пример малоизвестные кодексы. Затем ведущий предлагает участникам создать свой кодекс поведения в Сети. Для разработки кодекса участники делятся на три группы. Каждая группа в течение 10 минут должна придумать социальную сеть и разработать краткий кодекс для ее пользователей. Ведущий может зафиксировать на доске задание для групп.

1. Создать социальную сеть и ответить на вопросы:

• Каково ее название?

• Кого она объединяет? Кто является участниками этой социальной сети?

• Что объединяет ее участников? На основе чего существует их сообщество? Это может быть что угодно: хобби или любимое произведение, любимый фильм или музыкальная группа.

2. Придумать семь правил, которые должны соблюдать участники социальной сети, чтобы сеть развивалась и росла, а общение в ней было интересным и приятным. В течение 10 минут группы выполняют задание и фиксируют все на листе ватмана (или флип-чарте). По истечении времени участники — по одному от каждой группы — представляет свою социальную сеть и разработанные правила. Когда все группы представят свои сети,

ведущий предлагает им создать универсальный кодекс интернет-сообщества. Для этого ведущий просит участников выбрать два лучших, на их взгляд, правила из кодексов других групп (правила своей группы выбирать нельзя). Каждый участник получает по два клейких листочка для голосования. Участники приклеивают листочки на правила, которые считают лучшими. Затем ведущий предлагает участникам ознакомиться с правилами уже существующих социальных сетей. В качестве примера ведущий демонстрирует видеоролик «О правилах пользования YouTube»

Принципы сообщества YouTube[36]

Уважайте сообщество YouTube

Мы не просим того же уважения, которое оказывают священникам, пожилым людям и нейрохирургам. Мы просто хотим сказать: не пакостите на сайте. Каждая новая прикольная функция сообщества на YouTube подразумевает определенный уровень доверия. Мы уверены, что вы относитесь к этому ответственно, ведь миллионы пользователей уважают наше доверие. Будьте в их числе.

Мы проверяем видео, отмеченные как «Нарушение правил»

Ладно, теперь мы расскажем о себе. Если видео помечается как неприемлемое, мы оцениваем его, чтобы определить, нарушает ли оно наши Условия использования. Ролики, помеченные флажком «Нарушение правил», не удаляются системой автоматически. Если после проверки мы удалили ваше видео, можете быть уверены, что мы сделали это сознательно, и наше предупреждение следует воспринимать всерьез. Глубоко вдохните, перечитайте наши Условия использования и попробуйте нас понять. Если вам повстречаются на YouTube другие видео с подобными нарушениями, пожалуйста, пометьте их, чтобы мы смогли проверить и их! **Не выходи за рамки**

Здесь приведены некоторые простые правила, соблюдение которых поможет избежать проблем: • YouTube не предназначен для размещения порнографии и откровенного сексуального содержания. Если ваше видео

имеет подобный характер, не размещайте его на YouTube, даже если на нем засняты лично вы. Кроме того, имейте в виду, что мы сотрудничаем с органами правопорядка и сообщаем об эксплуатации несовершеннолетних. Прочитайте материалы, размещенные в нашем Центре безопасности, и следуйте им на YouTube.

• Не размещайте видео, содержащее сцены грубого обращения с животными, приема наркотиков, изготовления бомб и другие безнравственные действия.

• Подробно показанное или беспричинное насилие недопустимо. Если в вашем видео кому-то причиняют боль, нападают на кого-то или оскорбляют, не размещайте это видео.

• YouTube не место для скандалов. Не размещайте жестокие видео несчастных случаев, трупов и так далее.

• Соблюдайте авторские права. Добавляйте только созданные вами видео или те видео, на использование которых у вас есть разрешение. Это означает, что не следует добавлять видео, созданные не вами, или использовать в своих видео материалы, авторскими правами на которые владеет кто-то другой, например музыкальные дорожки, фрагменты программ, защищенных авторским правом, или видео, созданные другими пользователями, без их разрешения. Для получения дополнительных сведений прочитайте наши Советы по авторскому праву.

• Мы уважаем разные точки зрения, включая самые непопулярные; в общем, мы за свободу слова. Однако мы не допускаем разжигания нетерпимости (высказывания, направленные на группу, с апелляцией к таким понятиям, как расовое или этническое происхождение, религия, 90 ограниченная дееспособность, пол, возраст, статус ветерана, сексуальная ориентация или половая самоидентификация).

• Мы нетерпимо относимся к нападкам, приставаниям, угрозам, оскорблениям, нарушению конфиденциальности или раскрытию личной

информации других участников. Всякому, кто будет уличен в совершении этих поступков, доступ на YouTube будет закрыт навсегда.

