МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
профессионального образования
«Алтайский государственный гуманитарно-педагогический университет
имени В.М. Шукшина»
(ФГБОУ ВО «АГГПУ»)
Физико-математический факультет
Кафедра физики и информатики

Обучение школьников методам и средствам защиты информации в глобальных сетях в базовом курсе информатики и ИКТ

Выпускная квалификационная работа

Допустить к защите

Зав. кафедрой
физики и информатики
канд. пед. наук, доцент
_____ Е.В. Дудышева
« ___ » _____ 2016 г.

Выполнила: **студентка группы**
Ф-ZИ111
Кривцова Ирина Эдуардовна
_____

Научный руководитель:
канд. пед. наук, доцент
Дудышева Елена Валерьевна
_____

Оценка _____

«____» _____ 2016 г.

Председатель ГАК _____

Бийск - 2016

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 Кривцовой Ирины Эдуардовны группы Ф-ZИ111

Направление педагогическое образование

Профиль (при наличии) информатика

Тема Обучение школьников методам и средствам защиты информации в глобальных сетях в базовом курсе информатики и ИКТ

Abstract:

This paper discusses issues related to the various aspects of teaching ways and means of information protection in the basic course of informatics and ICT.

Relevance of the topic of this work is due to the need to ensure safe schoolchildren work in the Internet.

The first chapter deals with the methodical fundamentals of training organization for self-working with information in global networks.

The second chapter is invited to consider health-saving aspects of students' self-working in the intern network. Lessons conspectus and extra-curricular activities, as well as recommendations for teachers have been developed.

Автор ВКР _____ Кривцова И.Э

(Подпись) (ФИО)

Руководитель ВКР _____ Дудышева Е.В.

(Подпись) (ФИО)

Оглавление

Введение

Перед каждым учителем непременно возникают проблемы: как обеспечить успешность каждого учащегося в обучении, каким образом обеспечить не механическое усвоение суммы знаний, а приобретение каждым учащимся в ходе учебных занятий социального опыта. Ответом может стать принцип дифференцированного подхода к обучению, а значит учета индивидуальных особенностей ребенка, при выборе форм контроля приобретенных знаний, умений и навыков. Учащийся сам, исходя из своих особенностей, возможностей и потребностей, определяет личную «траекторию» своего развития. Задачей же педагогов при осуществлении данного подхода в обучении становится создание таких педагогических условий, которые обеспечивали бы активное стимулирование у учащихся самоценной образовательной деятельности на основе самообразования, саморазвития, самовыражения в ходе овладения знаниями.

Основные умения по поиску информации и информационной безопасности школьники получают на уроках информатики и ИКТ при изучении темы «Методы и средства защиты информации». Однако мы считаем, что этого будет недостаточно и необходимо использовать все возможные способы обеспечения информационной безопасности и здоровьесбережения школьников.

Объектом данного исследования является процесс обучения школьников в базовом курсе информатики и ИКТ.

Предметом исследования является обучение школьников методам и средствам защиты информации в глобальных сетях в базовом курсе информатики и ИКТ.

Цель работы: разработка учебно-методических материалов по обучению школьников поиску информации в сети интернет.

Для достижения поставленной цели сформулированы следующие *задачи*:

1. Изучить предметный компонент обучения школьников поиску информации в сети интернет в базовом курсе информатики и ИКТ.

2. Рассмотреть здоровьесберегающие аспекты самостоятельной работы школьников в сети интернет и общие педагогические принципы самостоятельной работы.

3. Разработать план-конспекты уроков и внеклассного мероприятия по безопасной работе школьников в сети интернет.

4. Составить рекомендации для учителей для обеспечения мер по безопасной работе школьников в сети интернет.

Методы исследования:

1. Теоретические: анализ и обобщение научно-педагогической литературы, публикаций по теме исследования, анализ учебников, обобщение педагогического опыта.

2. Эмпирические: педагогическое наблюдение, рефлексивный анализ.

Новизна работы состоит в рассмотрении аспекта здоровьесбережения при организации самостоятельного поиска информации школьниками в сети интернет.

Практическая значимость заключается в разработке содержания занятий для обучения школьников методам и средствам защиты информации, а также рекомендаций учителям по организации безопасной работы в сети интернет.

Дипломная работа состоит из введения, двух глав, заключения и библиографического списка.

Глава 1. Методические основы организации занятий по самостоятельной работе с информацией в глобальных сетях

1.1 Предметный компонент обучения школьников поиску в сети интернет в базовом курсе информатики и ИКТ

Хорошо известно, что достижения в обучении подростков во многом зависят от содержания и структуры учебника, по которому они занимаются. По одним учебникам школьники работают с удовольствием (разбирают, анализируют рисунки, активно выполняют предлагаемые задачи). Другие учебные тексты воспринимаются иначе; видно, что большая часть школьников с неохотой открывают учебник, находят нужный текст и равнодушно начинают работать с ним.

Главная задача базового уровня старшей школы заключается в изучении общих закономерностей функционирования, формирования и использования информационных систем, преимущественно автоматизированных. С точки зрения содержания это дает возможность сформировать основы системного видения мира, расширить возможности информационного моделирования, обеспечив тем самым существенное расширение и углубление межпредметных взаимосвязей информатики с иными дисциплинами. С точки зрения деятельности, это предоставляет возможность создать методологию применения основных автоматизированных информационных систем в решении определенных задач, связанных с анализом и представлением основных информационных процессов. Постараемся сравнить популярные школьные учебники с позиций легкости восприятия и доступности освоения учебного материала.

В современной школе наибольшее распространение получили учебники следующих авторов: Угринович Н.Д. [44], Макарова Н.В. и др. [18] и учебник Семакина И.Г. и др. [40], причем отмечается неоднозначный подход педагогов к данным учебникам. В методической литературе

существуют и позитивные и негативные отзывы о них; авторы различных статей полагают, что некоторые учебники негодны для современной школы, другие же, напротив, восторгаются тем или иным подходом автора к изложению школьного курса информатики. Одних интересует строгий аксиоматический подход, других большие возможности для организации мыслительной деятельности обучающихся.

В учебнике [18] изложено меньше материала по теме глобальные сети и интернет технологии, чем у [44] и [40]. Материал изложен более компактно, мало совпадающих тем, но есть темы, которые не затрагиваются в учебниках [40] и [44].

В учебнике [40] уроки по теме глобальные сети и интернет технологии сформулированы наиболее компактно, легче запоминается, но в тоже время сжатость не всегда дает возможность наиболее широко и подробно изучить весь материал, то есть этот учебник позволяет просто и легко изучить базовый материал, но не более того.

В учебнике [44] уроки по теме глобальные компьютерные сети разобраны наиболее подробно и обширно, что дает возможность изучить необходимый материал глубоко. Материал изложен просто, что позволяет основной массе школьников усвоить каждую тему. Каждая глава изложена подробно, что позволяет изучить многие материалы больше базового курса.

Хотелось бы подробнее остановиться на теме «Глобальные компьютерные сети», а также на теме поиск информации в компьютерных сетях.

Поиск информации всегда ориентирован на самостоятельную деятельность учащихся – индивидуальную, парную, групповую, которую учащиеся выполняют в течение определенного отрезка времени [7.с 54]. Самостоятельная работа подробно описана в следующем параграфе.

Как мы видим, тема «Глобальные компьютерные сети» может подходить, чтобы по ней осуществлять самостоятельную деятельность

учащихся. Что немало важно, ведь самостоятельная работа с информацией – это метод, в ходе которого у школьников формируются универсальные способы учебной деятельности, что дает толчок к саморазвитию, к самоанализу, самоцелеполаганию, самоорганизации, самоконтролю и самооценке, а также существенно расширяется круг интересов в предметных областях и происходит непроизвольное усвоение учебного материала и запоминание алгоритма научного исследования [4.с 33].Мы считаем, что это также относится к работе в глобальных сетях.

В ряде научных статей на тему поиска информации в глобальных сетях, например, в работе Павла Колесникова [48] указывается то, что работать с поисковой системой приходится достаточно сложно и это не сводится к простому вводу запроса в браузере, а для этого требуются определенные знания. И учитель, в свою очередь, должен помочь детям получить эти знания.

Рассмотрим понятия, связанные с безопасным поиском информации, так как это является близкой темой нашей работы.

Под понятиями "защита информации" и "информационная безопасность" понимается совокупность методов, средств и мероприятий, предназначенных для недопущения искажения, уничтожения или несанкционированного использования данных [12, с. 82].

Постоянно возрастающие объемы данных в информационных системах, расширение круга пользователей, обеспечение удаленного доступа пользователей к информационным ресурсам делают проблему защиты информации особенно актуальной. Проблем с информационной безопасностью очень много и подробно представлены в работе [46]

Проблемы защиты информации от искажения при ее передаче по каналам связи в условиях естественных помех возникли давно. Наиболее исследованным является случай, когда рассматриваются сообщения, элементы которых могут принимать два значения (обычно 0 и 1), и в качестве

помехи рассматривается инверсия элемента сообщения (превращение 0 в 1 или 1 в 0) [27, с. 38].

Существуют два способа описания помех: вероятностный и теоретико-множественный. В первом случае задаются вероятности искажения символов. Обычно, рассматривают симметричный канал связи, в котором вероятности искажения символов одинаковы. Во втором случае задается максимальное число искаженных символов в принятом сообщении.

Под несанкционированным доступом будем понимать использование информации лицом, не имеющим на это право. Для борьбы с этим применяются системы паролей или шифрование информации [46, с. 116].

Эффективная защита информации от несанкционированного изменения, в том числе и подмены, в настоящее время осуществляется с использованием криптографических методов.

Попытка нарушения информационной безопасности называется угрозой. Различают угрозы случайные и преднамеренные. Преднамеренные угрозы обычно направлены на системы обработки данных (СОД). Под объектом защиты понимается компонент системы, в котором находится или может находиться интересующая злоумышленника информация, а под элементом защиты – эта информация.

Основными источниками, которые могут привести к нарушению информации, являются люди, модели, алгоритмы и программы, технические устройства, информационные технологии, внешняя среда.

Объектами защиты информации в системе обработки данных могут быть ПК и рабочие станции компьютерной сети, узлы связи, хранилища носителей информации, средства документирования информации, сетевое оборудование и внешние каналы связи, накопители и носители информации.

