Автономная некоммерческая организация высшего образования «Поволжский православный институт имени Святителя Алексия, митрополита Московского»

Кафедра педагогики и психологии

Направление подготовки 44.03.01 Педагогическое образование
Направленность (профиль) «Информатика и информационные технологии»

БАКАЛАВРСКАЯ РАБОТА

на тему:

«Методическое обеспечение занятий по региональной программе дополнительного образования «Безопасность работы в Интернет детей и подростков»»

Выполнила студентка
4 курса группы ИТ-401
очной формы обучения
Молодец Анастасия Петровна

_____
(подпись)

Научный руководитель
старший преподаватель
Зоркин В.А.

_____
(подпись)

Научный руководитель
доцент, к. п. н.
Дудина И.П.

_____
(подпись)

Допустить к защите:
Заведующий кафедрой
педагогики и психологии _____ Е.А.Денисова
(подпись) *(И.О.Ф..)*

«___»_____20___г.

Тольятти
2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 5
Глава 1 Теоретические предпосылки разработки методики обучения по разделу «Безопасность в сети Интернет» в базовом курсе информатики 9
1.1 Научно-педагогические и методические основы реализации раздела «Безопасность в сети Интернет» в школьном курсе информатики 9
1.2 Методические особенности изучения раздела «Информационная безопасность в сети Интернет» в базовом курсе информатики средней школы 17
1.3 Электронный учебно-методический комплекс по разделу «Информационная безопасность в сети Интернет» как компонент дополнительного образования у детей и подростков 23
Выводы по главе 1 30
Глава 2 Проектирование и реализация ЭУМК по разделу «Безопасность в сети Интернет» 31
2.1 Дидактические, программно-технологические и технические характеристики ЭУМК 31
2.2 Педагогический и технологический сценарий ЭУМК 36
2.3 Проектирование и реализация теоретико-познавательного модуля ЭУМК 41
2.4 Проектирование и реализация контрольного модуля 46
Глава 3. Оценка эффективности разработанного ЭУМК 49
3.1 Общая характеристика исследования 49
3.2 Методика проведения и результаты педагогического эксперимента ... 51
ЗАКЛЮЧЕНИЕ 57
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 59
ПРИЛОЖЕНИЯ 69

ВВЕДЕНИЕ

Обучение информационной безопасности, как одно из важнейших направлений деятельности человека в информационной среде, рассматривается на сегодняшний день как важнейший компонент образования. В наши дни информационная безопасность востребована практически во всех сферах нашей жизни, таких как информатика, бизнес и экономика, физика. Довольно часто возникает вопрос кибербезопасности, так как кибератаки происходят ежесекундно. Для осознанного пользования интернет-ресурсами, получения пользы от нахождения в социальных сетях, избежания кибератак необходимо быть информационно грамотным, а этому способствует курс цифровой гигиены.

В 2019 году Министерством Образования и Науки Самарской области была разработана региональная программа «Цифровая гигиена». Данная программа рассчитана на учащихся 7-9 классов, а также на родителей обучающихся всех возрастов.

Основной целью изучения курса «Цифровая гигиена» является обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышение защищённости детей от информационных рисков и угроз.

Задачей курса является формирование общекультурных навыков работы с информацией, которые необходимы для различных форм коммуникаций.

Цифровая гигиена – это определённый свод правил, которым следуют люди для обеспечения себе информационной безопасности.

Информационная безопасность – это возможность предотвращения несанкционированного доступа, искажения, использования, изменения или уничтожения какой-либо информации.

Современные гаджеты формируют вокруг людей среду, которая оказывает влияние на поведение и восприятие окружающего мира. Часто из-за отсутствия информационной грамотности у человека образуется повышенная

уязвимость, так как Интернет и социальные сети стали местом для развития манипуляторов и мошенников.

Основная задача цифровой гигиены – помочь человеку, дать элементарные знания безопасной жизни в цифровом пространстве, уберечь от буллинга, несанкционированного доступа к различной информации и т.д.

Обучением информационной безопасности в сети Интернет в школьном курсе информатики занимались такие педагоги и ученые, как Е. К. Баранова [11], А.В.Бабаш [10], М. С. Цветкова[32], Е. В. Касперский[7] , А. Лукацкий[27], Саймон Сингх[43] и другие.

Комплексный анализ состояния методики обучения учащихся средних школ цифровой гигиене, а также современные исследования в указанной области позволили выделить противоречие между необходимостью создания учебных пособий и методических рекомендаций, позволяющих организовать процесс обучения информационной безопасности, и недостаточной разработанностью научно-практических рекомендаций в этой области.

На основе анализа актуальности и выявленных противоречий сформулирована проблема исследования, заключающаяся в обосновании методики обучения цифровой гигиене у учащихся 6-9 классов средних школ.

Теоретико-методологическую основу исследования составляют концепции в области педагогических и информационных технологий (Е. С. Полат [37], И. В. Роберт [40], Г. М. Киселев [20] и др.); теории и методики обучения информатике и информационной безопасности (Бабаш А. В.[10], Наместникова М. С.[32], Стрельцов А. А. [45] и др.); дидактические аспекты использования информационных технологий (Гафурова Н.В. [12] , Громов Ю. Ю. [14], Запечников С. В.[17] , Кузнецова А. В.[18] , Наместникова М. С. [32], Стрельцов А. А.[45] и др.).

Актуальность выявленной проблемы и ее недостаточная разработанность в частной дидактике определила выбор темы исследования.

Объект исследования – процесс обучения информационной безопасности в курсе информатики средней школы.

Предмет исследования – программно-методическое обеспечение по обучению информационной безопасности учащихся средней школы.

Цель исследования – разработка, обоснование структуры, содержания и методов реализации программно-методического обеспечения по обучению информационной безопасности учащихся.

Задачи исследования:

1. Провести анализ психолого-педагогической, научно-методической и учебной литературы, связанной с проблемой введения обучения на старшей ступени общего образования.
2. Выявить основные проблемы обучения разделу «Информационная безопасность в сети Интернет» учащихся средней школы.
3. Определить роль и место раздела «Информационная безопасность в сети Интернет» в базовом обучении информатике и ИКТ и сформулировать основные требования к его структуре, содержанию, методам, средствам и формам обучения.
4. Выделить и обосновать этапы разработки и использования программно-методического обеспечения обучения информационной безопасности учащихся средней школы.
5. Выполнить программную реализацию электронных образовательных ресурсов для обучения разделу «Цифровая гигиена. Информационная безопасность в сети Интернет»: разработать интерфейс пользователя; функционал компонентов на базе созданных сценариев и режимов использования.
6. Разработать методические рекомендации для учащихся и преподавателей.

Гипотеза исследования: использование предложенного программно-методического обеспечения обучения школьников информационной безопасности позволит обеспечить достижение предметных и личностных результатов обучения в соответствии с образовательным стандартом общего среднего образования.

Методы исследования:

1. Теоретические: системный анализ отечественной и зарубежной психолого-педагогической, научно-методической литературы по педагогике, психологии, информатике; изучение и анализ нормативных документов в сфере общего образования, критический анализ существующих подходов к обучению информационной безопасности в сети Интернет, а также использованию электронных ресурсов по рассматриваемой проблеме.

2. Эмпирические: обобщение опыта преподавания информатики; анализ содержания учебных программ, планов, пособий, материалов конференций по вопросам обучения информационной безопасности в сети Интернет в школе; наблюдение, беседа, анкетирование, тестирование учащихся с целью выяснения целесообразности использования предложенной методики и ее эффективности в области развития познавательного и творческого потенциала школьников.

Первая глава отражает теоретическое обоснование проводимого исследования, а именно научно-педагогические и методические основы реализации, особенности обучения цифровой гигиене, а также требования к электронному учебно-методическому комплексу по разделу «Информационная безопасность в сети Интернет».

Вторая глава представляет собой практическую проектную часть работы, результаты проектирования, поэтапной разработки и использования электронного учебно-методического комплекса по теме исследования.

В третьей главе представлены результаты обработки данных проведенного педагогического эксперимента, подтверждающие гипотезу об использовании предложенного программно-методического обеспечения для достижения предметных и метапредметных результатов обучения в соответствии с образовательным стандартом общего среднего образования.

В заключении подводятся итоги проделанной работы.

Библиографический список содержит перечень источников информации, использованных при выполнении бакалаврской работы.

Приложения включают разработанные практические задания и демонстрационные примеры их решения.

Глава 1 Теоретические предпосылки разработки методики обучения по разделу «Безопасность в сети Интернет» в базовом курсе информатики

1.1 Научно-педагогические и методические основы реализации раздела «Безопасность в сети Интернет» в школьном курсе информатики

Одной из главных задач образования является развитие и формирование инновационного мышления учащихся. Современный образовательный процесс стремительно меняется, для его построения должны учитываться новые требования к профессиональным компетенциям, которые связаны с формированием нового рынка труда.

Ученики проводят много времени в Интернете, в социальных сетях и различных приложениях. С каждым годом количество времени, которое проводят школьники в сети увеличивается, при этом польза от такого занятия есть не всегда. Также не все учащиеся умеют разумно и целесообразно относиться к информации в сети, это подвергает их опасности.

Информационная безопасность в сети Интернет – это один из ведущих разделов информатики и одно из важнейших направлений деятельности человека в современной информационной среде.

В настоящее время очень востребованы профессии связанные с безопасностью данных и безопасностью в сети Интернет.

Для того чтобы хорошо понимать что такое информационная безопасность необходимо дать основные определения понятиям и терминам.

В широком смысле информационная среда – это комплекс программного, технического и организационного обеспечения, который нужен для своевременного обеспечения пользователей той или иной системы, нужной информацией.

Информационная безопасность – ограничение несанкционированного доступа к информации.

Безопасность информации – это защищённость информации, которая хранится в определённом пользователем месте. Её целью является принятие

необходимых мер для предотвращения различных Интернет атак.

Изучение информационной безопасности в сети Интернет влияет на формирование научного мировоззрения будущего IT-специалиста.

Различают 4 уровня защиты информации:

1) предотвращение — доступ к информации и технологии только для персонала, который имеет допуск от собственника информации;
2) обнаружение — обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены;
3) ограничение — уменьшается размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению;
4) восстановление — обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

В 2019 году на региональном уровне разработан курс «Цифровая гигиена», который состоит из трёх модулей и направлен на учащихся 7-9 классов. Данная программа учитывает требования, которые выдвигает ФГОС.

Во многих школах города Тольятти с 2019 года уже реализуется данная программа. К примеру, в муниципальном бюджетном общеобразовательном учреждении городского округа Тольятти «Школа № 1 имени Виктора Носова», муниципальном бюджетном общеобразовательном учреждении городского округа Тольятти «Гимназия № 9», муниципальном бюджетном общеобразовательном учреждении городского округа Тольятти «Школа № 20», а также в муниципальном бюджетном общеобразовательном учреждении городского округа Тольятти «Классическая гимназия № 39», в которой проходил педагогический эксперимент. В дальнейшем планируется реализация данной программы во всех школах, не только городского округа Тольятти, но и области, а также и страны в целом.

Мы можем сделать вывод о том, что изучение информационной безопасности в школе – один из важнейших компонентов современного образования школьников. Данный раздел представлен в Федеральном

государственном образовательном стандарте среднего образования (ФГОС СОО) по предметной области «Информатика». Согласно ФГОС СОО[1] изучение рабочей программы «Цифровая гигиена» должен обеспечить условия для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз; формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Предметные результаты изучения курса «Цифровая гигиена» должны отражать владение приёмами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Предметные результаты изучения курса «Цифровая гигиена» должны включать требования к результатам освоения базового курса и дополнительно отражать овладение основами соблюдения норм информационной этики и права, основами самоконтроля, использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

Метапредметные результаты изучения курса «Цифровая гигиена» должны:

1) идентифицировать собственные проблемы и определять главную проблему;
2) выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
3) выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
4) составлять план решения проблемы (выполнения проекта, проведения исследования);
5) описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
6) оценивать свою деятельность, аргументируя причины достижения или

отсутствия планируемого результата;

7) работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
8) принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

1) выделять явление из общего ряда других явлений;
2) строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям
3) излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
4) самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
5) критически оценивать содержание и форму текста;
6) определять необходимые ключевые поисковые слова и запросы. Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

1) строить позитивные отношения в процессе учебной и познавательной деятельности;
2) критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
3) договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
4) делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его;
5) целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;

6) выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
7) использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
8) использовать информацию с учетом этических и правовых норм;
9) создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Личностные результаты:

1) осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
2) освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
3) освоение правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде;
4) сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Примерная основная образовательная программа среднего общего образования уточняет требования ФГОС СОО[8] к изучения информационной безопасности.