• Никто не любит спам. Не создавайте неверных описаний, тегов, названий или эскизов с целью увеличить количество просмотров. Не стоит размещать большие объемы нецелевого, нежелательного или повторяющего содержания, в том числе комментарии и личные сообщения. Отнеситесь к этим правилам как можно серьезнее. Не пытайтесь искать лазейки, чтобы их обойти — просто поймите их и постарайтесь уважать не букву, а дух. Нарушения условий предоставления услуг Google могут привести к предупреждению или к прекращению действия вашего аккаунта Если действие вашего аккаунта было прекращено, вам запрещается создавать новые аккаунты.

Кодекс блогеров

• Отвечайте за свои слова и ограничивайте высказывания, которые нарушают правила вежливости.

• Не пишите ничего такого, чего не сказали бы собеседнику в лицо. Не причиняйте вреда.

• Каждый имеет право высказать собственное мнение.

• В конфликтных ситуациях перед тем, как отвечать публично, сначала постарайтесь решить конфликт в личной переписке.

• Если видите, что нападают на другого пользователя, помогите защититься.

• Не оставляйте комментарии анонимно.

• Игнорируйте троллей.

• Создавайте информацию, интересную разным группам людей.

• Указывайте авторство и первоисточник, если информация не ваша.

Пока участники смотрят ролик, ведущий составляет универсальный кодекс, включая в него правила, которые:

• повторяются в кодексах двух или всех команд;

• отмечены наибольшим количеством стикеров по сравнению с другими правилами. После просмотра ролика ведущий обращает внимание участников на то, что правила могут быть трех типов:

• обязанности (что должны делать участники);

• права (что могут делать участники);

• запреты (что нельзя делать).

Ведущий демонстрирует универсальный кодекс, зачитывает каждое правило и просит участников определить, к какому типу оно относится. Созданный кодекс можно вывесить в классе или на сайте класса.

Пример универсального кодекса, созданного учащимися.

1. Соблюдайте этикет.

2. Запрещено распространение спама.

3. Запрещено распространение вирусов.

4. Запрещено оскорблять других пользователей.

5. Соблюдайте личное пространство друг друга.

6. Следите за временем, которое вы проводите в социальной сети.

7. Наслаждайтесь контентом.

Обсуждение

• Может, вы хотите добавить что-нибудь в универсальный кодекс? Все ли типы правил в нем представлены?

• Можно ли применить эти правила для всех пользователей Интернета?

• Зачем в Интернете и интернет-сообществах нужны обязанности и запреты?

Подводя итоги

Каждому сообществу нужны определенные правила, которые бы регламентировали поведение его членов. Даже сообщество самых близких друзей распалось бы, если бы его не регулировал негласный кодекс товарищества, который есть в любой группе. Правила необходимы любой группе, так как они сохраняют ее от внутренних конфликтов и распада, но если эти правила будут слишком строгими, то группа может перестать

развиваться и большинство членов покинет ее один за другим. В относительно больших группах, таких как интернет-сообщества, где достаточно много членов, которые могут не знать друг друга, лучше не полагаться на неписанные законы, а четко прописывать правила поведения.

Обычно правила включают в себя следующие компоненты:

• Что можно делать в сообществе (права).

• Что нужно делать в сообществе (обязанности).

• Чего нельзя делать в сообществе (запреты).

• Что будет, если нарушить правила (санкции).

Наиболее распространенными санкциями в интернет-сообществах является временное или постоянно исключение из группы или временный запрет на участие в деятельности группы, так называемый «бан». Прежде чем присоединиться к сообществу, необходимо досконально изучить правила поведения в нем и решить, готовы ли вы их соблюдать. Если вы уже присоединились к группе, то стоит соблюдать принятые на себя обязательства.

2.3. Результаты педагогического эксперимента

На педагогической практике мною проводилось внеклассное мероприятие для учащихся 7 классов на тему «Кодекс цифрового мира».

Целью данного мероприятия было познакомить учащихся с правилами общения с другими людьми в Интернете.

Задачи для данного мероприятия были следующими:

1. выделение правил интернет-сообществ;

2. обсуждение интернет-этикета и правил общения с другими людьми в Интернете;

3. создание кодекса цифрового мира. Необходимые материалы: листы ватмана или флип-чарт, маркеры, клейкие листочки для голосования, примеры кодексов.

На первом этапе предусмотрен организационный момент, настрой на работу и формирование навыков самоорганизации.