Перечислим основные принципы построения систем защиты информации:

1. системность (необходимость учета всех элементов, условий и факторов, существенно влияющих на безопасность системы),

2. комплексность (согласованное применение разнородных средств для перекрытия всех существенных каналов реализации угроз и ликвидации слабых мест на стыках компонентов системы),

3.непрерывность (принятие соответствующих мер на всех этапах жизненного цикла защищаемой информационной системы),

4.разумная достаточность

5. открытость используемых классов алгоритмов и механизмов защиты (конечно, пароли, ключи и т.п. являются секретными). Открытость. Исходный код всех версий программ кодирования доступен в открытом виде. Любой эксперт может убедиться в том, что в программе эффективно реализованы криптоалгоритмы. Так как сам способ реализации известных алгоритмов был доступен специалистам, то открытость повлекла за собой и другое преимущество - эффективность программного кода

6.гибкость управления и применения

7.простота применения защитных мер и средств (законный пользователь не должен иметь специализированных знаний).

При создании систем защиты информации используются различные комплексы средств:

- организационно-распорядительные,
- технические,
- программно-аппаратные.

Организационно-распорядительные средства защиты заключаются в регламентации доступа к информационным и вычислительным ресурсам, функциональным процессам СОД, к регламентации деятельности персонала и т.п. Целью этих средств является наибольшее затруднение или исключение возможности реализации угроз безопасности [46, с. 93].

Технические средства защиты используются для создания вокруг объекта и элементов защиты замкнутой среды (затруднение доступа к объекту). В их состав входят такие мероприятия как: установка физической преграды, ограничение электромагнитного излучения, обеспечение автономными источниками питания оборудования, обрабатывающего ценную информацию, применение жидкокристаллических или плазменных дисплеев и струйных и плазменных принтеров с низким уровнем электромагнитного и акустического излучения, использование индивидуальных средств защиты аппаратуры в виде кожухов, крышек с установкой средств контроля вскрытия аппаратуры.

Программные и программно-аппаратные средства и методы защиты широко используются для защиты информации в ПК и компьютерных сетях. Они осуществляют разграничение и контроль доступа к ресурсам, регистрацию и анализ протекающих процессов, событий, пользователей, предотвращают возможные деструктивные воздействия на ресурсы, осуществляют криптографическую защиту информации, идентификацию и аутентификацию пользователей.

В программно-аппаратных средствах защиты информации секретные ключи и алгоритмы реализованы в виде небольших технических устройств, подключаемых к компьютеру. Это существенно затрудняет их копирование (в отличие от дискет) [22, с. 72].

Технологические средства защиты информации органично встраиваются в технологические процессы обработки информации. К ним относятся создание архивных копий носителей, сохранение обрабатываемых данных во внешней памяти компьютера, регистрация пользователей в журналах, автоматическая регистрация доступа пользователей к ресурсам.

К *правовым* и морально-этическим средствам защиты информации относятся действующие законы, нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушение;

нормы поведения, соблюдение которых способствует защите информации [42, с. 25].

Рассмотрим *физические методы* защиты данных. В настоящее время наилучшим образом проявили себя структурированные кабельные системы, использующие одинаковые кабели для передачи данных в локальной вычислительной сети, телефонной сети, сетей пожарной и охранной сигнализации, сетей передачи данных системы видеонаблюдения. Название "структурированность" означает, что кабельную систему здания можно разделить на несколько уровней.

Для обеспечения надежной работы компьютеров и компьютерных сетей и для предотвращения потерь информации при кратковременных неполадках в системах электропитания необходимы специальные меры защиты. Наиболее надежным средством защиты в настоящее время является установка источников бесперебойного питания. Различные по своим техническим характеристикам, эти устройства могут обеспечить надежную защиту от кратковременных скачков напряжения в сети питания [12, с. 22].

Несмотря на все предосторожности, связанные с защитой данных от перепадов напряжения или неполадок в кабельной системе, возможны ситуации, когда эти проблемы все же могут привести к потере информации. Поэтому необходимо провести предварительное дублирование и архивирование информации.

В крупных локальных сетях не так уж редки случаи заражения отдельных компьютеров или целой группы компьютеров различными вирусами. Наиболее распространенными методами защиты от вирусов по сей день остаются всевозможные антивирусные программы [46, с. 49].

Однако все чаще и чаще защита с помощью антивирусных программ становится недостаточно эффективной. В связи с этим, распространение получают программно-аппаратные методы защиты. На сегодняшний день уже существует достаточное количество устройств, "умеющих" защищаться

от вирусов. Уже в 1994 году корпорация Intel разработала оригинальное решение для защиты от вирусов в компьютерных сетях. Сетевые адаптеры Ethernet в Flash-памяти содержат антивирусную программу. И вся информация сканируется на наличие вирусов. Преимущества такой технологии очевидны: во-первых, при сканировании не тратятся ресурсы процессора, т.к. он практически не включен в эту работу, и, во-вторых, вся проверка идет автоматически, без участия пользователя. Система просто не пустит вирусы на ваш компьютер [15, с. 184].

Проблема защиты данных, как уже говорилось ранее, предусматривает в себе такой важный раздел, как защита от несанкционированного доступа. Сама же проблема доступа к данным включает в себя и вопрос разграничения полномочий между пользователями. Каждый пользователь имеет свой индивидуальный пароль, открывающий только определенную информацию, доступную именно этому пользователю. В этом и заключается слабое место: пароль можно подсмотреть, подобрать. Поэтому система контроля доступа к информации усложнилась, и появились устройства контроля индивидуальных параметров человека, например, отпечатки пальцев, рисунки радужной оболочки глаз и т.п.

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации [11, с. 215].

Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства. Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств защиты информации. Из наиболее часто упоминаемых решений

следует отметить следующие две системы, позволяющие ограничить и контролировать информационные потоки.

Межсетевые экраны (также называемые брандмауэрами или файрволами — от нем. Brandmauer, англ. Firewall — «противопожарная стена»). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой [10, с. 245].

Proxy-servers (proxy — доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях — например, на уровне приложения (вирусы, код Java и JavaScript).

VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.

Таким образом, мы видим, что необходимо научить детей в школе правильно осуществлять поиск информации в глобальных сетях. Так как на уроках информатики нет возможности потренироваться в поиске информации, мы предлагаем провести внеклассное мероприятие, где школьники должны выполнить некоторые задания, способствующие развитию навыков быстрого поиска нужной информации в глобальных сетях.

В рамках базового курса информатики предлагаем разработку уроков: «Компьютерные вирусы и антивирусные программы», «Www.путешествие по всемирной паутине».

1.2. Здоровьесберегающие аспекты самостоятельной работы школьников в сети интернет

Информация может быть представлена в бумажном виде, в качестве учебников и пособий, а также в электронном варианте. Поскольку электронные тексты наиболее доступны, школьники прибегают к возможности поиска в сети Интернет. Работа с такими текстами имеет самостоятельный характер. В связи с этим, важно сообщить ученикам о здоровьесберегающих аспектах при работе с информацией в сети.

Современные школьники массово пользуются возможностями поиска информации в сети интернет. Но, к сожалению, негативное влияние средств массовой информации и рекламы, размещенные в открытом доступе, способствуют развитию вредных привычек у подрастающего поколения. Поэтому задача педагогов как можно чаще обращаться к темам здоровья и его сбережения. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» [45] способствует соблюдению условий информационной безопасности личности, но важнейшее значение целенаправленное формирование грамотного отношения школьников к своему здоровью со стороны учителей [3, с.83]. Важно не только проводить беседы, но в доступной и неформальной форме, в учебной и во внеклассной деятельности подталкивать ребенка к самостоятельной работе над собой, умению сопротивляться негативным воздействиям.

Основные умения по поиску информации и информационной безопасности школьники получают на уроках информатики и ИКТ [25, с. 177]. Поиск информации ориентирован на самостоятельную деятельность учащихся, в качестве заданий можно выбирать различные темы для поиска.

При этом поиск информации распространяется на всю учебную деятельность, на все предметы, в том числе, на информацию о собственном здоровье и безопасности.

Так как на уроках информатики и ИКТ не имеется возможность в полной мере потренироваться в поиске информации именно о здоровье, мы поддерживаем проведение внеклассных мероприятий [15, с.83], где ученики могут выполнять задания, способствующие развитию навыков быстрого поиска информации в сети интернет и при этом получить важную информацию о здоровом образе жизни. Внеклассное мероприятие хорошо подходит для того, чтобы развивать у учеников навыки самостоятельности, самоанализа и самоконтроля. Мы считаем, что здоровье будущего поколения – очень актуальная тема для нашего общества, поэтому разработали внеклассное мероприятие на тему «Формирование навыков школьников в области информационной безопасности и здоровьесбережения при самостоятельном поиске в сети интернет», проведенное с учениками девятого класса.

Рассмотрим педагогические основы самостоятельной работы школьников.

П.И. Пидкасистый указывает на то, что для того, чтобы создать условия для самостоятельной работы школьникам необходимо:

- обеспечение учеников необходимыми учебно-методическими материалами;
- обеспечение доступа школьников к информационным ресурсам сети Интернет;
- обеспечение школьников контролирующими материалами (тестами, заданиями и др.);
- предоставление ученикам перечня необходимой основной и дополнительной литературы [34, с. 114].

Самостоятельная работа способна реализоваться персонально или группами учащихся в зависимости от цели, тематики, степени сложности определенной самостоятельной деятельности, уровня знаний и умений учащегося.

Учитель обязан постепенно готовить ученика к результативной работе не только лишь во время аудиторных занятий, но и во внеучебное время. Каждое действие учащегося в ходе самостоятельной внеаудиторной работы должно быть подготовлено. Было бы не только бесполезно, но и нежелательно давать на дом такие задания, к выполнению которых ученики еще не готовы. Подобные задания приводят в лучшем случае к массовому списыванию или невыполнению основной массой школьников, более того, выполняя подобные задания, ученики будут закреплять неверные действия и ошибки. По этой причине необходимо говорить о выборе общедоступных заданий для самостоятельной работы.

Под самоуправляемой самостоятельной работой учеников в ходе подготовки по информационно-ориентированным специальностям понимается такого рода работа, в процессе которой ученик, следуя специальными методическими предписаниями педагога, обретает и улучшает знания, умения и навыки, накапливает навык самостоятельной деятельности в информационной среде.

Эффективность самостоятельной работы достигается, в случае если она является одним из сложных, базисных компонентов учебного процесса, и для нее предусматривается специальное время на каждом занятии, если она ведется регулярно и систематически, а не случайно и эпизодически.