Согласно примерной образовательной программе среднего общего образования в результате изучения предмета «Информационная безопасность в сети Интернет» на уровне среднего общего образования выпускник должен

гарантированно получить следующие результаты:

1) анализировать доменные имена компьютеров и адреса документов в интернете;
2) безопасно использовать средства коммуникации;
3) безопасно вести и применять способы самозащиты при попытке мошенничества;
4) безопасно использовать ресурсы интернета.

Согласно федеральному базисному учебному плану и примерным учебным планам для образовательных учреждений Российской Федерации реализующих программы общего образования по информатике и ИКТ, программа рассчитана на один год. А именно на 32 учебных часа, из них 22 часа - учебных занятий, 9 часов - подготовка и защита учебных проектов, 3 часа - повторение, т.е. по 1 часу в неделю в 7,8 и 9 классах, в течении одного учебного года.

В различных авторских программах ведущих авторов школьных учебников по информатике на изучение раздела «Информационная безопасноть в сети Интернет» отводится от 18 до 32 часов.

В работе Н.М. Тимофеева «Цифровая грамотность как компонент жизненных навыков»[36] определено понятие «цифровой грамотности». Цифровая грамотность - это набор знаний и умений, которые нобходимы для безопасного и эффективного использования цифровых технологий и ресурсов интернета.

Включает в себя такие понятия, как цифровое потребление; цифровые компетенции; цифровую безопасность.

Цифровое потребление - это интернет услуги, которые используются для работы и жизни. Оно включает в себя: мобильный интернет,различные цифровые устройства, новости, социальные сети, всевозможные облачные технологии.

Цифровые компетенции - это навыки, которые помогают эффективно пользоваться технологиями. Они включают в себя использование цифровых

устройств, функционала социальных сетей, а также совершение финансовых операций, онлайн-покупки и поиск информации.

Цифровая безопасность - это основы безопасности в использовании Сети. Она включает в себя: защиту всех персональных данных, культуру поведения в Сети, хранение информации и т.д.

Само понятие «цифровая грамотность» стало подразумевать не только умение использовать компьютер и технические устройства, но и рассматриваться на ряду с понятиями, связанными с технологической грамотностью.

В работе А.В. Бабаш, Е. К. Баранова, Д. А. Ларин «История защиты информации»[10], созданном на основе исторических документов, разбираются вопросы становления криптоанализа в России, популяризация криптографического подхода к защите информации и различными предпосылками в данной сфере.

В работе М.С. Цветкова, Е.В. Якушина «Информационная безопасность 5-6 классы»[50], где теме правила для пользователей сети интернет и пространство Интернета на планете Земля отводится целых 2 параграфа, учебник «Информационная безопасность 7-9 классы» М.С. Цветкова, И.Ю. Хлобыстова, где теме «Киберугрозы» отводится целая глава, представлены тесты, авторская программа, методическое пособие и задания по данной теме.

Таким образом, можно сделать вывод, что раздел «Информационная безопасность в сети Интернет» широко представлен в школьных учебниках информатики.

Примерная основная образовательная программа среднего общего образования [4] уточняет требования ФГОС СОО к изучению информационной безопасности на базовом и углубленном уровне.

Согласно примерной основной образовательной программе среднего общего образования в результате изучения учебного предмета "Информатика" на уровне среднего общего образования выпускник на базовом уровне должен гарантированно научится:

1) выполнять пошагово (с использованием компьютера или вручную) несложные алгоритмы управления исполнителями и анализа числовых и текстовых данных;
2) использовать готовые прикладные компьютерные программы в соответствии с типом решаемых задач и по выбранной специализации;
3) понимать и использовать основные понятия, связанные со сложностью вычислений (время работы, размер используемой памяти);
4) использовать компьютерно-математические модели для анализа соответствующих объектов и процессов, в том числе оценивать числовые параметры моделируемых объектов и процессов, а также интерпретировать результаты, получаемые в ходе моделирования реальных процессов; представлять результаты математического моделирования в наглядном виде, готовить полученные данные для публикации;
5) аргументировать выбор программного обеспечения и технических средств ИКТ для решения профессиональных и учебных задач, используя знания о принципах построения персонального компьютера и классификации его программного обеспечения;
6) создавать структурированные текстовые документы и демонстрационные материалы с использованием возможностей современных программных средств;
7) применять антивирусные программы для обеспечения стабильной работы технических средств ИКТ;
8) соблюдать санитарно-гигиенические требования при работе за персональным компьютером в соответствии с нормами действующих СанПиН.

Согласно примерной основной образовательной программе среднего общего образования в результате изучения учебного предмета "Информатика" на уровне среднего общего образования выпускник на углубленном уровне должен гарантированно научится:

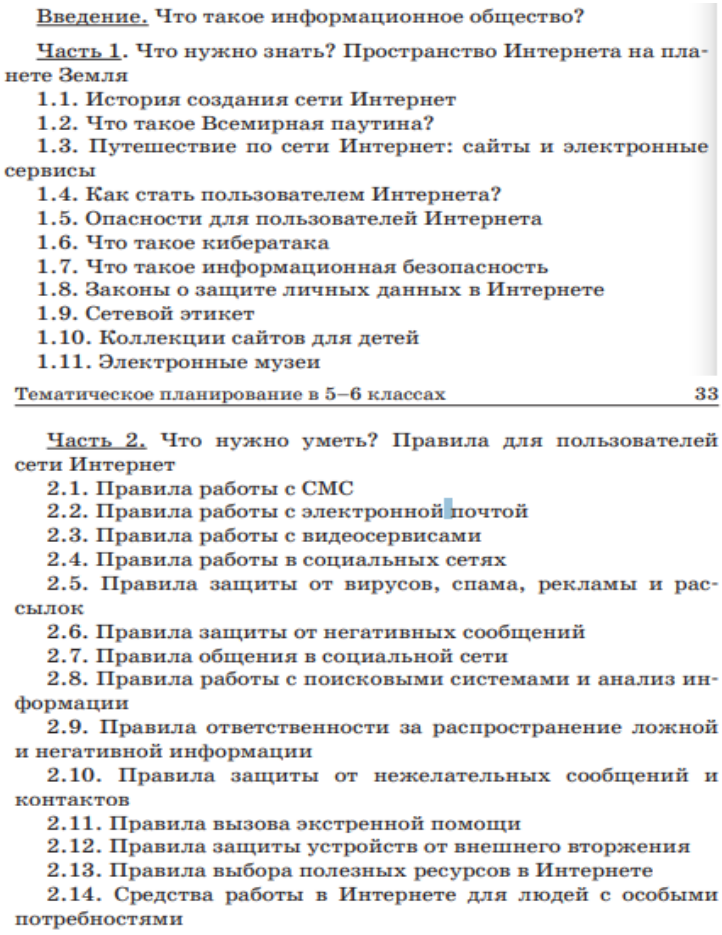
1) понимать структуру доменных имен; принципы IP-адресации узлов сети;

2) представлять общие принципы разработки и функционирования интернет-приложений (сайты, блоги и др.);
3) применять на практике принципы обеспечения информационной безопасности, способы и средства обеспечения надежного функционирования средств ИКТ; соблюдать при работе в сети нормы информационной этики и права (в том числе авторские права);
4) проектировать собственное автоматизированное место; следовать основам безопасной и экономичной работы с компьютерами и мобильными устройствами; соблюдать санитарно-гигиенические требования при работе за персональным компьютером в соответствии с нормами действующих СанПиН.

1.2 Методические особенности изучения раздела «Информационная безопасность в сети Интернет» в базовом курсе информатики средней школы

В курсе информатики 6-9 классов раздел «Информационная безопасность» подразумевает изучение информационных процессов и их роли в современном мире, изучение компьютерных сетей распространения и обмена информацией, использование информационных ресурсов общества с соблюдением правовых и этических норм, а также о правилах организации индивидуального информационного пространства.

В учебном пособии М.С. Цветкова, Е.В. Якушина «Информационная безопасность. Безопасное поведение в сети Интернет. 5-6 классы»[32,50] курс рассчитан на 30 уроков, которые можно реализовывать на уроках информатики по 1 уроку в неделю, а также на внеурочных занятиях. На них также отводится 1 час в неделю. Курс проводится по полугодиям в 5 и 6 классах, по 15 уроков в каждом.



Введение. Что такое информационное общество?

Часть 1. Что нужно знать? Пространство Интернета на планете Земля
1.1. История создания сети Интернет
1.2. Что такое Всемирная паутина?
1.3. Путешествие по сети Интернет: сайты и электронные сервисы
1.4. Как стать пользователем Интернета?
1.5. Опасности для пользователей Интернета
1.6. Что такое кибератака
1.7. Что такое информационная безопасность
1.8. Законы о защите личных данных в Интернете
1.9. Сетевой этикет
1.10. Коллекции сайтов для детей
1.11. Электронные музеи

Тематическое планирование в 5–6 классах 33

Часть 2. Что нужно уметь? Правила для пользователей сети Интернет
2.1. Правила работы с СМС
2.2. Правила работы с электронной почтой
2.3. Правила работы с видеосервисами
2.4. Правила работы в социальных сетях
2.5. Правила защиты от вирусов, спама, рекламы и рассылок
2.6. Правила защиты от негативных сообщений
2.7. Правила общения в социальной сети
2.8. Правила работы с поисковыми системами и анализ информации
2.9. Правила ответственности за распространение ложной и негативной информации
2.10. Правила защиты от нежелательных сообщений и контактов
2.11. Правила вызова экстренной помощи
2.12. Правила защиты устройств от внешнего вторжения
2.13. Правила выбора полезных ресурсов в Интернете
2.14. Средства работы в Интернете для людей с особыми потребностями

Рисунок 1 - Поурочное планирование учебного пособия 5-6 класс М.С. Цветкова, Е.В. Якушина

Учащихся знакомят с работой в сети Интернет с помощью демонстрации на примере использования различных устройств доступа к сети. Начинается курс с урока об информационном обществе. В каждом уроке практическая часть представлена в виде теста, компьютерного задания. Темы курса сформулированы в форме проблем, решить которые возможно благодаря знаниям о сети Интернет и тем, как использовать ресурсы сети при работе самостоятельно.

Также учащихся знакомят с понятиями всемирной паутины. Всемирная паутина — это Сеть с информацией, которая размещена на разных компьютерах. Информация имеет адрес (имя), по которому её можно отыскать в Сети. Она передаётся в цифровых кодах, а смотреть и читать на компьютерах и устройствах, подключённых к Сети, её можно в привычном нам виде.

Также для объяснения работы с Сетью вводят понятие веб-сайтов, которое для лучшего понимания поясняется на примере страниц в книге, информация на которых изменяется, включать видео- и аудио-вставки, а также ссылки — слова или картинки, по которым переходят на другие веб-страницы, в отличии от печатной версии книг.

В учебниках Н.Д.Угринович «Информатика и ИКТ.8 класс»[49] разделу «Коммуникационные технологии» отведена 3 глава, на её изучение отведено 8 часов. Данная глава состоит из нескольких параграфов: «3.4 Информационные ресурсы Интернета», «3.4.1. Всемирная паутина», «3.4.4. Общение в Интернете».

Учащихся знакомят с понятием браузера — специальная программа, с помощью которой осуществляется просмотр web-страниц. Объясняют его устройство и элементы окна приложения. Дают понятие интернет адреса и знакомят с электронной почтой.

Электронная почта(e-mail) — наиболее распространённый сервис Интернета, который не требует обязательного наличия высокоскоростных и качественных линий связи. Вводят понятие адреса электронной почты, рассказывают её подробное устройство и описание, при этом описывая функции электронной почты, процесс передачи писем от отправителя к получателю.

В свою очередь, учащихся знакомят с понятием электронного сервиса, рассказывают про социальные коммуникации, социальные сети — онлайн-платформы, которые используются людьми для передачи информации, общения и т.д.

Социальная сеть позволяет людям из разных уголков мира мгновенно связываться и общаться друг с другом, например, в группах, объединённых общими интересами.

Сайты сетей, которые проверены и разрешены для просмотра детям, отмечены категорией возраста. Для сайтов детских социальных сетей, предложенных далее, это «0+».

При этом поясняется, что интернет-коммуникации имеют и негативную сторону и могут нести в себе угрозы. Так, в процессе взаимодействия возможно распространение ложной, агрессивной, грубой, некорректной информации, навязчивой рекламы. Нельзя с точностью знать, кто выходит с нами на контакт, так как в Сети можно использовать заставку, которая совсем не соответствует реальному образу.