На втором этапе - постановка цели. На этом этапе урока развиваются навыки общения со сверстниками и учителем в процессе деятельности (технология сотрудничества - переход от педагогики требований к педагогике отношений) – коммуникативные УУД, формируется – личностные УУД, вырабатывается умение ставить учебную задачу, называть цель, формулировать тему. Мы вместе с учениками поставили цель и объявили тему данного мероприятия.

В самом начале, ученики были вовлечены в данную тему. В этом этапе происходит диалог учителя с учениками. Ученики проявляли активность. Так же были ознакомлены с правилами известного сайта Youtube.

Ребята разделились на три команды, каждая из которой представляла свое интернет сообщество. От каждой команды выступал командир, который озвучивал название сообщества, правила поведения на своем вебсайте. При этом весь класс внимательно их слушал и задавал вопросы.

1 команда во главе с командиром Сазоновым Денис придумала сообщество «Live», а также основные правила поведения, вторая команда во главе с командиром Скопинцевой Анной придумала сообщество «Школа наше все» и третья команда под руководством командира Белоноговой Алены создала сообщество «Ученики это круто».

Следующий важный этап - физкультминутка. Мы с ребятами, включили видеоролик с физкультминуткой на 2 минуты – все остались довольными.

После этого проходило обсуждение данных правил с учащимися и совместно составлен универсальный кодекс правил по поведению в Инетернет – сообществе.

У каждого мероприятия должен быть, чтокаждому сообществу нужны определенные правила, которые бы регламентировали поведение его членов.

Темп работы во время урока спокойный. Характер общения с учащимися доброжелательный, создан нужный для работы микроклимат. Психологическая атмосфера поддерживается непринужденной беседой, разговором, обсуждением.

Итог: Все цели, задачи, этапы выполнены. В течение всего времени учащиеся активно работали. Мне было легко проводить данное мероприятие, ученики активно включились в работу.

При проведении родительского собрания «Интернет – опасности для детей» обсуждалась проблема зависимости детей от Интернета. Поставлена задача: найти совместные пути решения данной проблемы, научить некоторым правилам и способам решения образующихся проблем с детьми.

На собрании рассказывалось какие существуют интернет-риски, какие меры профилактики необходимо знать и применять родителям. Представлена информация как научить детей отличать правду от лжи в интернете?

При подведении итогов родителям были заданы такие вопросы как: «Хотели бы вы продолжать обсуждать эту тему на родительских собраниях? Изменилось ли ваше отношение к использованию детьми сети Интернет?»

Ответы последовали положительные, родители высказали свое желание дальше обсуждать данную важную проблему.

Вывод по главе 2

В действующих учебниках по информатике и ИКТ недостаточно информации по правилам поведения в сети и по предотващению угроз в виртуальной среде. Пополнить знания учащихся по данной проблеме можно посредством проведения различных внеклассных мероприятий. Нами были разработаны два мероприятия. Поскольку проблема должны решаться на основе комплексного подхода, то необходимо к решению еепривлекать родителей учащихся. Для родителей нами было разработано родительское собрание. Целью мероприятий было познакомить учащихся и их родителей с правилами поведения в сети Интернет. Анализ проведенных мероприятий

позволяет сделать вывод о том, что разработанные методические материалы положительно влияют на уменьшение интернет-зависимости у школьников. Данные материалы будет полезно использовать в практической работе учителям информатики школ.

Заключение

В современном обществе компьютер стал для ребенка и «другом» и «помощником» в том числе и «воспитателем», «учителем». Вместе с тем есть ряд весомых аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, нравственное, духовное здоровье подрастающего поколения, то есть представляющих для детей опасность. Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более важной в связи с существенным увеличением различных угроз и необходимостью осуществлять различную защиту пользователям, не достигшим совершеннолетия. Необходимо направить все усилия на защиту детей от опасной информации, причиняющей вред их здоровью и развитию. Развитие подрастающего поколения, знание ребенком навыков правильного выбора информации, а также умение ей пользоваться способствует развитию системы защиты прав детей.

В информатике введено понятие информационной безопасности. Это понятие имеет ряд определений. К настоящему времени выделены основные риски и угрозы информационной безопасности в сети Интернет.

Проанализировав научные статьи по выбранной теме можно сделать вывод: большинство российских и зарубежных ученых пытаются противостоять данной проблеме. Описывают различные технологии и методы борьбы за безопасность в сети. Но на практике видно, что очень трудно противостоять современному информационному обществу в котором очень большое количество опасной и вредоносной информации. Предлагается научить детей элементарным правилам по обеспечению безопасной работы. Это можно осуществить посредством проведения тематических уроков и внеклассных мероприятий по безопасности работы в Интернете для детей и проведением родительских собраний, посвященных решению указанной проблемы.