Только при этом условии у учеников формируются устойчивые умения и способности в выполнении различных типов самостоятельной работы и наращиваются темпы в ее исполнении. При отборе типов самостоятельной работы, при определении ее объема и содержания необходимо придерживаться, как и во всем процессе обучения, главными принципами

дидактики. Наиболее важную роль в данном процессе имеют принципы доступности и систематичности, взаимосвязь теории с практикой, принцип постепенности в нарастании трудностей, принцип творческой активности, а кроме того правило дифференцированного подхода к ученикам.

Понятие самостоятельная работа применяется многими авторами в разном значении. Различные трактовки зависят, прежде всего, от того, какое содержание вкладывается в слово «самостоятельная». В основном встречаются три значения этого определения:

– обучающийся обязан выполнять работу сам, без непосредственного участия педагога;

– от обучающегося необходимы самостоятельные мыслительные действия, самостоятельное ориентирование в учебном материале;

– выполнение работы строго не регламентировано, обучаемому представляется свобода выбора содержания и методов выполнения задачи.

Именно самостоятельная работа формирует высокую культуру интеллектуального труда, которая подразумевает не только технику чтения, изучение книги, ведение записей, а, в первую очередь, потребность в самостоятельной деятельности, желание понять суть вопроса, идти вглубь ещё не решенных проблем. В процессе такого труда наиболее полно обнаруживаются индивидуальные способности учеников, их наклонности и круг интересов, которые содействуют формированию умения анализировать факты и явления, учат самостоятельному мышлению, которое приводит к творческому развитию и формированию своего мнения, собственных взглядов, представлений, своей позиции.

Учитель информатики, ровно, как и любой другой предметник, в своей педагогической работе должен решать самые разнообразные проблемы. Но именно преподаватель информатики встречается с максимальным разбросом знаний, умений и навыков учащихся по своему предмету в рамках одного класса. Причины этого понятны.

Во-первых, те учащиеся, у которых дома есть компьютер, как правило, на порядок выше по уровню знаний и умений, нежели ученики, не имеющие возможности пользоваться компьютером в домашних условиях.

Во-вторых, компьютер дает возможность ученикам заниматься творческой деятельностью. Но для этого школьники должны иметь доступ к компьютеру, отсутствие такой возможности весьма снижает творческий потенциал ученика.

В современной школе трудности, связанные с различным уровнем знаний и умений учеников, чаще всего решаются применением «технологии дифференциации по уровню». Но разделение по уровню интеллектуального развития, навыков и умений не получает в современной педагогике однозначной оценки. В ней наравне с позитивными имеются и отрицательные аспекты. Значительную часть негативных моментов, возможно, избежать или скомпенсировать при последовательном и педагогически правильном подходе.

Наиболее эффективным способом формирования учебно-информационных умений и навыков на уроке информатики является самостоятельная работа учащихся. Организация самостоятельной работы возможна на всех этапах изучения материала: формирования новых знаний, закрепления изученного материала и обобщения и систематизации знаний.

Рассмотрим виды самостоятельной работы.

В.И. Тихонова рассматривает такие виды самостоятельной работы, как: репродуктивная самостоятельная работа: самостоятельное чтение, просмотр, конспектирование учебной литературы, прослушивание лекций, магнитофонных записей, заучивание, пересказ, запоминание, Интернет-ресурсы, возобновление учебного материала [43, с.26].

Познавательно-поисковая самостоятельная работа: подготовка сообщений, докладов, выступлений на семинарских и практических

занятиях, отбор литературы сообразно дисциплинарным проблемам, написание рефератов, контрольных, курсовых работ и др.

Творческая самостоятельная работа: написание рефератов, научных статей, роль в научно-исследовательской работе, подготовка дипломной работы (проекта). Выполнение особых заданий и др., участие в студенческой научной конференции.

Самостоятельная работа содействует развитию таких умений как, анализ, суждение, сравнение, сопоставление, умение делать логические выводы, поиск новейших решений. Кроме этого, участие в самостоятельной деятельности формирует у учащихся познавательный энтузиазм, дает позитивную мотивацию к обучению, развивает интеллектуальную сферу личности, формирует умения и навыки в определенной сфере деятельности.

В современном мире ребенку становится все труднее и труднее ориентироваться в потоке информации. Появляется потребность в оптимизации ее поиска и отбора. В свете изменившейся парадигмы образования появляется проблема формирования у учащихся обще учебных умений, которые позволят им самостоятельно приобретать знания и умения при обучении любому предмету, в том числе и информатике. Одним из направлений решения этой проблемы является формирование у учащихся учебно-информационных умений, позволяющее вооружить ими учащихся в соответствии с требованиями современного информационного общества.

Л.Г. Веткин говорит нам о том, что индивидуально-групповая деятельность на уроке информатики складывается из следующих элементов:

- Предварительная подготовка учащихся к выполнению группового задания, постановка учебных задач, краткий инструктаж.
- Обсуждение и составление плана выполнения учебного задания в группе, распределение обязанностей.
- Работа по выполнению учебного задания.

- Наблюдение за работой и корректировка работы группы и отдельных учащихся.
- Взаимная проверка и контроль над выполнением задания в группе.
- Сообщение учащихся по вызову преподавателя о полученных результатах, общая дискуссия в группе под руководством преподавателя, добавление и исправление, дополнительная информация преподавателя и формирование окончательных выводов.
- Индивидуальная оценка работы групп и общей работы в целом [4, с. 24].

Вывод по 1 главе

В первой главе нами были подробно рассмотрены и описаны методы и средства защиты информации. Проведен сравнительный анализ отдельных тем из учебников базового курса информатики. Авторы учебников дают только основу знаний по теме компьютерные сети. Во втором параграфе мы рассмотрели понятие и виды самостоятельной работы, а также оценили важность самостоятельной работы в учебном процессе в рамках дисциплины «Информатика и ИКТ».

Глава 2. Учебно-методические материалы по обучению школьников поиску информации в сети интернет

2.1 Разработка уроков для базового курса информатики и ИКТ по работе с информацией в глобальных сетях

Из всех действующих учебников информатики за 8 класс мы выбрали учебник Н.Д. Угриновича. На тему компьютерные вирусы и антивирусные программы, согласно рабочей программе, отводится 1 час, а на тему компьютерные сети 5 часов. Ниже представлены конспекты уроков по теме компьютерные вирусы и антивирусные программы и WWW путешествие по всемирной паутине.

2.1.1. План-конспект урока по теме « Компьютерные вирусы и антивирусные программы»

Цель урока: ознакомление учащихся с путями распространения и методами борьбы с компьютерными вирусами.

Тип урока: урок объяснения нового материала.

Задачи урока:

Обучающие:

- сформировать знания о видах вирусов;
- способствовать овладению знаниями о способах защиты компьютера от вирусов;

Развивающие:

- способствовать развитию логического и критического мышления, культуры речи;
- развивать умение обобщать и синтезировать знания;
- планировать свою деятельность.

Воспитательные:

- воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению;
-

Структура урока:

1. Организационный момент (2 мин)
2. Информационная минутка (5 мин).
3. Изучение нового материала (24 мин)

– понятие компьютерного вируса и троянской программы. Признаки заражения компьютера;

– пути проникновения вируса в компьютер;

– типы компьютерных вирусов;

– методы защиты от компьютерных вирусов;

– антивирусные программы и лечение зараженных дисков.

4. Актуализация знаний (4 мин).
5. Практическая работа «Защита от вирусов: обнаружение и лечение» (8 мин)
6. Домашнее задание (2 мин).

Здравствуйте, ребята! Так же как человек, компьютер тоже может заразиться вирусом. И причиной заражения действительно является вирус, только компьютерный. Который так же проникает в «организм» компьютера из внешней среды, и начинает размножаться, передвигаться и самопроизвольно внедряться в другие объекты, (файлы, диски, программы). Постарайтесь сами сформулировать и дать определение, что же такое компьютерный вирус?

Компьютерный вирус – это программа, способная создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя..

Свое название компьютерный вирус получил за некоторое сходство с биологическим вирусом (например, в зараженной программе самовоспроизводится другая программа – вирус, а инфицированная программа может длительное время работать без ошибок, как в стадии инкубации).

Программа, внутри которой находится вирус, называется зараженной программой.

Когда инфицированная программа начинает работу, то сначала управление получает вирус. Вирус заражает другие программы, а также выполняет запланированные деструктивные действия. Для маскировки своих действий вирус активизируется не всегда, а лишь при выполнении определенных условий (истечение некоторого времени, выполнение определенного числа операций, наступления некоторой даты или дня недели и т.д.).

После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится. Внешне зараженная программа может работать так же, как и обычная программа. Подобно настоящим вирусам компьютерные вирусы прячутся, размножаются и ищут возможность перейти на другие ЭВМ.

Таким образом, вирусы должны инфицировать ЭВМ достаточно незаметно, а активизироваться лишь через определенное время (время инкубации). Это необходимо для того, чтобы скрыть источник заражения.

Вирус не может распространяться в полной изоляции от других программ. Очевидно, что пользователь не будет специально запускать одинокую программу-вирус. Поэтому вирусы прикрепляются к телу других полезных программ.

Несмотря на широкую распространенность антивирусных программ, предназначенных для борьбы с вирусами, вирусы продолжают плодиться. В среднем в месяц появляется около 300 новых разновидностей. Естественно, что вирусы появляются не самостоятельно, а их создают *кракеры* – вандалы (техно – крысы). Все пользователи лютой ненавистью ненавидят кракеров.

Различные вирусы выполняют различные действия:

– Выводят на экран мешающие текстовые сообщения (поздравления, политические лозунги, фразы с претензией на юмор, высказывания обиды

от неразделенной любви, нецензурные выражения, рекламу, прославление любимых певцов, названия городов);

- Создают звуковые эффекты (проигрываю гимн, гамму или популярную мелодию);
- Создают видеоэффекты (переворачивают или сдвигают экран, имитируют землетрясение, вызывают падение букв в тексте или симулируют снегопад, имитируют скачущий шарик, прыгающую точку, выводят на экран рисунки и картинки);
- Замедляют работу ЭВМ, постепенно уменьшают объем свободной оперативной памяти;
- Увеличивает износ оборудования (например, головок дисководов);
- Вызывают отказ отдельных устройств, зависание или перезагрузку компьютера и крах работы всей ЭВМ;
- Имитируют повторяющиеся ошибки работы операционной системы (например, с целью заключения договора на гарантированное обслуживание ЭВМ);
- Уничтожают FAT – таблицу, форматируют жесткий диск, стирают BIOS, стирают или изменяют установки CMOS, стирают секторы на диске, уничтожают или искажают данные, стирают антивирусные программы;
- Осуществляют научный, технический, промышленный и финансовый шпионаж;
- Выводят из строя системы защиты информации, дают злоумышленникам тайный доступ к вычислительной машине;
- Делают незаконные отчисления с каждой финансовой операции и т.д.;

Главная опасность самовоспроизводящихся кодов заключается в том, что программы – вирусы начинают жить собственной жизнью, практически не зависящей от разработчика программы. Так же, как в цепной реакции в ядерном реакторе, запущенный процесс трудно остановить.