Недостатком частого и бессистемного использования Интернета является также появление зависимости.

Сеть заменяет творчество, активный досуг, общение со сверстниками, близкими людьми, отбирает всё свободное время. Важно знать, что ваше подключение к любой социальной сети в Интернете предоставляет чужим людям вашу личную информацию, которой они могут воспользоваться в недобрых целях. Номер телефона, адрес проживания, номер школы, где вы учитесь, не должны передаваться в открытый доступ.

В учебнике К.Ю. Полякова , А Е. Еремина «Информатика, 7 класс. Часть 1» [39] на изучение Интернета отводится 1 параграф. Всего на раздел «Информационные и коммуникационные технологии» в 7 классе отводится 34 часа. На «Компьютерные сети» в данном учебнике в 7 классе отводится 1 час «Глава 1. Введение. §4 Интернет».

Учащиеся должны знать принципы построения компьютерных сетей. Также должны уметь искать информацию в сети Интернет, использовать сервисы Интернета, грамотно строить личное информационное пространство, соблюдая при этом правила информационной безопасности.

Тематическое планирование данного учебника с учетом минимального варианта учебного плана представлен ниже (рис.2).

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

Минимальный вариант учебного плана

для учебного плана объемом 102 часа
(7–9 классы, по 1 часу в неделю)

№	Тема	Количество часов/класс			
		Всего	7 кл.	8 кл.	9 кл.
Основы информатики					
1	Информация и информационные процессы	3			3
2	Кодирование информации	11		11	
3	Компьютер	11	9	1	1
4	Основы математической логики	3			3
5	Модели и моделирование	7			7
	Итого:	35	9	12	14
Алгоритмы и программирование					
6	Алгоритмизация и программирование	27	9	10	8
	Итого:	27	9	10	8
Информационно-коммуникационные технологии					
7	Обработка числовой информации	9	1	6	2
8	Обработка текстовой информации	10	5	5	
9	Обработка графической информации	5	5		
10	Компьютерные сети	5	1		4
11	Мультимедиа	3	3		
12	Базы данных	3			3
	Итого:	35	15	11	9
	Резерв	5	1	1	3
	Итого по всем разделам:	102	34	34	34

Рисунок 2. Тематическое планирование

Учащихся знакомят с глобальной сетью — самая большая компьютерная сеть Интернет. Она была создана во второй половине 20 века.

Интернет — это глобальная(всемирная) компьютерная сеть. Интернет состоит из узлов и каналов связи между ними. Узлы принадлежат провайдерам — поставщикам услуг, с которыми пользователи заключают договоры на подключение к Интернету. Узел состоит из одного или нескольких серверов — мощных компьютеров, которые обслуживают пользователей.

Сервер — это компьютер, который отвечает на запросы других компьютеров в сети.

Серверы никогда не отключаются от сети и постоянно ожидают запросов пользователей. Как только такой запрос приходит, сервер выполняет задание и

отправляет запрошенную информацию. Каждый сервер имеет свой адрес в сети, который называется IP-адресом.

Также ученикам даётся понятие гипертекста — это текст, содержащий активные ссылки (гиперссылки) на другие документы. В верхней части каждой вкладки есть адресная строка, в которой можно ввести имя нужного сайта или адрес веб-страницы. После нажатия клавиши Enter браузер отправляет запрос на узел Интернета (компьютер), зарегистрированный по этому адресу. На этом узловом компьютере должна быть запущена программа, которая называется веб-сервером.

Веб-сервис — это программа, которая пересылает на компьютеры пользователей веб-страницы и файлы по запросу браузера.

Ученикам дается пояснение того, что не вся информация размещённая в Интернете достоверна. В отличии от научных книг и журналов, статьи в Интернете чаще всего не рецензируются, поэтому истинность информации остаётся целиком на совести автора. Проверить достоверность информации в Интернете очень сложно. Для оценки достоверности информации важна авторитетность сайта — как часто на него ссылаются с других сайтов, как оценивают сайт поисковые системы.

Последнее с чем знакомят учащихся — это поисковые системы. Простейшие запросы для поисковых систем это просто перечисление ключевых слов.

Таким образом, можно сделать вывод, что во всех учебниках школьного курса информатики широко представлена тема «Информационная безопасность в сети Интернет». Однако, следует отметить, что практически ни в одном учебнике не представлена данная тема в полном объёме. Также, в учебниках и курсах, где в полной мере представлен теоретический материал, на практические занятия отводится недостаточно часов или данные занятия отсутствуют. Или наоборот, широко и подробно изучается лишь один вид практической деятельности на компьютере. Таким образом, возникает потребность изучения информационной безопасности в таком формате, где

достаточное количество учебных часов направлены не только на теоретический материал, но и на практическую деятельность.

1.3 Электронный учебно-методический комплекс по разделу «Информационная безопасность в сети Интернет» как компонент дополнительного образования у детей и подростков

Современное образование не стоит на месте и стремительно развивается. Привычные печатные информационные ресурсы (учебники, методические пособия, энциклопедии и т.д.) сменяются электронными информационными ресурсами и технологиями. Всё переходит в электронный формат.

В связи с активным распространением информационных ресурсов и технологий в различных сферах деятельности людей необходимым становится проектирование новых подходов образовательной среды. Используя автоматизированные системы управления и машинное обучение, на основе анализа информации преподаватели могут обеспечить эффективный подход к вопросам повышения качества образования.

В настоящий момент активно расширяется сфера применения информационных и коммуникационных технологий. В связи с этим вопрос применения информационных и коммуникационных технологий становится наиболее актуальным в системе образования на всех его уровнях.

Определение понятия «информационно-коммуникационные технологии» рассматривается в «Энциклопедии профессионального образования» Захаровой И.Г., И.В. Робертом, Семакиным И.Г., Григорьевой С.Г. [17,41,38].

Информационно-коммуникационные технологии — это программные, программно-аппаратные и технические средства и устройства, функционирующие на базе микропроцессорный, вычислительной техники, а также современных средств и систем транслирования информации, информационного обмена, обеспечивающие операции по сбору, продуцированию, накоплению, хранению, обработке, передаче информации и

возможность доступа к информационным ресурсам компьютерных сетей, в том числе глобальных.

Главной целью развития данных технологий является возможность быстрого доступа к информационным ресурсам и обеспечение оперативного информационного взаимодействия.

Информационная образовательная среда — сложная система, которая включает в себя интеллектуальные, культурные, программно-методические, организационные и технические ресурсы и обеспечивающая формирование гармонично развитой личности учащегося. Внедрение и использование цифровых образовательных ресурсов обеспечивает информационно-методическую поддержку учебного процесса, своевременный, системный мониторинг и анализ результатов образовательного процесса, дистанционное взаимодействие преподавателя и учащихся.

В учебном пособии А.А. Кузнецова, Т.Б.Захаровой, А.С.Захарова «Общая методика обучения информатике»[19] курс «Основы информационной безопасности» ориентирован на обучающихся 9 классов, которые проявляют интерес к защите информации, желают изучить правовые аспекты информационной безопасности, которые имеют представления о средствах защиты компьютеров от сбоя, защите данных в телекоммуникационных сетях.

Данный курс предполагает развитие знаний и умений, которые были сформированы на основном курсе, для углубленного осваивания оснв информационной безопасности.

Во введении ученикам рассказывается про сущность понятия информационной безопасности, а также про его эволюцию. Поясняется информационная безопасность в условиях информатизации общества, компьютерная безопасность, интересы личности в информационной сфере. А также национальные интересы РФ в информационной сфере, безопасность информационной технологии и системный подход к решению проблем защиты информации.

В теме 1 «Правовые аспекты информационной безопасности» рассматривается информация, как юридический объект защиты. Общедоступная, секретная и конфиденциальная информация. Поясняется что такое авторское право и основные положения закона «О правовой охране программ и данных».

Тема 2 «Методы и средства защиты информации» повествует о формировании электронной цифровой подписи и аутентификаторе, а также об управлении доступом к тем или иным данным.

В теме 3 «Защите данных в информационных системах» поясняет целостность данных в ИМ и ограничения целостности, особенности защиты данных в ИС, основанной на криптографии.

В 4 теме «Защита информации в сети Интернет» поясняются основные технологии обеспечения защиты информации в сети Интернет, средства защиты информации в сети Интернет, а также поясняются их функции.

В образовании все интенсивнее развиваются электронные средства обучения (ЭСО).

Электронные средства обучения — это программные средства, которые отражают определённую предметную область, где в той или иной мере реализуется технология её изучения с помощью средств информационно-коммуникационных технологий, а также обеспечиваются условия для осуществления различных видов учебной деятельности.

Электронные средства обучения содержат систематизированный материал по соответствующей научно-практической области знаний, обеспечивают творческое и активное овладение учащимися знаниями, умениями и навыками в этой области. ЭСО должно отличаться высоким уровнем исполнения и художественного оформления, полнотой информации, качеством методического инструментария, качеством технического исполнения, наглядностью, логичностью и последовательностью изложения. Благодаря специфике своего определения, ЭСО существенно повышают качество визуальной и аудиоинформации, она становится ярче, красочнее,

динамичнее. Огромными возможностями обладают в этом плане современные технологии мультимедиа. Разные виды ЭСО имеют свою специфику создания, назначения и использования.

Основными видами ЭСО являются: электронные учебно-методические комплексы (ЭУМК); электронные курсы; электронные учебники (ЭУ); автоматизированные обучающие системы (АОС); программные средства для контроля и измерения уровня знаний, умений и навыков обучающихся; электронные тренажеры; программные средства лабораторий удаленного доступа и виртуальных лабораторий; экспертные обучающие системы (ЭОС); интеллектуальные обучающие системы (ИОС).

Основой для ЭСО является грамотно составленное методическое обеспечение образовательного процесса.

Методическое обеспечение образовательного процесса (МООП) — это комплекс всей учебно-методической документации, представленной в виде систематизированного описания образовательного процесса, которое впоследствии будет реализовано на практике. Именно методическое обеспечение задаёт структуру образовательного процесса, отражает его основные элементы.

Основными требованиями к содержанию МООП вне зависимости от его направления являются:

1) полное отражение содержания по подготовке учащихся по конкретной учебной дисциплине, курса, модуля, раздела и т.д;
2) обязательное содержание всего необходимого дидактического материал, позволяющего учащимся достичь необходимо уровня усвоения;
3) предоставление каждому учащемуся возможность в удобное время самостоятельно проверить собственные знания и откорректировать свою учебную деятельность;
4) включение в комплекс наиболее объективных и эффективных методов контроля качества предоставляемого образования.

В ряду ЭСО особое значение имеют электронные учебно-методические комплексы. Если традиционный учебно-методический комплекс – это система нормативной и учебно-методической документации, средств обучения и контроля, необходимых и достаточных для качественной организации основных и дополнительных образовательных программ, согласно учебного плана. Возможности ЭУМК значительно шире.

С позиций системотехники электронный учебно-методический комплекс (ЭУМК) – это автоматизированная информационная система (АИС) учебного назначения, которая на новом качественном уровне обеспечивает непрерывность и полноту дидактического цикла процесса обучения и содержит организационные и систематизированные теоретические, практические, контролирующие материалы, построенные на принципах интерактивности, информационной открытости, дистанционности и формализованности процедур оценки знаний.

Электронный учебно-методический комплекс — это версия учебно-методических материалов, которая представлена в виде программного мультимедиа продукта учебного назначения. Он обеспечивает непрерывность и полноту дидактического цикла процесса обучения.

Структура ЭУМК должна включать в себя, помимо обучающего блока, блока контроля и оценки знаний, блок обо всех компонентах учебной дисциплины, которые входят в состав рабочей программы, для планирования образовательной траектории и расписания обучающихся.

И. А. Позанова [33] выделяет в зависимости от масштаба охватываемой предметной области электронные учебно-методические комплексы по дисциплинам (ЭУМКД) и по специальности (или направлению) (ЭУМКС). В плане функционирования электронный учебно-методический комплекс имеет обеспечивающую и функциональную части.