В учебниках по информатике и ИКТ также отражена исследуемая проблема и предлагаются некоторые способы ее решения. Пополнить знания учащихся по данной проблеме можно посредством проведения различных внеклассных мероприятий.

Изучив методы и средства решения проблемы были разработаны внеклассные мероприятия для учащихся и родительское собрание. В данных разработках были учтены все рекомендации, указанные в методической литературе. Мероприятия направлены на повышение уровня сознательности учащихся и их родителей при работе в сети Интернет с аудио, видео и текстовым контентом.

Таким образом, поставленные цель и задачи можно считать выполненными.

Разработанные нами материалы могут быть использованны учителями информатики и ИКТ в своей практической работе.

Библиографический список

1. Абраров Р.Д, Курязов Д.А [Текст]: «Информационная безопасность в компьютерных сетях». – 2016г. – № 9.5. Библиогр: 10-12 с.

2. Багрова Е.А, Лысакова И.В, к.п.н., Э.Г Счастная, В.П Малыш, М.В Салыгина [Текст]: Методические рекомендации «Безопасность школьников в сети Интернет». – 2017г.

3. Бадарч Дендев [Текст]: Информационные и коммуникационные технологии в образовании. – М.: ИИТО ЮНЕСКО., 2013г. Библиогр: 19-76 с.

4. Баскакова Н.И [Текст]: Рекомендации «Безопасный Интернет». – Тамбов: ТОИПКРО, 2011г. Библиогр: 27-90 с.

5. Безопасность в Интернете [Электронный ресурс]. Режим доступа http://www.intuit.ru/studies/courses/3462704/info. (дата обращения 11.11.2018 время 16:30)

6. Безопасность детей в Интернете [Электронный ресурс]. Режим доступа http://www.Microsoft.com/rus/childsafety . - Библиогр.: 16-17с. (дата обращения 04.10.2018 время 18:00)

7. Безопасный Интернет. – [Электронный ресурс]. – Режим доступа http://school385.ru/bezopinternet/ (дата обращения 04.10.2018 время 19:31)

8. Безопасный Интернет. – [Электронный ресурс]. – Режим доступа https://polzablog.ru/bezopasnost-v-seti-internet-dlya-detej.html (дата обращения 05.10.2018 время 20:00)

9. Безопасный Интернет. - [Электронный ресурс]. Режим доступа https://ishmurzino.02edu.ru/school/about/bezopasnost-v-seti-internet/ (дата обращения 05.10.2018 время 21:30)

10. Библиотека научных статей. Электронный ресурс. Режим доступа - [https://elibrary.ru/item.asp?id=23763782] Научная статья Беленов Н.В, Самсонова О.С .[Текст]: «Формирование навыков информационной безопасности в сети интернет у обучающихся 5-9 классов // Проблемы современной науки образования. – 2015г.- (дата обращения 06.10.2018 время 16:35)

11. Библиотека научных статей. Электронный ресурс. Режим доступа- [https://elibrary.ru/item.asp?id=32879947] Научная статья Неустроева А.А «О проблеме обеспечения безопасности школьников в информационной сфере России». (дата обращения 07.10.2018 время 17:00)

12. Библиотека научных статей. Электронный ресурс. Режим доступа - [https://elibrary.ru/item.asp?id=20587560]. Научная статья Желтова И.А «Сетевая культура и информационная безопасность школьников в интернет – пространстве». (дата обращения 08.10.2018 время 23:00)

13. Библиотека научных статей. Электронный ресурс. Режим доступа - [https://elibrary.ru/item.asp?id=28401037] Научная статья Неустроева А.А «Некоторые аспекты создания безопасного информационного пространства для школьников в социальной сети». (дата обращения 09.10.2018 время 11:00)

14. Босова Л.Л «Информатика и ИКТ». [Текст]: учебник для 9 класса / Л.Л Босова. – 4-е издание. М.: БИНОМ. Лаборатория знаний 2013 г. – Библиогр: 146-151 с.

15. Босова, Л.Л «Информатика». [Текст]: учебник для 7 класса / Л.Л Босова. – 4-е издание. М.: БИНОМ. Лаборатория знаний 2013 г. – Библиогр: 22-30 с.

16. Герасименко В.А Основы защиты информации. /В.А. Герасименко, А.А. Малкок.: - М.: Издательство МИФИ, 1997, - 537с.