Основные симптомы вирусного заражения ЭВМ следующие.

- Замедление работы некоторых программ.
- Увеличение размеров файлов (особенно выполняемых).
- Появление не существовавших ранее “странных” файлов.
- Уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы).
- Внезапно возникающие разнообразные видео и звуковые эффекты.
- Появление сбоев в работе операционной системы (в том числе зависание).
- Запись информации на диски в моменты времени, когда этого не должно происходить.
- Прекращение работы или неправильная работа ранее нормально функционирующих программ.

Впервые большое внимание к проблеме вирусов привлекла книга Фреда Коэна «Компьютерные вирусы, теория и эксперименты» вышедшая в свет в 1984 г.

Большой общественный резонанс вызвало первое неконтролируемое распространение вируса в сети. 2 ноября 1988 года двадцатитрехлетний студент последнего курса Корнельского университета Роберт Таппан Моррис запустил в сети свою программу, которая из-за ошибки начала бесконтрольное распространение и многократное инфицирование узлов сети. В результате было заражено около 6200 машин, что составило 7,3 % общей численности машин в сети.

Существует большое число различных классификаций вирусов.

По *среде обитания* они делятся на сетевые, файловые, загрузочные и файлово–загрузочные вирусы.

По *способу заражения* – на резидентные и нерезидентные вирусы.

По *степени опасности* – на неопасные, опасные и очень опасные вирусы.

По особенностям алгоритма – на вирусы-компаньоны, паразитические вирусы, репликаторы (черви), невидимки (стелс), мутанты (призраки, полиморфные вирусы, полиморфики), макро-вирусы, троянские программы.

По целостности – на монолитные и распределенные вирусы.

По алгоритмической сущности вирусы подразделяются на:

- вирусы-«черви» – распространены в компьютерных сетях;
- вирусы-невидимки – перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо них незараженные объекты;
- вирусы-мутанты – самовоспроизводясь, воссоздают копии, явно отличающиеся от оригинала;
- вирус-«троянский конь» – это программа, которая, маскируясь под полезную программу, выполняет дополнительные функции, о которых пользователь не догадывается.

Классификация компьютерных вирусов

По среде обитания различаются загрузочные вирусы (внедряются в сектор, содержащий программу загрузки системного диска), файловые вирусы (внедряются в основном в исполняемые файлы с расширением COM и EXE), сетевые вирусы (обитают в компьютерных сетях), системные вирусы (проникают в системные модули, поражают программы-интерпретаторы).

По степени воздействия вирусы подразделяются на:

- неопасные вирусы – они не разрушают файлы, но могут переполнять оперативную и дисковую память, выводить на экран различные графические эффекты;
- опасные вирусы – приводят к различным нарушениям в работе компьютера;
- очень опасные вирусы – это вирусы разрушительные, они приводят к стиранию информации, полному или частичному нарушению работы прикладных программ.

По способу заражения вирусы подразделяются на:

– резидентные вирусы – при заражении компьютера они оставляют в оперативной памяти свою резидентную часть, которая затем при каждом обращении к операционной системе и к другим объектам внедряется в них и выполняет свои разрушительные действия до выключения или перезагрузки компьютера;

– нерезидентные вирусы – не заражают оперативную память.

Сетевые вирусы распространяются по различным компьютерным сетям.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot – сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record – MBR). Некоторые вирусы записывают свое тело в свободные сектора диска, помечая их в FAT – таблице как “плохие” (Bad cluster).

Файловые вирусы инфицируют исполняемые файла компьютера, имеющие расширения com и exe. К этому же классу относятся и макровирусы, написанные помощью макрокоманд. Они заражают неисполняемые файлы (например, в текстовом редакторе MS Word или в электронных таблицах MS Excel).

Загрузочно – файловые вирусы способны заражать и загрузочные секторы и файлы.

Резидентные вирусы оставляют в оперативной памяти компьютера свою резидентную часть, которая затем перехватывает обращения неинфицированных программ к операционной системе, и внедряются в них. Свои деструктивные действия и заражение других файлов, резидентные вирусы могут выполнять многократно.

Нерезидентные вирусы не заражают оперативную память компьютера и проявляют свою активность лишь однократно при запуске инфицированной программы.

Действия вирусов могут быть *не опасными*, например, на экране появляется сообщение: “Хочу чучу”. Если с клавиатуры набрать слово “чуча”, то вирус временно “успокаивается”.

Значительно опаснее последствия действия вируса, который *уничтожает часть файлов* на диске.

Очень опасные вирусы самостоятельно форматируют жесткий диск и этим уничтожают всю имеющуюся информацию. Примером очень опасного вируса может служить вирус CIN (Чернобыль), активизирующийся 26 числа каждого месяца и способный уничтожать данные на жестком диске и в BIOS.

Компаньон-вирусы (companion) – это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE – файлов новые файлы-спутники (дубликаты), имеющие то же самое имя, но с расширением COM, например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM – файл и никак не изменяет одноименный EXE – файл. При запуске такого файла DOS первым обнаружит и выполнит COM – файл, т.е. вирус, который затем запустит и EXE – файл.

Паразитические вирусы при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу относятся все вирусы, которые не являются “червями” или “компаньонами”.

Вирусы – *черви* (worm) – распространяются в компьютерной сети и, так же как и компаньон – вирусы, не изменяют файлы или секторы на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Черви уменьшают пропускную способность сети, замедляют работу серверов.

Репликаторы могут размножаться без внедрения в другие программы и иметь «начинку» из компьютерных вирусов.

Вирусы–*невидимки* (стелс – Stealth) используют некоторый набор средств для маскировки своего присутствия в ЭВМ. Название вируса аналогично названию американского самолета – невидимки.

Стелс–вирусы трудно обнаружить, так как они перехватывают обращения операционной системы к пораженным файлам или секторам дисков и «подставляют» незараженные участки файлов.

Вирусы, которые шифруют собственное тело различными способами, называются *полиморфными*. Полиморфные вирусы (или вирусы – призраки, вирусы – мутанты, полиморфики) достаточно трудно обнаружить, так как их копии практически не содержат полностью совпадающих участков кода. Это достигается тем, что в программы вирусов добавляются пустые команды (мусор), которые не изменяют алгоритм работы вируса, но затрудняют их выявление.

Макро-вирусы используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы и электронные таблицы) распространяются макро – вирусы, заражающие документ Word и Excel.

В настоящее время широко Компьютерные вирусы бывают следующих типов:

1) Файловые вирусы, поражающие exe и .com файлы, иногда только com. Первым заражается командный процессор, а через него все остальные программы. Наиболее опасны резидентные вирусы, которые остаются в оперативной памяти постоянно. Заражение происходит при запуске зараженной программы (хотя бы однократном), то есть когда вирус получает управление и активизируется. Такие вирусы портят программы и данные, но иногда могут уничтожить содержимое всего жесткого диска.

2) Загрузочные или бутовые вирусы – поражают загрузочные сектора жестких дисков и дискет. Они наиболее опасны для компьютера, так как в результате их разрушительной работы компьютер перестает загружаться, иногда сразу после заражения, которое происходит даже при выводе

оглавления зараженной дискеты.

3) Вирусы, поражающие драйверы, указанные в файле config.sys, и дисковые файлы DOS. Это ведет к прекращению загрузки компьютера.

4) Невидимые или стелс-вирусы. Их очень трудно обнаружить. Простейший способ маскировки - при заражении файла вирус делает вид, что длина файла не изменилась.

5) Сетевые вирусы – поражают машины, работающие в сети, в том числе в сети Интернет.

6) Вирусы Word (6.0 и старше), Excel, Access, PowerPoint – поражают документы и макросы программ из MS Office.

7) Вирусы Windows-95/98 – функционируют и портят данные в среде Windows – 95/98.

Один из самых опасных из всех известных вирусов из Интернета – вирус "Чернобыль". Вирус активизируется 26 апреля, но модификации вируса могут принести вред и 26 числа каждого месяца. Кроме порчи информации на диске, он перепрограммирует BIOS (CMOS Setup) компьютера и компьютер перестает загружаться. Приходится обращаться в мастерскую и восстанавливать BIOS.

Вирус ILOVEYOU филиппинского происхождения, распространялся по E-mail. Он вывел из строя 45 млн. компьютеров во всем мире, в том числе в Пентагоне, ЦРУ, ФБР в США, Форин-офисе Великобритании и в других крупнейших странах. Вскоре вирус мутировал, так как были созданы его разновидности, и нанес дополнительный ущерб. Основная вирусная атака произошла 4 мая 2000 г. Вирус уничтожал графические .jpg и звуковые .mp3 файлы. Материальный ущерб составил около 10 миллиардов $ (USD). В России ущерб был сравнительно невелик - около 1000 компьютеров.

Троянская программа маскируется под полезную или интересную программу, выполняя во время своего функционирования еще и разрушительную работу (например, стирает FAT-таблицу) или собирает на

компьютере информацию, не подлежащую разглашению. В отличие от вирусов троянские программы не обладают свойством самовоспроизводства.

Троянская программа маскируется, как правило, под коммерческий продукт. Ее другое название “троянский конь”.

Программа *монолитного* вируса представляет собой единый блок, который можно обнаружить после инфицирования.

Программа *распределенного* вируса разделена на части. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать вирус. Таким образом, вирус почти все время находится в распределенном состоянии, и лишь на короткое время собирается в единое целое.

Для борьбы с вирусами разрабатываются антивирусные программы. Говоря медицинским языком, эти программы могут выявлять (диагностировать), лечить (уничтожать) вирусы и делать прививку «здоровым» программам.

Различают следующие виды антивирусных программ:

- Программы – детекторы (сканеры);
- Программы – доктора (или фаги, дезинфекторы);
- Программы – ревизоры;
- Программы – фильтры (сторожа, мониторы);
- Программы – иммунизаторы.