В состав обеспечивающей части входит:

1) информационное обеспечение — это совокупность проектных решений по объемам, размещению, формам организации учебной и методической

информации (ФГОС для данной специальности; рабочие программы; фондовые лекции; учебные пособия для отработки практических и лабораторных заданий; перечни выносимых на зачет и экзамен учебных вопросов; тесты промежуточного контроля остаточных знаний; учебные и учебно-методические пособия; список рекомендованной литературы, адреса веб-сайтов в сети Интернет);

2) техническое обеспечение — комплекс технических средств, предназначенных для обеспечения его работы, а также соответствующая документация на эти средства и технологические процессы (мультимедийные проекторы; интерактивные доски; системы видеоконференций; компьютерные тренажеры; средства компьютерной техники; компьютерные сети и устройства для подключения компьютеров к ним; средства для оперативной печати (копирования) раздаточного материала);
3) математическое и программное обеспечение ЭУМК — это совокупность математических методов, моделей, алгоритмов, используемых в учебных целях для решения задач, а также системные и специальные программные продукты, прикладное программное обеспечение и техническая документация к ним;
4) методическое и организационное обеспечение ЭУМК — это совокупность средств и методов, средств и документов, регламентирующих взаимодействие преподавателя и ЭУМК, обучаемого и преподавателя, обучаемого и ЭУМК в этапах его разработки и использования в учебном процессе.

Функциональная часть ЭУМК должна определяться теми задачами, для которых он разрабатывается:

1) для оказания методической помощи преподавателям при подготовке и проведении занятий по данной дисциплине;

2) как средство комплексного воздействия на обучаемого путём сочетания концептуальной, иллюстративной, справочной, тренажерной и контролирующей частей.

Структура и пользовательский интерфейс обеспечивающей и функциональной частей ЭУМК должны обеспечить эффективную помощь преподавателю для организации учебного процесса и обучаемому при изучении дисциплины. Использование ЭУМК в образовательном процессе дает педагогам дополнительные дидактические возможности:

1) обратную связь между пользователем и ЭСО, что позволяет обеспечить интерактивный диалог;
2) компьютерную визуализацию учебной информации, предполагающую реализацию возможностей современных средств визуализации объектов, процессов, явлений (как реальных, так и виртуальных), а также их моделей, представление их в динамике;
3) компьютерное моделирование изучаемых объектов, явлений, процессов;
4) автоматизацию процессов вычислительной и информационно-поисковой деятельности;
5) автоматизацию процессов управления учебной деятельностью и контроля за результатами усвоения материала.

Таким образом, необходимо отметить, что использование разных видов ЭСО в образовательном процессе значительно влияет на формы и методы представления учебного материала, характер взаимодействия между обучаемым и педагогом и, соответственно, на методику проведения занятий. Вместе с тем ЭСО не заменяют традиционные подходы к обучению, а значительно повышают их эффективность. Любой из типов уроков может быть проведен с использованием ЭСО. Главное для педагога — найти соответствующее место ЭСО в образовательном процессе. Создание ЭУМК имеет особое значение, так как позволяет комплексно подходить к решению основных дидактических задач с использованием информационных ресурсов и

ЭСО. ЭУМК - это инновационный образовательный продукт, обладающий новыми дидактическими возможностями.

Выводы по главе 1

Подводя итог теоретической части исследования можно сделать несколько обобщающих выводов:

1. В результате всестороннего анализа научно-педагогических и методических основ обучения информационной безопасности в сети Интернет в школьном курсе информатики было выявлено, что тема «Интернет» представлена как обязательная в:
   1) Федеральном государственном образовательном стандарте среднего образования [1];
   2) примерной образовательной программе среднего общего образования [2];
   3) учебниках И.Г. Семакина [17], К. Ю. Полякова [26, Н.В. Макаровой [28], Н.Д. Угринович [45], И.Н. Калинина [49], А.Г. Гейна [13], М.Ю. Монахова [30].
2. Анализ содержания обучения раздела «Информационная безопасность в сети Интернет» в курсе информатики средней школы позволил нам выделить и определить основные понятия глобальная сеть, ее виды и уровень сформированности практических навыков учащихся в среде современных информационных ресурсов.
3. В соответствии с утвержденной Министерством образования Российской Федерации «Концепцией базового обучения на младшей ступени общего образования» [3] методическое обеспечение занятий «Информационная безопасность в сети Интернет» может рассматриваться в качестве дополнительного компонента образования основной ступени школы.

Глава 2 Проектирование и реализация ЭУМК по разделу «Безопасность в сети Интернет»

2.1 Дидактические, программно-технологические и технические характеристики ЭУМК

Для проектирования и реализации ЭУМК по информационной безопасности в сети Интернет необходимо проанализировать целевую аудиторию, выполнить постановку целей и задач ЭУМК, определить его структуру и содержание, выбрать формы и средства представления учебных материалов.

Программа курса «Цифровая гигиена» состоит из двух модулей и адресована учащимся 7, 8, 9 классов (Модуль1), а также родителям обучающихся всех возрастов с 1 по 9 класс (Модуль 2). Программа учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам. Разработана на основании примерной рабочей программы учебного курса «Цифровая гигиена», рекомендованной Координационном советом Учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019), на основе программы курса «Информаци-онная безопасность, или на расстоянии одного вируса» Наместниковой М.С

Цель ЭУМК по информационной безопасности в сети Интернет – это формирование у учащихся 7-9 классов навыков самоанализа и систематизации знаний, позволяющих эффективно и безопасно использовать технические и программные средства решения различных задач, в том числе использования компьютерных сетей, полученных в процессе обучения; закрепление основных понятий информационной безопасности в сети Интернет, развитие умений своевременно распознавать онлайн-риски.

Задачи ЭУМК:

1) сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
2) создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
3) сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
4) сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
5) сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Предметные результаты освоения ЭУМК по информационной безопасности:

учащийся должен знать:

1) приёмы безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов;
2) основы соблюдения норм информационной этики и права;
3) безопасное использование средств коммуникаций.

учащийся должен уметь:

1) анализировать доменные имена компьютеров и адреса документов в интернете;
2) безопасно использовать средства коммуникации;

3) безопасно вести и применять способы самозащиты при попытке мошенничества;
4) безопасно использовать ресурсы интернета

учащийся должен владеть:

1) основами соблюдения норм информационной этики и права;
2) основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
3) использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

Метапредметные результаты:

Регулятивные универсальные учебные действия. В результате освоения учебного курса обучающийся сможет:

1) идентифицировать собственные проблемы и определять главную проблему;
2) выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
3) ставить цель деятельности на основе определенной проблемы и существующих возможностей;
4) выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
5) составлять план решения проблемы (выполнения проекта, проведения исследования);
6) описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
7) оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
8) находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;

9) работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
10) принимать решение в учебной ситуации и нести за него ответственность. Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

1) выделять явление из общего ряда других явлений;
2) определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
3) строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
4) излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
5) самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
6) критически оценивать содержание и форму текста;
7) определять необходимые ключевые поисковые слова и запросы. Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

1) строить позитивные отношения в процессе учебной и познавательной деятельности;
2) критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
3) договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
4) делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его;

5) целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
6) выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации; использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
7) использовать информацию с учетом этических и правовых норм; - создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Личностные результаты:

1) осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
2) готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
3) освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
4) сформированность понимания ценности безопасного образа жизни;
5) интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

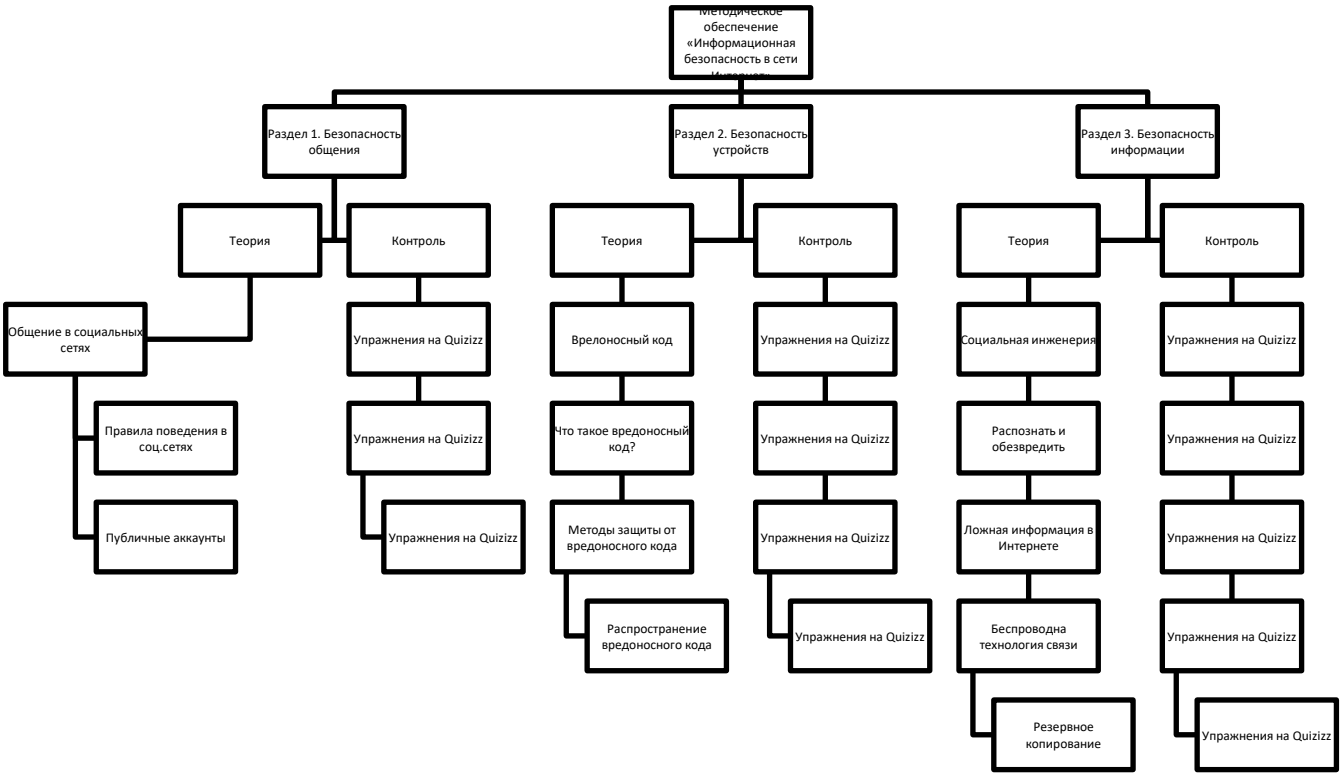


Рисунок 3. Структура методического обеспечения

2.2 Педагогический и технологический сценарий ЭУМК

Перед тем, как начинать создание учебно-методический комплекс, необходимо разработать общий план и его структур. Процесс разработки ЭОР состоит из двух основных этапов:

На первом подготовительном этапе производится:

1) подбор источников и формирование основного содержания;
2) структуризация материала и разработка оглавления или сценария;
3) переработка текста и формирование основных разделов;
4) выбор, создание и обработка материала для мультимедийного воплощения (видеосюжеты, звуковое сопровождение, графические изображения).

На втором этапе компоновки производится сборка в единое целое всех отобранных и разработанных частей ЭОР (информационных, обучающих,

контролирующих) для предъявления обучающимся в соответствии с задуманным автором сценарием.

Планирование педагогического сценария предполагает тщательное проектирование содержания учебной деятельности и использования педагогических технологий. Для решения этих задач на этапе проектирования необходимо подготовить развернутую программу, подобрать учебный материал, подготовить задания, проставить порог прохождения каждого из заданий, прописать формулу оценивания результатов по курсу, составить сценарии лекций и рекламного видеоролика, подготовить для слушателей приветственное обращение и разработать методические рекомендации по изучению курса. Эти сведения представлены в виде таблиц 1 и 2.