17. Голубев, О.Б, Никифоров О.Ю. [Текст]: «Организация безопасного информационного пространства школьников в сети Интернет». – журнал «современные научные исследования и инновации». – 2014г.- №8.

18. Грин С., Фенвик Л., Киселев А., Кот Д. Демократии и диктатуры? // Дети в информационном обществе. — 2012. — № 11. — Библиогр: 10-15 с.

19. Днепров А.Г. Защита детей от компьютерных опасностей. [Текст]: А.Г. Днепров. – СПб. : Питер, 2008. -188с. – Библиогр.: 175-177 с.

20. Заботин, Ю.А. Интернет в вашем доме. / С.В. Гроднева, Ю.А Заботин. – М.6 рипол КЛАССИК, 2001.- 480с.

21. Информационная культура, информационная грамотность и компьютерная компетентность [Электронный ресурс] // МОО «Информация для всех» [Офиц. сайт]. Режим доступа- [http://www.ifap.ru/projects/infolit.htm]. (дата обращения 11.10.2018 время 13:00)

22. Крошилин С.В., Вехова Е.Л. Поддержка электронного обучения в социальных сетях. // Электронное обучение в непрерывном образовании. 2016. - № 1 (3). - . 1096-1105 с.

23. Лапчик, М.П. Методика преподавания информатики: [Текст]. Учеб. Пособие для студ. пед. Вузов / М.П. Лапчик, И.Г.Семакин, Е.К. Хеннер. – 2-е изд., стер. – М.: Издательский центр «Академия», 2005 г. – 624 с.

24. Лау Х. [Текст] Руководство по информационной грамотности для образования на протяжении всей жизни. — М.: МОО ВПП ЮНЕСКО «Информация для всех», 2007. –С. 616.

25. Обухович В.В. Интернет – безопасность школьник // Педагогика высшей школы. – 2016. - №3.1. – 149-151 с. [Электронный ресурс]. – режим доступа https://moluch.ru/th/3/archive/43/1468/ (дата обращения 13.10.2018 время 16:00)

26. Петровская Л. А. Компетентность в общении. Социально-психологический тренинг. — М.: МГУ, 1989. — 216 с. [Электронный ресурс]- режим доступа http://azbez.com/safety/intemet . (дата обращения 15.10.2018 время 14:20)

27. Парфентьев, У.В. Обеспечение безопасности несовершеннолетних в Интернете. [Текст] У.В. Парфентьев. – Народное образование. – 2009. - №7. – 320 с. Библиогр.: 261-289 с.

28. Руководящие указания для детей и молодых людей по защите в онлайновой среде. Электронный ресурс. Режим доступа -

http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/children/glchild 2009r.pdf. (дата обращения 25.10.2018 время 12:00)

29. Семакин, И.Г, Шестакова Л.В. «Информатика» [Текст]: учебник для 9 класса / И.Г. Семакин, Е.К, Хеннер. – М.: БЕНОМ. Лаборатория знаний, 2015 г. 185-196 с.

30. Семакин, И.Г, Шестакова Л.В. «Информатика». [Текст]: учебник для 8 класса / И.Г. Семакин, Е.К, Хеннер. – М.: БЕНОМ. Лаборатория знаний, 2015 г. 10-41 с.

31. Симонович, С.В. Компьютер в вашей школе: учебное пособие./ С.В. Симонович. – М.: АСТ ПРЕСС КНИГА ,2002. – 336 с. – Библиогр.: 254-256 с.

32. Склямина М.Ю «Обеспечение информационной безопасности учащихся в системе общего образования»//Молодой ученый. – 2015-№6.4-52-55 с.

33. Солдатова Г., Зотова Е., Чекалина А., Гостимская О. [Текст]: Пойманные одной Сетью: социально-психологическое исследование представлений детей и взрослых об Интернете. — М.: Фонд Раз- вития Интернет, 2011. — 176 с.

34. Угринович, Н.Д. «Информатика и ИКТ» [Текст]: учебник для 8 класса / Н.Д. Угринович. – 4-е изд. – М.: БИНОМ. Лаборатория знаний, 2015, 80 с. Библиогр.: 24-28 с.

35. Угринович, Н.Д. «Информатика и ИКТ» [Текст]: учебник для 9 класса / Н.Д. Угринович. – 6-е изд. – М.: БИНОМ. Лаборатория знаний, 2012, 90 с. Библиогр.: 34-35 с.

36. Электронный ресурс [http://www.YouTube.com/watch?v=HbVgg6-3EWo/]. Дата обращения 28.11. 2018 время 20:00)