Программы–*детекторы* рассчитаны на обнаружение конкретных вирусов и основаны на сравнении характерной (спецификой) последовательности байтов (сигнатур или масок вирусов), содержащихся в теле вируса, с байтами проверяемых программ. Программы – детекторы нужно регулярно обновлять, так как они быстро устаревают и не могут выявлять новые виды вирусов.

Следует подчеркнуть, что программы – детекторы могут обнаружить только те вирусы, которые ей «известны», то есть, сигнатуры этих вирусов заранее помещены в библиотеку антивирусных программ.

Таким образом, если проверяемая программа не опознается детектором как зараженная, то еще не следует считать, что она «здорова». Она может быть инфицирована новым вирусом, который не занесен в базу данных детектора.

Для устранения этого недостатка программы – детекторы стали снабжаться блоками эвристического анализа программ. В этом режиме делается попытка обнаружить новые или неизвестные вирусы по характерным для всех вирусов кодовым последовательностям. Наиболее развитые эвристические механизмы позволяют с вероятностью около 80% обнаружить новый вирус.

Программы – *доктора* не только находят файлы, зараженные вирусами, но и лечат их, удаляя из файла тело программы – вируса. Программы – доктора, которые позволяет лечить большое число вирусов, называют полифагами.

В России получили широкое распространение программы – детекторы, одновременно выполняющие и функции программ – докторов. Наиболее известные представители этого класса – AVP (Antiviral Toolkit Pro, автор – Е. Касперский), Aidstest (автор – Д. Лозинский) и Doctor Web (авторы – И. Данилов, В. Лутовин, Д. Белоусов).

Ревизоры – это программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние BOOT – сектора, FAT – таблицы, а также длина файлов, их время создания, атрибуты, контрольные суммы.

Контрольная сумма является интегральной оценкой всего файла (его слепком). Получается контрольная сумма путем суммирования по модулю

для всех байтов файла. Практически всякое изменение кода программы приводит к изменению контрольной суммы файла.

Антивирусы – фильтры – это резидентные программы (сторожа), которые оповещают пользователя обо всех попытках какой – либо программы выполнить подозрительные действия. Фильтры контролируют следующие операции:

- обновление программных файлов и системной области диска;
- форматирование диска;
- резидентное размещение программ в ОЗУ.

Обнаружив попытку выполнения таких действий, сторож (монитор) сообщает об этом пользователю, который окончательное решение по выполнению данной операции. Заметим, что она не способна обезвредить даже известные вирусы. Для “лечения” обнаруженных фильтром вирусов нужно использовать программы – доктора.

К последней группе относятся наименее эффективные *антивирусы – вакцинаторы* (иммунизаторы). Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной, и поэтому не производит повторное инфицирование. Этот вид антивирусных программ морально устарел.

После подробного описания вирусов и антивирусных программ переходим к работе с антивирусом, установленным на школьном компьютере. В нашем случае – это антивирус Касперского. Поговорим о функциях и содержимом данной программы. Покажем на примере быструю проверку.

4. Актуализация знаний.

5. Практическая работа «Защита от вирусов: обнаружение и лечение» - с помощью антивирусной программы проверить и вылечить флешку и диск с от вирусов

Домашнее задание: дома проверить свой компьютер с помощью различных антивирусных программ.

Самоанализ урока

Данный урок проводился в 8 «А» классе Красногорской СОШ в период педагогической практики под руководством учителя информатики Поликарпова Виталия Владимировича. Большой объем информации на уроке детьми воспринимался легко, так как тема была для всех очень интересна. Дети внимательно слушали и задавали вопросы. В конце урока с легкостью выполнили практическую часть заданий. Учитель информатики также одобрил мое изложение материала. Содержание моего конспекта соответствует учебнику Н.Д.Угриновича.

2.1.2. План-конспект занятия «Www.путешествие по всемирной паутине»

Цели урока:

- понимать основные принципы организации поиска информации в Интернете.
- развивать алгоритмическое мышление, умение выделять главное, расширить кругозор учащихся путем введения новых терминов;
- формирование навыков поиска информации в сети Интернет;
- воспитывать культуру общения: ученик-ученик, учитель-ученик

Тип урока: изучение нового материала.

Задачи урока:

- знакомство с понятием WWW
- Web- страница, Web-сайт
- адресация страниц в Интернет
- знакомство с возможностями поисковых систем, поисковыми запросами

- использовать поиск и отбор информации в практической деятельности и повседневной жизни.

Оборудование и программные средства: интерактивная доска, проектор, презентация к уроку, карточки - задания, комплект оценок.

Ход урока

I. Организационный момент.

II. Актуализация знаний. Изложение нового материала.

Здравствуйте, ребята. Сегодня мы совершим с Вами путешествие.

Внимательно посмотрите на слайд. Как вы думаете, куда мы с вами отправимся?

В путешествие по Интернету.

На экране представлено примерное графическое изображение связей между сетями Интернета. Изображены только связи между серверами.

На что похожа эта картинка? (На звездное небо, на паутину.).

*Тема урока***:** “WWW. Путешествие по Всемирной паутине”.

Но прежде чем отправится в круиз по просторам Сети, мы познакомится с понятием WWW, Web-страница, Web-сайт, браузер, поисковая система, а затем перейдем к практической части: будем работать с поисковыми системами, осуществлять запросы, находить необходимую информацию и применять её на практике.

Что же такое Интернет? Интернет всемирная система объединённых компьютерных сетей для хранения и передачи информации. На основе Интернета работает Всемирная паутина

WWW – что означает эта аббревиатура? (World Wide Web, WWW)

World Wide Web (WWW, Web) – всемирная СЕТЬ (паутина)

WWW – всемирное хранилище информации, существующее на технической базе сети ИНТЕРНЕТ (ведь интернет – пользователей более 2-х млрд.)

WWW – объединение многочисленных ресурсов, распределённых по всему миру;

WWW – организация информационных ресурсов, снабжённых гиперссылками.

WWW – содержит информацию самого разного характера: новости, научную, техническую, образовательную информацию, рекламу товаров и услуг, ресурсы для досуга и развлечений, общение через социальные сети, порталы и форумы, и многое другое. Жизнь современного человека невозможно сейчас представить без Интернета.

Любой человек может размести в сети информацию, и к этой информации будет иметь доступ весь мир!

Информация в WWW организована в виде *Web-страниц*. Для примера откроем сайт нашей школы.

Web-сайт – это несколько Web-страниц, связанных между собой по содержанию. В текстах, размещенных на страницах сайтов, могут быть выделены ключевые слова – гиперссылки.

Гиперссылки – ключевые слова или изображения, от которых идут гиперсвязи. Они выделяются *цветом* или *подчёркиванием*.

Адрес любого файла во всемирном масштабе определяется унифицированным_указателем ресурса — URL. URL-адрес представляет собой стандартизованную строку символов, указывающую местонахождение ресурса, документа или его части в Интернете, и состоит из трех частей.

Структура адреса:

- имя протокола для доступа к службе Интернет;
- имя сервера, на котором хранится ресурс и работает сервер-программа службы Интернет. Вот здесь мы часто видим аббревиатуру www;
- полное имя файла, который хранится на сервере.

www.schuv1996.mskobr.ru.

1. *http:// протокол*
2. *schuv1996.mskobr.ru – сервер*
3. *novosti/ - страница файл*

Огромное число гипертекстовых электронных документов, хранящихся на серверах WWW, образует своеобразное гиперпространство документов, между которыми возможно перемещение.

А вот перемещаться пользователю по «паутине» помогают специальные программы. (Web-браузеры; browse просматривать, изучать)

Назовите известные вам браузеры?

А есть ли какая-нибудь система хранения информации в Интернет, можно ли “запутаться” в паутинной сети? Это хаос или есть какая-то система, логика?

Чтобы не запутаться, нужно знать, где и как извлечь нужную информацию, нужен опыт поисковой работы. Как можно искать информацию:

- путем указания адреса документа (wikipedia.org)
- путем перемещения по паутине гиперссылок
- путем использования поисковых систем. YANDEX, RAMBLER

ПОИСКОВЫЕ СИСТЕМЫ (технология поиска)

Все системы поиска информации во Всемирной паутине располагаются на специальных серверах. Ежеминутно они обслуживают огромное количество клиентов. Действие поисковых систем основано на постоянном, последовательном изучении всех страниц всех сайтов. Для каждого документа, станицы существует определенный набор ключевых слов, отражающих содержание страницы. При получении запроса поисковая система формирует список страниц, соответствующих критериям поиска. Найденные документы упорядочиваются в зависимости от местоположения ключевых слов, частоты их появления в тексте и др.

Открыв браузер, находим поисковую строку, просим учеников найти информацию, например о Тульском самоваре. Информации будет большой поток. А как же найти тот сайт, на котором будет только нужная информация?

1. Ненужная информация отсекается простым приемом. Хотите, чтобы поиск осуществлялся только по четко заданной фразе? Заключите ее в кавычки «»

2. Поиск фразы с неизвестной переменной. Заключите запрос в кавычки, а вместо неизвестного слова вставьте знак *

3. Поиск одного из нескольких синонимов или просто одного из нескольких слов. Перечислите все возможные слова, разделив их знаком |, а если они входят в определенную фразу, то заключите их в скобки:

4. Как правильно искать в Яндексе слова в пределах одного предложения? Для этого используется знак &

5. Поиск по фразам, которые должны обязательно содержать определенное слово. Если вы хотите, чтобы какое-то слово обязательно входило в поисковую фразу, то перед ним нужно поставить знак +

6. Как правильно искать в Яндексе фразы, в которые НЕ входят определенные слова. «Ненужное» слово можно исключить из поиска, если написать его со знаком «минус»

7. Поиск фразы на определенном сайте. К поисковой фразе нужно всего лишь добавить вот такой оператор: «site:http://www.адрес сайта»

8. Поиск любых документов. Нужно только указать тип документа, который вы ищете, при помощи команды «mime:формат»

9. Поиск сайтов на определенных языках. Если вы хотите найти сайты на определенном языке, то просто напишите в конце фразы команду lang:язык (ru, uk, be, en, fr и т. д.)

Теперь Вы знаете основные правила поиска нужной информации.

*Домашняя работа***.**

Подготовить доклад на тему: «Какие вы знаете поисковые системы?» Рассказать их общие черты и отличия. Какой системой пользуетесь Вы и почему?