Таблица 1 – Общие данные о ЭУМК

Название ЭУМК	Объектно-ориентированное программирование
Основная информация	Данный курс будет полезен для учащихся 6-9 классов, которые начинают знакомиться и активно использовать сеть Интернет. В курсе будут поэтапно разобраны понятия, связанные с использованием Интернета, опасности, которые ожидают пользователя Интернетом,и как их избежать. Изучение теории, которую возможно будет проверить на практике.
Формат	Курс состоит из 10 уроков Нагрузка: 1 занятие в неделю (лекция и тестирование)
Требования	Для прохождения курса необходимо: • иметь доступ в Интернет • завести аккаунт в Google • уметь пользоваться ПК
Программа ЭУМК	1. Введение. Использование Google Classroom 2. Общение в сети 3. Публичные аккаунты 4. Вредоносный код 5. Что такое вредоносный код 6. Методы защиты от вредоносного кода 7. Распространение вредоносного кода 8. Социальная инженерия: распознать и избежать 9. Ложная информация в Интернете 10. Беспроводная технология связи

Продолжение таблицы 2

Результаты обучения	Формирование у учащихся 6-9 классов навыков самоанализа и систематизации знаний, полученных в процессе обучения; развитие умения анализировать полученные знания.
Информация о преподавателе	Молодец Анастасия Петровна, студентка Поволжского православного института Электронная почта: Anastasiya.molodecz@mail.ru Телефон: 89171343999

Таблица 2 – Структура ЭУМК

Раздел	Содержание	Компоненты
Введение	Описание курса	Приветственное видео
	Ознакомление с курсом	Вспомогательное видео для использования GoogleClassroom
Тема 1. Использование Google Classroom	Лекция 1. Использование Google Classroom	Презентация, конспект
	Упражнения для закрепления материала	Упражнения на Quizizz
Тема 2. Общение в сети Интернет	Лекция 2. Общение в сети	Презентация, конспект
	Упражнения для закрепления материала	Упражнения на Quizizz
Тема 3. Публичные аккаунты в сети Интернет	Лекция 3. Публичные аккаунты	Презентация, конспект
	Упражнения для закрепления материала	Упражнения на Quizizz
Тема 4. Вредоносный код	Лекция 4. Вредоносный код	Презентация, конспект
	Упражнения для закрепления материала	Упражнения на Quizizz
Тема 5. Что такое вредоносный код?	Лекция 5. Что такое вредоносный код	Презентация, конспект
	Упражнения для закрепления материала	Упражнения на Quizizz
Тема 6. Методы защиты	Лекция 6. Методы защиты от вредоносного кода	Презентация, конспект
	Упражнения для закрепления материала	Упражнения на Quizizz

Продолжение Таблицы 2

Тема 7. Распространение вредоносного кода	Лекция 7. Распространение вредоносного кода	Презентация, конспект
	Упражнения для закрепления материала	Упражнения на Quizizz
Лекция 8. Социальная инженерия: распознать и избежать	Лекция 8. Социальная инженерия: распознать и избежать	Презентация, конспект
	Упражнения для закрепления материала	Упражнения на Quizizz
Тема 9. Ложная информация в сети	Лекция 9. Ложная информация в Интернете	Презентация, конспект
	Упражнения для закрепления материала	Упражнения на Quizizz
Тема 10. Беспроводные технологии связи	Лекция 10. Беспроводная технология связи	Презентация, конспект
	Упражнения для закрепления материала	Упражнения на Quizizz

Электронный учебно-методический комплекс представлен введением и десятью темами, включающими в себя теоретический материал и практические задания.. В качестве дополнительных средств обучения в курсе используются авторские электронные образовательные ресурсы (ЭОР): видеолекция и интерактивные упражнения в облачном сервисе LearningApps [2] и Quizizz[3]. Сам ЭУМК расположен в системе управления обучением GoogleClassroom [13].

В таблице 3 представлено тематическое планирование ЭУМК по для учащихся младших классов базового курса информатики с использованием разработанных электронных образовательных ресурсов

Таблица 3 – Тематическое планирование ЭУМК

Тема урока	Практическое задание	Количество часов
Тема 1. Введение. Использование Google Classroom	-	0,5
Тема 2. Общение в сети Интернет	Интерактивное упражнение «Социальные сети»	1

Продолжение таблицы 3

Тема 3. Публичные аккаунты в сети Интернет	Интерактивное упражнение «Общение в социальных сетях»	1
Тема 4. Безопасность устройств	Интерактивное упражнение «Поняти вредоносного кода»	1
Тема 5. Вредоносный код.Что такое вредоносный код?	Интерактивное упражнение «Виды вредоносного кода»	1
Тема 6. Методы защиты	Интерактивное упражнение «Защита в Сети»	1
Тема 7. Распространение вредоносного кода	Интерактивное упражнение «Как распространяется вредоносный код»	1
Лекция 8. Социальная инженерия: распознать и избежать	Интерактивное упражнение «Безопасность информаии»	1
Тема 9. Ложная информация в сети	Интерактивное упражнение «Целевая атака»	1
Тема 10. Беспроводные технологии связи	Интерактивное упражнение «Резервное копирование данных»	1
	Всего часов	10,5

ЭУМК включает в себя две части: теоретическую и практическую. Первая часть представлена в виде лекций. Каждая лекция содержит определенный набор определений и понятий.

Вторая часть организованна в виде практических заданий. В ходе практических занятий учащиеся не только закрепляют навыки и умения пользования сетью Интернет, но и развивают этические нормы общения.

Подробное описание каждого из модулей содержится в следующих параграфах.

2.3 Проектирование и реализация теоретико-познавательного модуля ЭУМК

Теоретико-познавательный модуль ЭУМК по оинформационной безопасности в сети Интернет организован в форме лекций и рассчитан на 10 учебных часов (таблица 4).

Таблица 4 – Структура теоретико-познавательного модуля

№	Тема	Описание	Кол-во часов
1	Безопасность общения	Лекция знакомит учащихся с понятиями социальной сети, её появлением, знакомит с понятием мессенджера, аккаунтом социальной сети и его элементами, пользовательским контентом и т.д.	1
2	Общение в социальных сетях	Видео- материал рассказывает учащимся про общение в социальных сетях.	1
3	Публичные аккаунты	Лекция знакомит учащихся с понятиями публичного аккаунта, поясняет разницу между публичным и приватным аккаунтами, что представляет собой аккаунт, поясняет правила ведения публичной страницы.	1
4	Безопасность устройств. Что такое вредоносный код?	Лекция знакомит учащихся с понятиями вируса, виды вредоносных кодов, признаки, классификация вредоносвх кодов, а также с понятиями руткит и бэкдор. Рассказывает про самые страшные компьютерные вирусы в истории человечества	1

Продолжение таблицы 4

5	Вредоносный код	Лекция знакомит учащихся с вредоносным кодом, деструктивные функции вредоносных кодов, а также даёт основные признаки проявления вирусов, признаками вредоносных кодов, исторические факты про вредоносные коды, виды вредоносных кодов.	1
6	Методы защиты от вредоносного кода	Лекция знакомит учащихся с распространением вредоносного кода для мобильных устройств, принцип действия антивируса, история мобильного вируса, рассказывает о важности антивируса и о том, как избежать взлом устройства, виды вредоносного мобильного ПО.	1
7	Распространение вредоносного кода	Лекция знакомит учащихся с распространение вредоносного кода, как его опознать, определить вредоносное расширение, в каких случаях возможно заражение вредоносным кодом, даёт понятие спама, скрипта, лицензионный и пиратский контент, пользовательский контент.	1
8	Социальная инженерия: распознать и избежать	Лекция знакомит учащихся с понятиями социальной инженерии, целевой атакой, также приводится примеры опасных действий, киберприступники, транзакции,критический анализ	1

Продолжение таблицы 4

9	Ложная информация в Интернете.	Лекция знакомит учащихся с понятиями ложной информации, фейковыми новостями, СМИ, безопасностью при использовании платёжных карт в Интернете.	1
10	Беспроводная технология связи. Резервное копирование данных.	Лекция знакомит учащихся с понятиями Wi-Fi, роутером, понятием публичной сети, правила работы с Wi-Fi в публичном месте, резервным копированием данных, автоматическим созданием резервных копий.	1

Цель - сформировать представление об информационной безопасности, о ключевых принципах и понятиях, о правилах поведения в Сети, о технологиях беспроводной связи.

Задачи:

1) изучить базовые понятия информационной безопасности в Сети Интернет;
2) рассмотреть принципы и устройство Сети Интернет.

Изучив данный модуль, учащийся должен:

знать:

1) приемы безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
2) основы соблюдения норм информационной этики и права;
3) использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет ресурсы и другие базы данных.

уметь:

1) анализировать доменные имена компьютеров и адреса документов в интернете;
2) безопасно использовать средства коммуникации;
3) безопасно вести и применять способы самозащиты при попытке мошенничества;
4) безопасно использовать ресурсы интернета.

Темы уроков и основные моменты.

Тема 1. Безопасность общения.

Учебные вопросы:

- Социальная сеть.
- История социальных сетей.
- Мессенджеры.
- Назначение социальных сетей и мессенджеров.
- Пользовательский контент.

Тема 2.Общение в социальных сетях

Учебные вопросы:

- Персональные данные.
- Публикация личной информации.

Тема 3. Публичные аккаунты.

Учебные вопросы:

- Настройки приватности публичных страниц.
- Правила ведения публичных страниц.

- Определение кибербуллинга.

Тема 4. Безопасность устройств. Что такое вредоносный код?

Учебные вопросы:

- Виды вредоносных кодов.
- Возможности и деструктивные функции вредоносных кодов

Тема 5. Безопасность устройств. Что такое вредоносный код?

Учебные вопросы:

- Виды вредоносных кодов.
- Возможности и деструктивные функции вредоносных кодов.

Тема 6. Методы защиты от вредоносного кода

Учебные вопросы:

- Способы защиты устройств от вредоносного кода.
- Антивирусные программы и их характеристики.
- Правила защиты от вредоносных кодов.

Тема 7. Распространение вредоносного кода для мобильных устройств.

Учебные вопросы:

- Расширение вредоносных кодов для мобильных устройств.
- Правила безопасности при установке приложений на мобильные устройства

Тема 8. Социальная инженерия: распознать и избежать

Учебные вопросы:

- Приемы социальной инженерии.
- Правила безопасности при виртуальных контактах

Тема 9. Ложная информация в Интернете.

Учебные вопросы:

- Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей.
- Фейковые новости.
- Поддельные страницы

Тема 10. Беспроводная технология связи. Резервное копирование данных.

Учебные вопросы:

- Уязвимость Wi-Fi-соединений.
- Публичные и непубличные сети.
- Правила работы в публичных сетях.
- Безопасность личной информации.
- Создание резервных копий на различных устройствах.

2.4 Проектирование и реализация контрольного модуля

Контрольный модуль курса «Информационная безопасность в сети Интернет» реализован в виде тестового задания и интерактивных упражнений в сервисе Quizizz [3] и рассчитан на 2 учебных часа.

Интерактивные упражнения - это различные задания, направленные на закрепление знаний в игровой форме. Данные электронно-образовательные ресурсы способствует формированию познавательного интереса учащихся и повышает мотивацию к обучению. Также, они обеспечивают чередование учебной деятельности, что снизит усталость и напряжение учащихся.

Для интерактивных упражнений был выбран веб-сервис Quizizz. Данное приложение – это конструктор различных заданий, которые можно использовать непосредственно на уроках или внеклассной работе. Они направленны на проверку и закрепление знаний в игровой форме. Данный веб-инструмент направлен для проведения экспресс-опросов, тестов, викторин по различным предметам. Каждый преподаватель с помощью данного веб-сервиса может создать свое уникальное интерактивное упражнение по разным предметам и дисциплинам из предложенной коллекции различных шаблонов. Quizizz можно проводить как в классе, так и предлагать в качестве домашней работы. При проведении опроса учащиеся отвечают на вопросы в индивидуальном темпе. Также на сервисе имеется функция поиска для нахождения различных заданий конкретного автора или по конкретной теме, и на примере понравившегося создать свое упражнение и разместить его на своей своем сайте. Одним из ключевых достоинств данного веб-сервиса является мгновенная проверка правильности выполнения задания, что облегчает этап контроля знаний и их оценки.

Итоговая оценка результатов прохождения курса может формироваться по результатам публичной открытой защиты зачетной работы ученика или по накопительной балльно-рейтинговой системе оценивания (за выполнение каждого упражнения, теста и т.д.).

ВЫВОДЫ ПО ГЛАВЕ 2

Практическая часть нашего исследования посвящена проектированию и реализации программно-методического обеспечения курса по безопасности в Сети Интернет.

Были описаны структура и содержание курса: цель, задачи, образовательные результаты, тематическое планирование и т.д.

Курс состоит из двух частей: теоретической и контрольной.

В процессе изучения теоретической части курса учащиеся должны познакомиться с основами устройства Интернета, с методами и способами защиты информации, основными понятиями и определениями.

Вторая часть курса представляет собой модуль контроля и диагностики знаний в форме тестирования и интерактивных упражнений.

Глава 3. Оценка эффективности разработанного ЭУМК

3.1 Общая характеристика исследования

Проведенный педагогический эксперимент был направлен на изучение реально складывающегося опыта организации учебного процесса и реализацию следующих целей:

1) исследование проблем теории и методики обучения информационной безопасности в Сети Интернет в общеобразовательной школе;
2) построение методики обучения информационной безопасности в Сети Интернет и внедрение её в практику обучения учащихся 7-9 классов;
3) проверка эффективности разработанной методики.

Педагогический эксперимент проводился в три этапа:

1. На первом (поисковом) исследовались: состояние проблемы обучения информационной безопасности в Сети Интернет в средней школе; оптимальная последовательность представления учебных материалов; теоретические и методологические предпосылки разработки методики обучения информационной безопасности в Сети Интернет в курсе информатики и ИКТ средней школы.