Самоанализ урока

Данный урок проводился в 8 «А» классе Красногорской СОШ в период педагогической практики под руководством учителя информатики Поликарпова Виталия Владимировича. В ходе изложения материала старалась вести диалог с ребятами, задавая наводящие вопросы. Это позволило активизировать их деятельность и оживило урок. Подобный прием дает возможность задействовать каждого ученика. В начале урока были такие ребята, которые не проявляли себя, но в процессе диалога удалось увлечь каждого. В итоге все отвечали на вопросы.

2.2. Проведение внеклассного мероприятия по теме «Формирование навыков школьников в области информационной безопасности и здоровьесбережения при самостоятельном поиске в сети интернет»

Понятие внеклассной работы широко и неоднозначно. Оно включает в себя различные по содержанию, назначению, методике проведения, формам и способам руководства занятия. Например, заседание предметного кружка, внеклассное чтение, проведение школьных праздников и вечеров относятся к внеклассной работе. Но в одних случаях (кружок, внеклассное чтение) ею руководит учитель, в других (организация досуга и развлечений) она приобретает характер деятельности учащихся на основе самоуправления.

В связи с этим возникает необходимость в дифференциации понятия «внеклассная работа», для чего в педагогической литературе и практике используются термины «внеучебная работа» и «внеурочная работа».

В своем исследовании мы придерживаемся определения Малеева В.В., так как считаем его более точным: «Внеклассная работа – это организация педагогом различных видов деятельности школьников во внеучебное время, обеспечивающих необходимые условия для социализации личности ребенка» [23.с 27].

Определяющая роль в планировании и организации внеклассой работы принадлежит педагогу. Примером тому может служить работа, которую ведут учителя–предметники как по расширению и углублению знаний программного материала со способными учащимися, так и в целях коррекции знаний слабоуспевающих. Важно отметить, что внеклассная работа по информатике может иметь межпредметный характер в силу разнообразия возможностей и средств, предоставляемых компьютером и информационными технологиями. Компьютерные методы могут с успехом применяться во внеклассной работе по информатике, физике, иностранным языкам, изобразительному искусству, географии и т.д.

Формы внеклассной работы по информатике:

Первая группа - фронтальные формы. Деятельность учащихся организована по принципу "рядом": они не взаимодействуют друг с другом, каждый осуществляет одинаковую деятельность самостоятельно. Педагог воздействует на каждого ребенка одновременно. Обратная связь осуществляется с ограниченным количеством учащихся.

Вторая группа форм организации внеклассной деятельности характеризуется принципом "вместе". Для достижения общей цели каждый участник выполняет свою роль и делает свой вклад в общий результат. От действий каждого зависит общий успех. Педагог влияет не на каждого в отдельности, а на их взаимосвязь, что способствует лучшей обратной связи между ним и учащимися [37.с 106].

Первая группа отличается простотой организации для педагога, но мало формирует навыки коллективного взаимодействия. Вторая группа незаменима для развития умений сотрудничать, оказывать помощь друг другу, брать на себя ответственность.

Формы массовой внеклассной работы позволяют педагогу косвенно воздействовать на каждого учащегося через коллектив. Они способствуют

развитию умений понимать другого, взаимодействовать в коллективе, сотрудничать со сверстниками и взрослыми.

Во внеклассной деятельности следует широко использовать такие формы массовой работы, как соревнование, конкурсы, олимпиады, смотры. Они стимулируют активность, развивают инициативу, укрепляют коллектив. Массовая работа содержит в себе большие возможности активизации учащихся, хотя степень ее может быть различной [47.с 73].

Мероприятие

Перед мероприятием, за несколько дней, ученикам даются темы «Здоровье», «Здоровый образ жизни», «Питание», «Сон» для самостоятельной подготовки. Предлагаются адреса ссылок на сайты (http://dzdorov.ru/, http://www.7ya.ru), чтобы ребята знали, где искать нужную информацию. На предложенных сайтах можно найти информацию о процентном соотношении здоровых детей и детей, уже имеющих хронические заболевания, а также найти ответы на вопросы о правильном питании, о том, как правильно заниматься физической культурой и не навредить себе и многое другое.

У ребят, скорее всего, возникнет вопрос «Почему на информатике мы будем говорить о здоровье?» Но в этом-то и вся суть мероприятия! На уроке биологии или ОБЖ, скорее всего, нет времени сидеть за компьютером и искать информацию о здоровье. Важно знать, как заниматься своим здоровьем и при этом не навредить себе, как обеспечить информационную безопасность от негативного воздействия внешней среды.

После нескольких дней подготовки, учитель назначает дату мероприятия. Учитель предлагает ученикам разделиться на несколько команд (зависит от числа учеников), выбирают жюри (возможно, что жюри – это дети из другого класса), выбирают капитанов.

1. Первое задание заключается в том, чтобы придумать девиз своей команды.

2. Второе задание состоит из нескольких вопросов. Ответы на вопросы ученики могут искать в интернете, но тот, кто первый ответит, получает 1 балл.

- Витамин, который содержится только в растительных продуктах *(Витамин* С).
- Как влияет реклама на стройность нашего тела? *(Телевизор и глянцевые журналы навязывают образ худого тела. Девочки с нормальным весом начинают худеть, подгоняя себя под этот образ).*
- Считают, что пред приемом пищи полезно выпить полстакана воды. Почему? *(Вода раздражает желудочные железы, повышает аппетит и улучшает переваривание пищи).*
- Сколько раз в день необходимо принимать пищу и в какое время? *(Не менее 4 – 5раз в день и в одно и то же время).*
- К какому времени полезнее отнести последний прием пищи перед сном? *(Позже 7 часов вечера есть не рекомендуется).*
- К дефициту какого микроэлемента в организме приводит чрезмерное употребление газированных вод в детстве, в результате возрастает опасность переломов костей *(Кальция).*
- Почему мы едим, когда не голодны? *(Так поступает человек, который находится в состоянии стресса).*
- Сколько времени длиться здоровый ночной сон для детей 12-14 лет? *(9-9,5 часов).*
- Правда ли, что белый шоколад полезнее черного и молочного? *(Нет).*
- Какой прием пищи является основным? *(Обед).*

3. Третье задание - кто больше найдет пословиц и поговорок на тему здоровье. Сложность заключается в том, что времени всего 3 минуты.

Победители получают 3 балла.

4. Четвертое задание заключается в том, чтобы при помощи компьютера создать небольшую презентацию, в которой будет описан один из видов закаливания (его принципы, правила и польза). Можно выбрать такую тему для презентации как: « Правильный режим труда и отдыха», «Компьютер – польза или вред», «Для чего нужен спорт».

Количество баллов максимально «5» – это за лучшую презентацию, в которой четко будут соблюдены заданные цели.

После проведения всех конкурсов, жюри подводит итоги и объявляет результат. Победителем становится тот, у кого наибольшее количество баллов.

Считаем, что здоровье подрастающего поколения является самой актуальной темой для обсуждения. Поэтому необходимо постараться, даже при изучении информатики и ИКТ, затронуть эту важную тему, еще раз поговорить с ребятами о необходимости заботиться о своем здоровье и научить соблюдать правила информационной безопасности при работе в сети интернет.

2.3 Состав рекомендаций для учителей для обеспечения мер по безопасной работе школьников в сети интернет

Нами были разработаны рекомендации по защите информации для учителей разного профиля работы. Так как все педагоги работают с информацией в сети Интернет, необходимо их научить правильно обращаться и защищать информацию от

Мы разработали рекомендации для учителей по фильтрации веб-контента.

1. Обзор систем, обеспечивающих контроль над содержанием потоков информации, передаваемых из учреждения образования в Интернет и получаемых из Интернета на компьютер (в локальную сеть) учреждения образования.

2. Рекомендации по защите школьников от просмотра и скачивания информации с веб-сайтов, не совместимых с задачами работы образовательного учреждения (порносайты, сайты антисоциальной направленности и т.п.).

3. Рекомендации по предотвращению неконтролируемого доступа и скачиванию из Интернета информации большого объема для внеучебных целей (видеофильмы, музыка, файловые архивы программного обеспечения и т.п.).

Система безопасного управления контентом, или, Secure Content Management (SCM) - это система, которая должна обеспечивать контроль над содержанием потоков информации, передаваемых и получаемых организацией из Сети. SCM-система должна обеспечивать управление контентом на базе определенных политик, проводимых организацией, и обычно включает управление Web-контентом, контроль над обменом сообщениями, защиту от вирусов и нежелательных, скачиваемых из Сети приложений [5, с. 27].

Обычно выделяются следующие SCM-подсистемы:

- Employee Internet Management (EIM) — контроль доступа сотрудников (учащихся) в Интернет;
- Internet Application Security (IAS) — контроль проникновения нелегального контента в сеть организации;
- E-mail scan (ES) — контроль утечки приватной информации из сети организации и фильтрация спама;
- Virus scan (VS) — контроль проникновения вирусов.

Для ограничения нецелевого использования Интернета на рабочих местах существует целый ряд технических решений как отечественного, так и западного производства:

- Proventia Web Filter (Технология, положенная в основу данного продукта, была приобретена у компании Cobion) — это блокиратор нежелательного

Web-содержимого, который ежемесячно анализирует 120 млн. Web-страниц и ежедневно добавляет в базу 100 тыс. новых и обновленных Web-страниц.

– CS MIMEsweeper for Web — средство контроля и разграничения доступа к Web, обеспечивающее, в том числе защиту от утечки конфиденциальных материалов через бесплатные Интернет-сервисы — Web-почту, чаты и доски объявлений. Эта программа защищает от распространения вирусов через Web, от потери конфиденциальной информации, от запрещенного серфинга, от нецелевых скачиваний и помещения нелегальной информации на внешние Web-ресурсы.

– SurfControl Web Filter — средство управления доступом в Интернет в корпоративных сетях. Программа предоставляет сотрудникам компаний доступ к полезной информации в Интернете, одновременно преграждая им доступ к Web-сайтам, не относящимся к их трудовой деятельности. Кроме того, вероятность потери важных данных или выхода из строя всей сети может быть снижена за счет запрещения загрузки потенциально опасных файлов, которые могут содержать вирусы либо другой разрушительный или опасный программный код (файлы *.doc, *.vbs, *.elm, *.exe и *.zip).

Webwasher URL Filter резко сокращает нецелевое использование Web-ресурсов за счет блокировки определенных категорий сайтов, например из разделов Shopping и Entertainment. Система также предотвращает возможность скачивания файлов определенных расширений, в частности MP3 [5, с. 79].

Системы контроля безопасности контента в первую очередь призваны осуществлять контроль над содержанием потоков информации, передаваемых из компании в Интернет и получаемых из Сети в локальную сеть организации. К задачам систем контент-секьюрити относятся также проверка информации, хранящейся в локальной сети предприятия, контроль над содержанием корпоративной электронной почты, а также контроль за

просматриваемой сотрудниками информацией с целью предотвращения использования Интернета в личных целях в рабочее время.

Необходимость систем контент-секьюрити диктуется тем, что Интернет — это источник информации, за который никто не несет ответственности, и вероятность получения из него недостоверной, оскорбительной, пиратской или запрещенной по другим причинам информации весьма велика.

Рекомендации по защите от доступа к информации, не совместимой с задачами образовательного учреждения

1. 0бзор систем, обеспечивающих контроль над содержанием потоков информации, передаваемых из учреждения образования в Интернет и получаемых из Интернета на компьютер (в локальную сеть) учреждения образования.

2. Рекомендации по защите школьников от просмотра и скачивания информации с веб-сайтов, не совместимых с задачами работы образовательного учреждения (порносайты, сайты антисоциальной направленности и т.п.).

3. Рекомендации по предотвращению неконтролируемого доступа и скачиванию из Интернета информации большого объема для внеучебных целей (видеофильмы, музыка, файловые архивы программного обеспечения и т.п.).

Проблема скачивания вредоносного контента

Интернет является мощным инструментом обучения. Однако помимо полезной информации в Интернете ученики могут встретиться с нежелательным контентом.

Отметим, что нежелательным контентом может являться тот, который отвлекает детей от учебного процесса. Дети могут вместо выполнения учебного задания в Сети, заниматься просмотром материалов разрешенного характера, но не имеющего ничего общего с учебным процессом.

Проблема утечки контента из учебного заведения

До сих пор мы говорили о том, что в учебном заведении есть проблема проникновения нежелательного контента внутрь учебной сети. Но существует также проблема утечки контента. В данном случае, во-первых, речь идет об утечке приватных персональных данных. В современном обществе существует проблема похищения детей, сексуальные домогательства и проч. Поэтому личная информация о ребенке (его фотография, расписание уроков, e-mail, телефон) не должны вывешиваться в Сети для свободного доступа [3, с. 74].

При размещении фотографий в Сети (например, на школьном Web-сайте) желательно размещать фотографии детей только с согласия родителей, и только групповые. Не стоит указывать имена детей и другую личную информацию.

Вторая проблема — это рассылка по почте или размещение на школьном (или другом) сайте запрещенного контента. Рассылка пиратского ПО, порнографии и т.п.

Трафикоемкие (объемные) процедуры доступа к информации

Трафикоемкие процедуры — скачивание видеофильмов, музыки, файловых архивов программного обеспечения ведут к резкому увеличению трафика, что может замедлять работу сети и увеличивать расходы на оплату трафика. Большинство программ, которые блокируют доступ у запрещенным Web-сайтам обеспечивают и контроль трафикоемких процедур.

Масштабы ущерба от вредоносного контента

Прежде всего, следует сказать, что проблема защиты от вредоносного контента далеко не только школьная проблема. Использование Интернета сотрудниками или учащимися, не связанное с учебной или служебной деятельностью, получило название «киберслэкинг» (от англ. cyberslacking — дословно «кибербездельничание»).

Учебные заведения отнюдь не первыми стали пытаться решить проблему фильтрации Интернета. Это, с одной стороны, говорит о том, что проблема глобальная и просто не решается, а с другой, что учебным заведениям в ряде случаев могут подойти решения, созданные для организаций широкого профиля.

Варианты проникновения/утечки контента

Нежелательный контент попадает в сеть учебного заведения преимущественно по двум каналам: через Web-трафик и через почтовый трафик. Проблема фильтрации почтового трафика широко известна как проблема спама. В качестве спама могут распространяться сообщения оскорбительного характера, призывы к насилию и т.п. Помимо всех вышеперечисленных проблем с наличием нежелательного контента в письмах спам генерирует лишний трафик, отвлекает пользователей.

Конечно, возможно попадание подобного контента также с flash-накопителей, CD, DVD дисков.

Борьба с нежелательным контентом

В борьбе можно выделить организационные меры (назначение ответственных лиц, режим доступа в компьютерный класс, доведение до сведения учащихся норм поведения в Сети, ответственности за противоправные действия и т.п.) и технические. К техническим мерам относится фильтрация трафика, и мониторинг действий учащихся [12, с. 364].

Наличие мониторинга (даже без фильтрации) уже может стать эффективной мерой.

Если ученик будет знать, что за его действиями (всеми посещениями ведется постоянный мониторинг и все его действия записываются в log-файлах с указанием того, кто, когда и что посещал) то это уже в существенной мере ограничит вероятность посещения нежелательных сайтов.

Варианты фильтрации контента

Контент может фильтроваться на уровне провайдера, на уровне шлюза в Интернет защищаемой сети и на уровне клиентской станции.

Фильтрация может быть построена на основе внешней обновляемой базы данных запрещенных ресурсов и может быть построена на основе локальной программы, которая действует по собственным принципам фильтрации («черные», «белые» списки, ключевые слова и т.п.).

Сложности фильтрации контента в школах

Каждый день в Интернете появляются тысячи новых сайтов, поэтому, даже используя обновления баз данных с нежелательными ресурсами, добиться 100%-ной фильтрации невозможно. Отдельная проблема это недостаточная фильтрация русскоязычного контента западными продуктами. Возможны ошибки, когда фильтр будет отсеивать сайты полезного содержания. В общем, чем более интеллектуален фильтр, и чем больше база, на которую он опирается, тем дороже решение и тем оно менее доступно для школ.

Часто в школах установлено различное компьютерное оборудование и необходимы продукты фильтрации контента (Web и e-mail), работающие на различных платформах.

Администраторы в школах имеют различный опыт работы с компьютерами, и даже непрофессионал должен иметь возможность создавать и поддерживать политику фильтрации. Образовательный процесс включает множество различных областей науки и фильтрация должна быть всеобъемлющей, настраиваемой, а также обеспечивать защиту от новейших угроз.

Мониторинг и протоколирование — это во многих случаях первый и важнейший шаг в контролировании интернет доступа. Данная функция наглядно показывает серфинг-профиль пользователя. Учитель может

проверить, где находился ученик, что просматривал, в какое время и как долго.

Мониторинг дает быструю и точную картину Web серфинга. Данные об интернет активности защищены криптографически и хранятся в недоступном для неавторизованного просмотра виде. Любой посещенный ресурс может быть просмотрен, и впоследствии добавлен в список разрешенных или запрещенных листов.

Отчеты мониторинга (Monitoring Reports) четко показывают, какие Web-страницы посещались, время визита, Web-адрес, и прочая информация.

Фильтрация сетевого контента - системы позволяющие ограничивать доступ к тем или иным сетевым сервисам или сайтам.

– Фильтры системы CyberPatrol позволяют учителям контролировать как, когда и кому интернет-доступ разрешен, (разрешен с ограничением (в виде фильтрации контента) или заблокирован в принципе).

– Фильтрация или блокирование web-сайтов, групп новостей и результатов, которые выдают поисковые машины, базируются на базе данных (категории CyberLIST), которая может донастраиваться путем добавления ваших собственных запрещенных или разрешенных сайтов или списков сайтов.

– Программа позволяет блокировать чаты и программы класса Instant Messaging

– Чат-сессии могут быть также подвергнуты фильтрации для предотвращения утечки важной информации, (имена, адреса телефоны и т.п.).

Программа поддерживает Лист разрешенных сайтов (YES List), который ограничивает пользователей серфингом только по заранее заданному разрешенному списку сайтов. Это хорошее решение для младших школьников.

– Программа предоставляет возможность выбирать заранее заданные настройки (Preset Filter Strengths). Имеются группы Ребенок (Child), Младшие тинэйджеры (Young Teen), Старшие тинэйджеры (Mature Teen) и т.п.

Возможен контроль за скачиванием программ из Сети, поскольку скачивание программ из Сети может быть небезопасным, нарушать политику школы в отношении пользования пиратским ПО. Вы можете заблокировать скачивание без разрешения игр, музыки, графических файлов, видео. Это в свою очередь снизит риск загрузки шпионского ПО вирусов, скачивание пиратской продукции.

Кроме того, вероятность потери важных данных или выхода из строя всей сети может быть снижена за счет запрещения загрузки потенциально опасных файлов, которые могут содержать вирусы либо другой разрушительный или опасный программный код (файлы *.doc, *.vbs, *.elm, *.exe и *.zip).

Фильтр пресекает действия, ведущие к увеличению трафика вследствие посещения развлекательных сетевых ресурсов, скачивания музыки или просмотра видеоклипов, и составляет подробный отчет об использовании Интернета.

Стандартные и настраиваемые отчеты позволяют определять эффективность применяемых правил использования Интернет. То есть, вы можете получать данные о посещенных сайтах, кем они были посещены, как часто, как долго и когда. Мониторы реального времени могут информировать администраторов, учителей и студентов о попытках нарушения политики. Вы также можете установить правила обращения с определенными типами e-mail-сообщений - удаление, изоляция, задержка, пересылка или доставка получателю [15, с. 75].

Разносторонняя база данных SurfControl обладает наиболее современной и комплексной базой данных контента, предлагая обширную

базу данных, классифицированную по категориям риска, как web, так и e-mail. Кроме того, продукт использует технологии искусственного интеллекта, динамически расширяющих определяемый контент, что помогает защитить пользователей от угроз прежде, чем они получили широкое распространение или были помещены в базу данных.

Вывод по второй главе

Мы подошли к выявленной проблеме комплексно: нами были разработаны конспекты уроков и внеклассное мероприятие, а также рекомендации для педагогов. Конспекты уроков – это часть образовательной деятельности, внеклассное мероприятие – воспитательный аспект, а рекомендации являются организационным моментом.

Заключение

Целью нашей работы являлась разработка учебно-методических материалов по обучению школьников поиску информации в сети интернет.

Решая первую задачу, мы проанализировали учебную литературу и научные статьи, выделили и описали основные понятия, рассмотрели методы и средства для безопасной работы в сети интернет. В ходе исследования мы убедились, что умение защитить себя и свой компьютер от вредоносных программ дело очень важное и серьезное. Доказали, что использование только антивирусов, не дает надежной защиты, необходим комплексный подход к обеспечению безопасности компьютера.