Это потребовало анализа соответствующей педагогической, дидактической, методической, психологической литературы, учебных планов и программ школьного предмета «Информатика и ИКТ», а также существующих учебных и методических пособий (глава 1).

Результаты поискового этапа эксперимента позволили нам обосновать актуальность темы исследования в связи с выявившимся противоречием между необходимостью создания учебных пособий и методических рекомендаций, позволяющих организовать процесс информационной безопасности в Сети

Интернет, и недостаточной разработанностью научно-практических рекомендаций в этой области.

На основе анализа актуальности и выявленных противоречий сформулирована проблема исследования, заключающаяся в обосновании дополнительных методических рекомендаций по обучению к информационной безопасности в Сети Интернет учащихся средних школ.

2. Целью второго (дидактического) этапа педагогического эксперимента являлась детальная разработка каждого компонента методики обучения информационной безопасности в Сети Интернет учащихся средних школ: определение целей и задач обучения; обоснование принципов отбора содержания обучения с последующей его детализацией и преобразованием в учебный материал; выбор оптимальных методов, средств и форм организации учебного процесса. Одной из главных задач второго этапа исследования была разработка ЭУМК курса «информационной безопасности в Сети Интернет». (Список лекционных и контрольных работ приведен в табл. 2 и 3)

Результаты этого этапа педагогического эксперимента позволили сформулировать гипотезу нашего исследования, согласно которой обучение компьютерной графике с использованием разработанного программно-методического обеспечения будет способствовать повышению:

1) теоретической и практической направленности предмета «Информатика и ИКТ» в целом;
2) уровня предметных и межпредметных результатов обучения информационной безопасности учащихся средних школ в соответствии с образовательным стандартом общего среднего образования;
3) уровня информационной и логической культуры мышления учащихся средней школы.

Проверка выдвинутой гипотезы потребовала проведения третьего (формирующего) этапа педагогического эксперимента, заключающегося в исследовании эффективности разработанной методики обучения информационной безопасности в Сети Интернет учащихся средних школ.

3.2 Методика проведения и результаты педагогического эксперимента

Педагогический эксперимент проводимого исследования был организован на базе муниципального бюджетного общеобразовательного учреждения «Классическая гимназия №39» в рамках прохождения педагогической и преддипломной практик. Изучение предмета «Информатика и ИКТ» в 7-х классах, реализуемого в рамках ФГОС [1] и учебного плана школы, проходит на базовом уровне. Обучение проводилось в компьютерном классе. Аудитория оборудована 15-ю персональными компьютерами, интерактивной электронной доской, видео-проектором, аудио-колонками, маркерной доской, организован доступ к сети Интернет.

К эксперименту были привлечены обучающиеся 7 класса.

Всего в эксперименте участвовало 25 учащихся. Во время проведения педагогического эксперимента были использованы такие эмпирические методы исследования как наблюдение, анкетирование, тестирование.

1. Организация и методика проведения констатирующего этапа педагогического эксперимента

Констатирующий этап педагогического эксперимента проводился с целью анализа состояния сформированности предметных и межпредметных результатов обучения будущих учителей информатики при освоении раздела «Информационная безопасность в Сети Интернет» в базовом курсе информатики. На этом этапе решались задачи: формирование выборки обучающихся для участия в эксперименте, а также определение диагностического инструментария. Выборка составила 20 человек. Для проверки уровня сформированности предметных и межпредметных результатов

обучения информационной безопасности в сети Интернет на констатирующем этапе был проведен проверочный тест из состава учебно-методического комплекса (УМК) «Информационная безопасность, или На расстоянии одного вируса. 7-9 классы» Наместниковой М.С. [32].

Тест состоит из 39 вопросов (приложение А). Он направлен на проверку знаний основ о безопасности информации, безопасности общения и безопасности устройств.

Количество правильных ответов учащихся свидетельствует об уровне сформированности предметных и межпредметных результатов обучения информационной безопасности в Сети Интернет. Высокий уровень предусматривает, что учащийся дает правильные ответы на не менее 90% тестовых заданий, базовый уровень – от 76 до 89% заданий, начальный – 61% до 75% и низкий – менее 60%.

Результаты тестирования учащихся экспериментальной группы на констатирующем этапе педагогического эксперимента представлены в таблице 5.

Таблица 5 - Уровень предметных и межпредметных результатов обучения по разделу «Информационная безопасность в Сети Интернет» на констатирующем этапе.

Уровень	Экспериментальная группа			
	Оценка	Количество оценок	Общее количество баллов	Среднее значение
Низкий	2	5	10	
Начальный	3	9	27	
Базовый	4	7	28	
Высокий	5	4	20	
Всего		25	85	3,4

Данные проведенного начального среза показали, что среди обучаемых экспериментальной группы на низком уровне –20% учащихся, на начальном уровне –36%; на базовом уровне–28%; на высоком уровне –16% (рис.4)

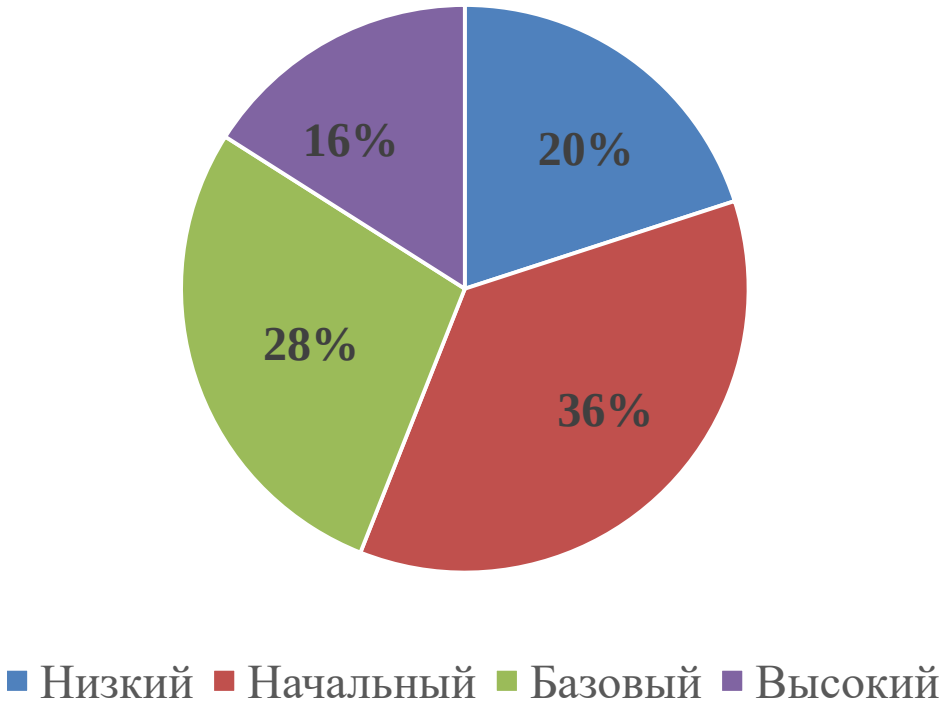


Рисунок 4 - Уровень предметных результатов обучения в экспериментальной группе на констатирующем этапе эксперимента

2. Организация и методика проведения формирующего этапа педагогического эксперимента

Целью формирующего этапа была проверка эффективности применения разработанного ЭУМК в образовательном процессе учащихся 7-х классов для формирования предметных и межпредметных результатов обучения по разделу «Информационная безопасность в сети Интернет».

На формирующем этапе педагогического эксперимента учащиеся экспериментальной группы осваивали раздел «Информационная безопасность в Сети Интернет» с использованием разработанного ЭУМК. После изучения раздела с учащимися экспериментальной группы был вторично проведен

контрольный тест на проверку уровня предметных и межпредметных результатов обучения в соответствии с ФГОС [2].

Таблица 6 - Уровень предметных и межпредметных результатов обучения по разделу «Информационная безопасность в Сети Интернет» на формирующем этапе

Уровень	Экспериментальная группа			
	Оценка	Количество оценок	Общее количество баллов	Среднее значение
Низкий	2	1	2	
Начальный	3	6	18	
Базовый	4	10	40	
Высокий	5	8	40	
Всего		25	100	4

Данные проведенного конечного среза (табл. 6) показали, что учащиеся экспериментальной группы имеют более высокие предметные и межпредметные результаты обучения: на низком уровне – 4% обучающихся; на начальном уровне – 24%; на базовом уровне – 40% и на высоком уровне – 32% обучающихся (рис. 5).

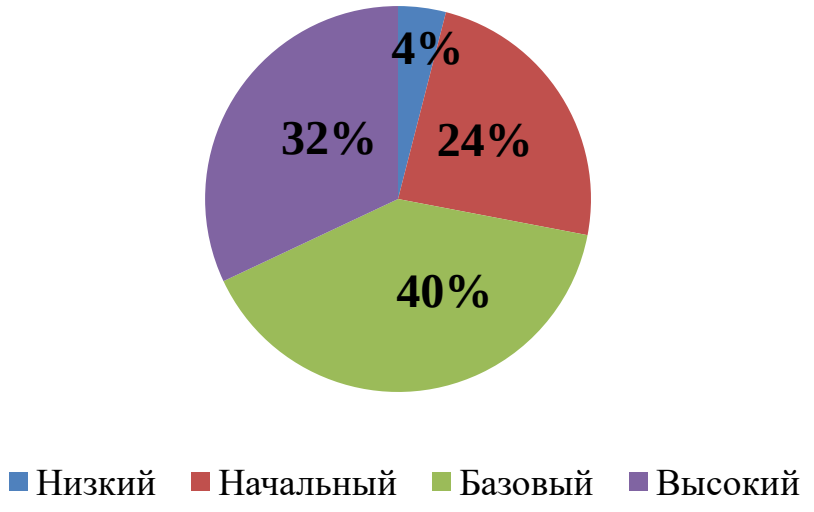


Рисунок 5 - Уровень предметных результатов обучения в экспериментальной группе на формирующем этапе эксперимента

Количество учащихся, находившихся на низком уровне сформированности предметных и межпредметных результатов обучения по разделу «Информационная безопасность в Сети Интернет» после обучения по предложенной методике снизилось до 4%, а на начальном уровне снизилось на 3 человека. Прослеживается динамика изменения количества обучающихся, находившихся на базовом уровне и высоком. На формирующем этапе их количество увеличилось на 3 человека на базовом уровне и на 4 на высоком уровне (рис. 6). Обучающиеся, имеющие на констатирующем этапе высокий уровень предметных и межпредметных результатов, в ходе прохождения курса совершенствовали свои знания, практические умения и навыки по информационной безопасности. Средняя оценка учащихся возросла на 16% (с 16% до 32%).