Решая вторую задачу, мы дали понятие определению самостоятельная работа, выделили общие педагогические принципы самостоятельной работы, определили важность и необходимость умения самостоятельно работать с информацией. Мы доказали, что первая задача учителя заключается в том, чтобы развить у учащихся самостоятельность в познавательной деятельности, научить их самостоятельно овладевать знаниями, формировать свое мировоззрение, а вторая — в том, чтобы научить их самостоятельно применять имеющиеся знания в учении и практической деятельности.

Решая следующую задачу, мы подобрали и проработали специальную литературу, выстроили структуру урока. После этого, уроки и внеклассное мероприятие были проведены на практике, сделан самоанализ. Мы увидели, что после проведенных мероприятий, школьники стали пользоваться правильными принципами поиска информации в сети. В ходе исследований мы показали, что у учеников повысился интерес к предмету, появилось желание работать и получать хорошие отметки.

Решая последнюю задачу, мы доказали, что безопасность детей, работающих с информацией в глобальных сетях, очень важна, и педагог обязан научить школьников, как правильно обращаться с Интернет-ресурсами. Актуальность этого подтверждается тем, что сейчас очень много

детей попадают в интернет-ловушки. Педагоги, как никто другой, должны рассказать ученикам обо всех возможных уловках и научить их обходить стороной подобные сайты.

Полученный опыт и отдельные положения дипломной работы были использованы при написании статьи: «Формирование навыков школьников в области информационной безопасности и здоровьесбережения при самостоятельном поиске в сети интернет», представленной на III Всероссийской научно-практической конференции «Методика преподавания математических и естественнонаучных дисциплин: современные проблемы и тенденции развития».

Библиографический список

1. Андреев, В.И. Педагогика творческого саморазвития. Инновационный курс. [Текст] /В.И. Андреев – Казань, 1996. – 160 с.

2. Бабанский, Ю.К. Педагогика [Текст] / Бабанский, Ю.К. – М.: Педагогика, 1988. − 156 с.

3. Богатырева, Ю. И. Педагогическая деятельность и обеспечение информационной безопасности личности [Текст] Ю.И. Богатырева / Информатика и образование 2013 – С. 88.

4. Веткин, Л. Г. Самостоятельная работа учащихся на уроке [Текст] /Л.Г. Веткин - Изд-во Саратовского университета, 1978. – 24 с.

5. Внедрение ИКТ в учебный процесс [Электронный ресурс]. – Режим доступа http: // www.uchportal.ru (дата обращения 28.09.2015).

6. Дворецкая, А.В. Основные типы компьютерных технологий [Текст] / А.В. Дворецкая / Школьные технологии. – 2004. –№ 3. – 201 с.

7. Есипов, Б. П. Самостоятельная работа учащихся на уроках [Текст] / Б.П. Есипов: М.: Гос. учебно-педагогическое издание министерства просвещения РСФСР. 1961. – 239 с.

8. Есипова, Н. Д. Дифференцированный подход в обучении информатике. Информатика и образование [Текст] / Н.Д. Есипова — М.: издание №6, 1996. –23 с.

9. Жарова, Л.В. Управление самостоятельной деятельностью учащихся [Текст] / Л.В. Жарова – СПб., 2002. − 18 с.

10. Замогильнова, Л.В. Дифференциация обучения на уроках информатики [Текст] / Л.В. Замогильнова – М.: издание № 1, 1999. – 36 с.

11. Захаров, В.А. Информационное общество [Текст] / В.А. Захаров, М.Б. Игнатьев, Ю.Ф. Шейнин // Системы и средства информатики – М.,1999. — 97с.

12. Захарова, И.Г. Информационные технологии в образовании [Текст] / учебное пособие для студ.выс.пед.учеб.заведений / И.Г. Захарова. – М.: Академия, 2003. – 192 с.

13. Зимняя, И. А. Педагогическая психология. Учебник для вузов. [Текст] /И.А. Зимняя: Изд. второе, доп., испр. и перераб. – М.: Издательская корпорация «Логос», 2000. — 384 с.

14. Златопольский Д.М. Сборник заданий для внеклассной работы по информатике / Д.М. Златопольский. – М.: Чистые пруды, 2006. – 32 с. –

15. Идрисова А. А. Информационная безопасность школьников в сети интернет: проблемы и пути решения // Современные инновации./ [Текст] /А.А. Идрисова – 2015. –. 118 с.

16. Ильин, Т.А. Педагогика [Текст] / Ильин, Т.А. – М.: Просвещение, 2014. – 256 с.

17. Ильина, Т.А. Курс лекций: учебное пособие для студентов педагогических институтов [Текст] / Т.А. Ильина – М.: Просвещение, 1984. – 494 с.

18. Информатика и ИКТ. Учебник для 8-9 классов под ред. Макаровой Н.В. СПб.: 2010. — 416 с.

19. Кларин, В.М. Педагогические технологии в учебном процессе [Текст] / В.М. Кларин – М.,1989. – 114 с.

20. Крысько, В.Г. Психология и педагогика: Схемы и комментарии [Текст] / Крысько, В.Г. – М. : Владос, 2007. – 36 с.

21. Ксензова, Г.Ю. Перспективные школьные технологии. [Текст] / Г.Ю. Ксензова: учеб. пособие – М.: Пед. общество России, 2000. – 215 с.

22. Лочина, Г.М. Применение информационно - коммуникативных технологий для оптимизации образовательного процесса [Текст] / Г.М. Лочина, С.Ю Крупнова, Е.Е. Курносова //.Материалы научно-практической конференции – Саранск: МРИО, 2007 г. – 379 с.

23. Малеев, В. В. Общая методика преподавания информатики: учебное пособие [Текст] / В.В. Малеев – Воронеж, 2005. – 271 с.

24. Малкин, И. И. Рационально организовать самостоятельную работу учащихся. Приложение к журналу «Народное образование» [Текст] / И.И. Малкин, – М. № 10, 2006. – 23 с..

25. Мардахаев, Л. В. Основы социально-педагогической технологии: Учебное пособие [Текст] / Л.В. Мардахаев – Рязань, 2008. – 92 с.

26. Мезенцев, К.Н.: Автоматизированные информационные системы [Текст] / К.Н. Мезенцев – М.: Академия, 2011. – 112 с.

27. Мельников, Ю. Н. Обеспечение целостности информации в вычислительных системах. Техническая кибернетика [Текст] / Ю.П. Лутковский, Ю.Н. Мельников, В.А. Мясников – М. 1985г – 79 с.

28. Мельников, Ю.Н. Многоуровневая безопасность в корпоративных сетях. Международный форум информатизации [Текст] / Д.Ю. Иванов, Ю.Н. Мельников – М.: Издательство "Станкин", 2000. – 245 с.

29. Михеева, Е.В.: Информационные технологии в профессиональной деятельности [Текст] / Е.В. Михеева – М.: Академия, 2011. 138 с.

30. Новые педагогические технологии в системе образования [Текст]/ Под ред. Е.С. Полат. – М.: Академия, 1999. – 224 с.

31. Орлов, В.Н. Активность и самостоятельность учащихся [Текст] / В.Н. Орлов – М., 2001. – 33 с.

32. Панюкова, С.В. Информационные и коммуникационные технологии в личностно ориентированном обучении [Текст] / С.В. Панюкова. – М.: ИОСО РАО – 2008. – 225 с.

33. Пидкасистый, П. И. Самостоятельная деятельность учащихся [Текст] М.: «Педагогика», 1972. – 184 с.

34. Пидкасистый, П.И. Самостоятельная познавательная деятельность школьников в обучении [Текст] / Пидкасистый, П.И. – М. : Педагогика, 1980г. – 240 с.

35. Подласый, И. П. Педагогика: Новый курс: Учебник для студентов высших учебных заведений [Текст] / Подласый, И. П. – М. : Владос, 1999. – 256 с.

36. Ратинер, Т. Г. Информационно-психологическая безопасность школьников при работе в интернете. Современное образование [Текст] / Т.Г. Ратинер – М. 2014. – 96 с.

37. Рубин, А.А. Внеурочная работа по общественным предметам [Текст] / А.А. Рубин, З.В. Юрченко, – М.2011 – 113 с.

38. Селевко, Г.К. Дифференциация учебного процесса на основе интересов детей [Текст] / Г.К. Селевко – М., 1996. – 87 с.

39. Селевко, Г.К. Современные образовательные технологии [Текст] / Г.К. Селевко – М.: Народное образование, 1998. – 144 с.

40. Семакин И.Г. Информатика и ИКТ. Базовый курс. Учебник для 8 класса [Текст] / Л.А Залогова, С.В Русакова, И.Г. Семакин, Л.В. Шестакова – М.: Бином, 2005. –168 с.

41. Социальные характеристики молодёжи Ряз. обл. Анализ результатов социалогического исследования. Молодёжь 97 [Текст] / Г. В. Гаврилова, В. А. Горнов, Н. А. Степанов – Рязань, 2012. – 121 с.

42. Ташков П.А.: Защита компьютера на 100% [Текст] / П.А. Ташков – СПб.: Питер, 2011. – 199 с.

43. Тихонова, В. И. Самостоятельна работа студентов как проблема высшей профессиональной школы [Текст] / А. В. Арапов, Т. В. Стародубцева, В. И. Тихонова – М., 2011. – 50 с.

44. Угринович Н.Д. Учебник по информатике за 8 класс. Издание: 4-е изд. — М.: Бином, 2011. – 178 с.

45. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

46. Федотов,Н.Н. Защита информации Учебный курс HTML-версия [Текст] / Н.Н. Федотов (http://www.college.ru/UDP/texts)

47. Щуркова Н.В. Новые формы воспитательной работы [Текст] / Н.В. Щуркова – .М.,№ 4,5,6 2014г. – 55 с.

48. Электронные образовательные ресурсы. Точка доступа http://collegy.ucoz.ru/load/9-1-0-143 (Дата обращения 15.04.2016).

49. Электронные образовательные ресурсы. Точка доступа http://window.edu.ru/catalog/resources?p_str=задания+на+поиск+использование+информации+в+глобальной+сети (Дата обращения 18.04.2016).

50. Электронные образовательные ресурсы. Точка доступа http://xreferat.com/71/5569-3-vneklassnaya-rabota-i-stepen-ee-vliyaniya-na-razvitie-social-nyh-kachestv-lichnosti.html (Дата обращения 22.03.2016).

51. Электронные образовательные ресурсы. Точка доступа Каймин В.А.: Информатика. — М.: ИНФРА-М, 2012 (Дата обращения 29.04.2016)

52. Электронные образовательные ресурсы. Точка доступа Каймин В.А.: Информатика. – М.: ИНФРА–М, 2012 (Дата обращения 13.04.2016)