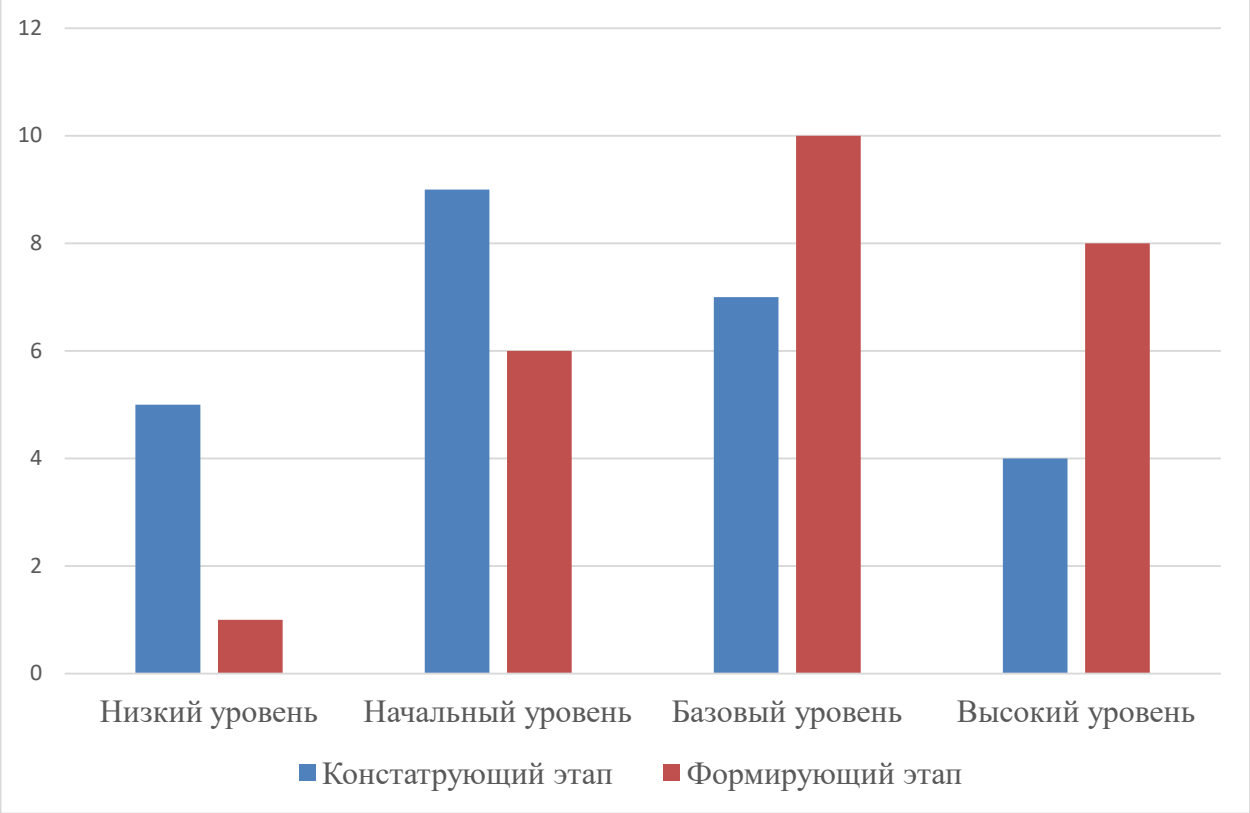


Рисунок 6 - Сравнение уровней сформированности предметных результатов обучения в экспериментальной группе на констатирующем и формирующем этапах эксперимента

Результаты педагогического эксперимента показали, что организация образовательного процесса с использованием разработанного программно-

методического обеспечения способствует повышению уровня предметных и метапредметных результатов обучения информационной безопасности в Сети Интернет учащихся средних школ в соответствии с образовательным стандартом общего среднего образования, а также положительно влияет на их уровень информационной и логической культуры мышления.

По окончанию курса, учащимся экспериментальной группы была предложена анкета, которая показала, что преподаваемая тема вызывает повышенный интерес у учащихся. Также 100% учащихся отметили положительный эффект использования разработанных электронных образовательных ресурсов (видео-уроков, интерактивных тестов) при освоении учебного материала раздела «Информационная безопасность в Сети Интернет».

Таким образом, мы можем сделать вывод о достоверном повышении результативности обучения по предлагаемой методике и подтверждении гипотезы, выдвинутой в начале исследований.

ЗАКЛЮЧЕНИЕ

В ходе теоретического и экспериментального исследования, направленного на проектирование и разработку ЭУМК - курса «Информационная безопасность в сети Интернет» для учащихся средней школы, были получены следующие основные результаты:

- в теоретической части исследования обоснована актуальность; описаны состояние проблемы обучения информационной безопасности в средней школе, теоретические и методологические предпосылки разработки методики обучения информационной безопасности в курсе информатики; проанализированы педагогическая, дидактическая, методическая и психологическая литература, нормативно-правовая документация, учебные планы и программы школьного предмета «Информатика и ИКТ»;

- практическая часть исследования представлена программно-методическим обеспечением «Информационная безопасность с Сети Интернет». Были описаны структура и содержание ЭУМК, разработаны теоретико-познавательный и контрольные модули, направленные на знакомство учащихся с информационной безопасностью, методами и способами защиты от вредоносного кода, основными понятиями и определениями, а также на приобретение навыков и умений работы в различных Интернет ресурсах, браузерах и т.д.;

- был проведен педагогический эксперимент в рамках прохождения педагогической и преддипломной практик на базе муниципального бюджетного общеобразовательного учреждения «Классическая гимназия №39». Эксперимент был разделен на два этапа: констатирующий – целью которого было получение результатов о уровне сформированности предметных и метапредметных результатов обучения информационной безопасности в 7-х классах; формирующий - посвященный проверки эффективности применения

разработанного ЭУМК в образовательном процессе учащихся 7-х классов для формирования предметных и метапредметных результатов по разделу «Информационная безопасность в Сети Интернет». Результаты педагогического эксперимента показали, что организация образовательного процесса с использованием разработанного ЭУМК обеспечения способствует повышению уровня предметных и межпредметных результатов обучения информационной безопасности учащихся средних школ в соответствии с образовательным стандартом общего среднего образования, а также положительно влияет на их уровень информационной культуры мышления.

Таким образом, мы можем сделать вывод о достоверном повышении результативности обучения по предлагаемой методике и подтверждении гипотезы, выдвинутой в начале исследований.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ N 24480 Федеральный Государственный образовательный стандарт среднего общего образования: утвержден приказом Министерства образования и науки Российской Федерации от 17 мая 2012г., №413 / Министерство образования и науки Российской Федерации. – Москва: 2012г. – URL: http://school20.tgl.ru/sp/pic/File/2014/iyun/prikaz_MON_Ob_utverjdenii_federalnogo_gosudarstvennogo_obrazovatelnogo_standarta_srednego_polnogo_obshego_obrazovaniya.pdf. – (дата обращения: 08.05.2020). – Текст: электронный.

2. ГОСТ N 258 Федеральный базисный учебный план и примерные учебные планы для образовательных учреждений Российской Федерации, реализующих программы общего образования: утвержден Постановлением Правительства Российской Федерации от 09.03.2004 №258. – Москва: 2012г. – URL: http://docs.cntd.ru/document/901895864. – (дата обращения: 08.05.2020). – Текст: электронный.

3. ГОСТ N 2783 Концепция профильного обучения на старшей ступени общего образования: утверждена приказом Министерства образования Российской Федерации от 18.06.2002г., N 2783 – URL: https://usperm.ru/docs/ob-utverzhdenii-koncepcii-profilnogo-obucheniya-na-starshey-stupeni-obshchego-obrazovaniya. – (дата обращения: 09.05.2020). – Текст: электронный.

4. ГОСТ N 2/16-з. Примерная образовательная программа среднего общего образования: одобрена решением федерального учебно-методического объединения по общему образованию, протокол от 28.06.2016г, №2/16-3 / Министерство образования и науки Российской Федерации. – Москва: 2016г. – URL :https://mosmetod.ru/files/dokumenty/Primernaya-osnovnaya-obrazovatelnaya-programma-srednego-obshhego-obrazovaniya.pdf. – (дата обращения: 08.05.2020). – Текст: электронный.

5. ГОСТ N 7.60-2003. Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Издания. Основные

виды. Термины и определения [Электронный ресурс]. – Взамен ГОСТ 7.60-90; введ. 2004-07-01. – М.: Госстандарт России: Изд-во стандартов, 2003. – 42 с. – URL: http://www.consultant.ru/document/cons_doc_LAW_135715/

6. ГОСТ Р 52653-2006. Информационно-коммуникационные технологии в образовании. Термины и определения [Электронный ресурс]. – Введ. 2008-07-01. – М.: Госстандарт России: Изд-во стандартов, 2006. – 12 с. – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9057#07652045227597943

7. Примерная образовательная программа среднего общего образования [Электронный ресурс]: одобрена решением федерального учебно-методического объединения по общему образованию, протокол от 28.06.2016г. , №2 /16-3 / Министерство образования и науки Российской Федерации. – Москва: 2016г. – URL: http://www.consultant.ru/document/cons_doc_LAW_161101/

8. Федеральный базисный учебный план и примерные учебные планы для образовательных учреждений Российской Федерации, реализующих программы общего образования [Электронный ресурс]: - утвержден Постановлением Правительства Российской Федерации от 09.03.2004 N 258. – Москва: 2012 г. – URL: http://www.consultant.ru/document/cons_doc_LAW_47213/

9. Федеральный Государственный образовательный стандарт среднего общего образования [Электронный ресурс]: - утвержден приказом Министерства образования и науки Российской Федерации от 17.05.2012 №413 / Министерство образования и науки Российской Федерации. – Москва: 2012 г. – URL: http://www.consultant.ru/document/cons_doc_LAW_131131/

10. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с

11. Баранова, Е. К. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В. - 3-е изд. - Москва : ИЦ РИОР,

НИЦ ИНФРА-М, 2016. - 322 с. (Высшее образование) ISBN 978-5-369-01450-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/495249

12. Гафурова, Н.В. Методика обучения информационным технологиям. Теоретические основы [Электронный ресурс]: учебное пособие / Н.В. Гафурова, Е.Ю. Чурилова. – Красноярск : Сибирский федеральный университет, 2012. – 111 с. URL : http://biblioclub.ru/index.php?page=book &id=229302

13. Гейн, А.Г. Информатика и ИКТ. 11 класс [Электронный ресурс] : учеб. Для общеобразват. Учреждений: базовый и профил. Уровни / А.Г. Гейн, А.И. Сенокосов. – 2-е изд. – М. : Просвещение, 2009. – 336с. : ил. – URL : https://yadi.sk/d/qDBsp5TXC5y8Z

14. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.

15. Днепровская, Н.В. Открытые образовательные ресурсы [Электронный ресурс] / Н.В. Днепровская, Н.В. Комлева. – 2-е изд., испр. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 140 с. – URL: http://biblioclub.ru/index.php?page=book&id=428994

16. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИДАНА, 2016. – 239 с.

17. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.

18. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 с.

19. Кузнецов, А.С. Общая методика обучения информатике: учебное пособие / А.С. Кузнецов, Т.Б. Захарова, А.С. Захаров. – Москва: Прометей, 2016. – 300 с. – URL: http://biblioclub.ru/index.php?page=book&id=438600. – (дата обращения: 16.05.2020). – Текст: электронный.

20. Киселев, Г.М. Информационные технологии в педагогическом образовании: учебник [Электронный ресурс]/ Г.М. Киселев, Р.В. Бочкова. – 2-е изд., перераб. И доп. – М.: Дашков и Ко, 2014. – 304 с.: ил. – (Учебные издания для бакалавров). – URL:http://biblioclub.ru/index.php?page=book&id=253883

21. Кнут, Д. Алгоритмическое мышление и математическое мышление [Электронный ресурс] : сайт. – URL : https://www.kph.npu.edu.ua/!e-book/clasik/data/math/knut.html

22. Красильникова, В.А. Использование информационных и коммуникационных технологий в образовании [Электронный ресурс]: учебное пособие / В.А. Красильникова. – М.: ДиректМедиа, 2013. – 292 с. – URL: http://biblioclub.ru/index.php?page=book&id=209293

23. Лапчик, М. П. Методика преподавания информатики: учебное пособие для студ. пед. вузов / М. П. Лапчик, И. Г. Семакин, Е. К. Хеннер; под общей ред. М. П. Лапчика. — Москва: Издательский центр «Академия», 2001. — 624 с. – URL: http://zojkin.moy.su/nauka/metodika_prepodavanija_informatiki_lapchik-semakin.pdf. – (дата обращения: 15.06.2020). – Текст: электронный.Леонтьев, А. Н. Деятельность. Сознание. Личность [Электронный ресурс] / А.Н. Леонтьев. - 2-е изд. - Москва : Политиздат, 1977. - 304 с. – URL: https://www.marxists.org/russkij/leontiev/1975/dyeatyelnost/deyatyelnost-soznyanie-lichnost.pdf

24. Леонтьев, А. Н. Деятельность. Сознание. Личность [Электронный ресурс] / А.Н. Леонтьев. - 2-е изд. - Москва : Политиздат, 1977. - 304 с. – URL: https://www.marxists.org/russkij/leontiev/1975/dyeatyelnost/deyatyelnost-soznyanie-lichnost.pdf (дата обращения: 19.05.2020). – Текст: электронный.

25. Лобачев, С. Л. Основы разработки электронных образовательных ресурсов [Электронный ресурс]: учебный курс / С. Лобачев. – 2-е изд., исправ. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 189 с. – URL: http://biblioclub.ru/index.php?page=book&id=429160 (дата обращения: 20.05.2020). – Текст: электронный.

26. Макарова, Н. В. Методическая поддержка деятельности учителя информатики в условиях многоцелевой образовательной среды / Н.В. Макарова, Ю.Ф. Титова / Известия РГПУ им. А.И. Герцена. – 2019. – № 194. – с. 143 – 155. – URL: https://drive.google.com/file/d/0B6696ckkWj_zZEtKMjJwYkN6aFk/view. – (дата обращения: 20.05.2020). – Текст: электронный.

27. Малев, В.В. Общая методика преподавания информатики: учебное пособие / В.В. Малев. – Воронеж: Воронежский государственный педагогический институт, 2005 – 273 с. — URL: http://biblioclub.ru/index.php?page=book&id=103305. – (дата обращения: 23.05.2020). – Текст: электронный.

28. Малев, В.В. Практикум по методике преподавания информатики [Электронный ресурс]: практикум / В.В. Малев, А.А. Малева. – Воронеж: ВГПУ, 2006. – 146 с. – URL: http://biblioclub.ru/index.php?page=book&id=103304

29. Машбиц, Е. И. Психолого-педагогические проблемы компьютеризации обучения [Электронный ресурс] : (Педагогическая наука — реформе школы).— М.: Педагогика, 1988. — 192 с. – URL: http://pedlib.ru/Books/6/0442/index.shtml Национальный Открытый Университет «ИНТУИТ», 2016. – 286 с. – URL: http://biblioclub.ru/index.php?page=book&id=429034

30. Мещерякова, И.Н. Возможности электронного обучения в развитии познавательной активности студентов [Электронный ресурс]: учебно-методическое пособие / И.Н. Мещерякова. – М.: Флинта, 2014. – 63 с. – URL: http://biblioclub.ru/index.php?page=book&id=279813

31. Минькович, Т.В. Модель методических систем обучения информатике [Электронный ресурс] / Т.В. Минькович. – М.: Логос, 2011. – 307 с.: - URL: http://biblioclub.ru/index.php?page=book&id=119451

32. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.

33. Новак, Н. М. Элективные курсы как компонент профильного обучения в старшей школе: учебно-методическое пособие для студентов физико-математических факультетов педагогических вузов и учителей математики / Н.М. Новак; Мин-во образования и науки Рос. Федерации, ФГБОУ ВПО «Оренб. гос. пед. ун-т». — Оренбург: Изд-во ОГПУ, 2014. — 407 с.

34. Околелов, О.П. Справочник по инновационным теориям и методам обучения, воспитания и развития личности: настольная книга педагога [Электронный ресурс]: справочник / О.П. Околелов. – М.; Берлин: Директ-Медиа, 2015. – 272 с.-URL:http://biblioclub.ru/index.php?page=book&id=278853

35. Осин А. В. ЭОР нового поколения: открытые образовательные модульные мультимедиа системы. [Электронный ресурс] : сайт. - URL:https://studfiles.net/preview/5877379/

36. Пиаже, Ж. В. Ф. Психология интеллекта [Электронный ресурс] : монография / Ж. В. Ф. Пиаже. – Москва : Директ-Медиа, 2008. – 351 с. – URL: http://biblioclub.ru/index.php?page=book&id=39214

37. Полат, Е. С. Новые педагогические и информационные технологии в системе образования: Учебное пособие для студ. пед. вузов и системы повыш. квалиф. пед. кадров [Электронный ресурс] : учебное пособие / Е. С. Полат, М. Ю. Бухаркина, М. В. Моисеева, А. Е. Петров; Под ред. Е. С. Полат. — М.: Издательский центр «Академия», 2002. — 272 с. – URL : https://www.studmed.ru/view/polat-es-novye-pedagogicheskie-i-informacionnye-tehnologii-v-sisteme-obrazovaniya_2acf2a8d0c8.html

38. Полежаева, О. А. Информатика. УМК для старшей школы [Электронный ресурс] : 10-11 классы. Углубленный уровень. Методическое пособие для учителя / О. А. Полежаева, М. С. Цветкова. – М. : БИНОМ. Лаборатория знаний, 2013. -114 с. – URL : http://files.lbz.ru/pdf/mpSemakin10-11uufgos.pdf

39. Поляков, К.Ю. Информатика. Углубленный уровень: учебник для 11 класса : в 2 ч. Ч. 2 / К.Ю, Поляков, Е.А. Еремин. – Москва: БИНОМ, 2013. – 240 с. - URL: https://drive.google.com/file/d/0B6696ckkWj_zeU0tR0RmX1gyNG8/view - (дата обращения 9.05.2020). – Текст: электронный.

40. Потапенко, С.М. Задачи регионального содержания как фактор активизации познавательной деятельности на уроках информатики [Электронный ресурс]: монография / С.М. Потапенко; Министерство образования и науки Российской Федерации, Северный (Арктический) федеральный университет имени М.В. Ломоносова. – Архангельск: САФУ, 2013. – 103 с. – URL: http://biblioclub.ru/index.php?page=book&id=436191

41. Роберт, И. В. Теория и методика информатизации образования: психолого-педагогический и технологический аспекты [Электронный ресурс] : [монография] / И. В. Роберт .— эл. изд. — М. : БИНОМ. Лаборатория знаний., 2014. — 400 с. – URL : https://studref.com/501151/pedagogika/teoriya_i_metodika_informatizatsii_obrazovaniya_psihologo-pedagogicheskiy_i_tehnologicheskiy_aspekty

42. Рогожин, М.Ю. Подготовка и защита письменных работ [Электронный ресурс]: учебно-практическое пособие / М.Ю. Рогожин. – М. ; Берлин : Директ-Медиа, 2014. – 238 с. – URL: http://biblioclub.ru/index.php?page=book&id=253712

43. Рубинштейн, С.Л. О мышлении и путях его исследования [Электронный ресурс] : монография / С.Л. Рубинштейн. – Москва : Издательство Академии Наук СССР, 1958 – 151 с. – URL: http://biblioclub.ru/index.php?page=book&id=476734

44. Саймон Сингх Книга шифров: тайная история шифров и их расшифровки [Электронный ресурс] : / Саймон Синггх; пер. с англ. А. Галыгина. - М.: АСТ: Астрель, 2009. - 447, [1] с.: ил. - URL: http://www.vixri.com/d/Singx%20Sajmon%20_Kniga%20shifrov.pdf

45. Семакин, И. Г. Информатика. Углубленный уровень [Электронный ресурс] : учебник для 11 класса : в 2 ч. Ч. 1 / И. Г. Семакин, Е. К. Хеннер, Л. В. Шестакова. – М. : БИНОМ. Лаборатория знаний, 2014. – 176 с. – URL: https://vk.com/doc67715714_489017864?hash=8a70655fb95c2cc46a&dl=fa5ee96d06b4fe539a

46. Стрельцов, А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. [Электронный ресурс] : Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В. А. Садовничего и В. П.Шерстюка. — М., МЦНМО, 2002. — 296 с. – URL: http://labs.rulezz.ru/files/241/str.pdf

47. Тимофеева Н.М. Цифровая грамотность как компонент жизненных навыков // Психология, социология и педагогика. 2015. № 7 [Электронный ресурс]. - URL: http://psychology.snauka.ru/2015/07/5573 (дата обращения: 07.02.2019)

48. Трайнев, В.А. Электронно-образовательные ресурсы в развитии информационного общества: обобщение и практика [Электронный ресурс]: монография / В.А. Трайнев. – М.: Дашков и Ко, 2015. – 256 с.- URL: http://biblioclub.ru/index.php?page=book&id=253962

49. Угринович, Н. Д. Информатика. 7 класс. Базовый уровень [Электронный ресурс] : учебник / Н. Д. Угринович. — М. : БИНОМ. Лаборатория знаний, 2017. — 288 с. – URL: http://old.school259.spb.ru/DswMedia/informatika_uchebnik11kl_ugrinovich.pdf

50. Угринович, Н. Д. Информатика. 8 класс. Базовый уровень [Электронный ресурс] : учебник / Н. Д. Угринович. — М. : БИНОМ. Лаборатория знаний,

2017. — 288 с. – URL: http://old.school259.spb.ru/DswMedia/informatika_uchebnik11kl_ugrinovich.pdf

51. Цветкова, М. С. Информационная безопасность. Безопасное поведение в сети Интернет. 5–6 классы : учебное пособие / М. С. Цветкова, Е. В. Якушина. — 2-еизд., пересмотр. — М.: БИНОМ. Лабораториязнаний, 2020. Текст : электронный. - URL: http://www.lbz.ru/books/1105/11205/)

52. Цветкова, М. С. Информационная безопасность. 7-9 классы : учебное пособие / М. С. Цветкова, И. Ю. Хлобыстова.— 2-е изд., пересмотр.—М.: БИНОМ. Лаборатория знаний, 2020. — 64 с. : ил. ISBN 978-5-9963-5897-7.

ЭЛЕКТРОННЫЕ РЕСУРСЫ

1. GeekBrains – образовательный портал // Mail.ru: сайт. – URL: https://geekbrains.ru/. – (дата обращения: 21.05.2020). – Текст: электронный
2. Quizizz - [Электронный ресурс]. — URL: https://quizizz.com/admin/quiz/5deddb5cb6eb58001cbfe6d3/qr-коды – (дата обращения: 21.05.2020). – Текст: электронный.
3. LearningApps.org – создание мультимедийных интерактивных упражнений // MoodleCloud: сайт. – URL: https://learningapps.org/. – (дата обращения: 21.05.2020). – Текст: электронный.
4. Skillbox – онлайн-университет [Электронный ресурс] : сайт. – URL : https://skillbox.ru/– (дата обращения: 21.05.2020). – Текст: электронный.
5. YouTube [Электронный ресурс] : сайт. – URL : https://www.youtube.com/
6. Всероссийский урок безопасности в сети Интернет [Электронный ресурс]. — Режим доступа: https://safetylesson.rosuchebnik.ru/
7. Евгений Касперский. Лаборатория Касперского. Активируй будущее [Электронный ресурс]. — Режим доступа: https://www.youtube.com/user/KasperskyChannelRU
8. Дети в информационном обществе [Электронный ресурс] : сайт. – URL : // http://detionline.com/journal/about – (дата обращения: 21.05.2020). – Текст: электронный.

9. Лига безопасного Интернета [Электронный ресурс] : сайт. – URL : http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=3652 – (дата обращения: 30.05.2020). – Текст: электронный.
10. Онлайн-курсы Udemy [Электронный ресурс] : сайт. – URL : https://www.udemy.com/ru/
11. Час кода: сайт. – URL: https://codewards.ru/hourofcode. – (дата обращения: 30.05.2020). – Текст: электронный.
12. Google Класс: сайт. - URL: https://classroom.google.com/ – (дата обращения: 23.04.05.2020). – Текст: электронный.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А

Входной тест из состава учебно-методического комплекса (УМК) «Информационная безопасность, или На расстоянии одного вируса. 7-9 классы» Наместниковой М.С.

1. Установите соответствие между названиями функций браузера и их описаниями:
   1) История посещения страниц.
   2) Защита от фишинга и вредоносного программного обеспечения.
   3) Автозаполнение
   4) Управления информацией о местоположении
   5) Сохранение паролей
   6) Управление всплывающими окнами

   A. Упрощает доступ к регулярно посещаемым сайтам за счет автоматического ввода.

   B. Автоматическая блокировка всплывающих окон, чтобы они не загромождали экран

   C. Использование данных о вашем местоположении для вывода ближайших к вам запрашиваемых мест.

   D. Доступ к регулярно посещаемым сайтам за счет автоматического заполнения учётных данных.

   E. Запрос на подтверждение операции при загрузке файла

   F. Возврат на посещённую страницу или восстановление события.

2. Выберите правильный ответ.

   Социальная сеть — это:

   A. Онлайн-сервис, предоставленный провайдером.

   B. Веб-сайт.

   C. Программное обеспечение, позволяющее переписываться.

   D. Онлайн-сервис в Интернете для общения и связи.

3. Что такое аккаунт социальной сети?

   A. Веб-страница в Интернете.

   B. Учётная запись пользователя в каком-либо сервисе.

   C. Логин и пароль для входа в социальной сети.

4. Выберите информацию, которую безопасно размещать на своей странице в Интернете для незнакомых людей.
    A. Домашний адрес.
    B. Номер школы, в которой учитесь.
    C. Паспортные данные или фотографию паспорта.
    D. Геолокацию устройства, с которого осуществляется ввод.
    E. Секцию, в которую ходите.
    F. Любимые места в городе.
    G. Фотографии родителей, находящихся на отдыхе.
    H. Ваше хобби.
    I. Любимые книги.
5. Какие настройки приватности в социальных сетях следует установить, чтобы обезопасить себя от мошенников?
    A. Приватность аудиозаписей.
    B. Приватность фотографий.
    C. Приватность списка друзей.
    D. Приватность подарков.
    E. Приватность персональных данных.
    F. Приватность местоположения.
6. Отметьте простые(слабые) пароли для использования в учётной записи:
    A. 654321ToPas&.
    B. yetrewq.
    C. Asdf123#Mnb.
    D. drowssap.
    E. Mypassword.
    F. Ivan1968.
7. Отметьте процесс, который носит название *кибербуллинг*.
    A. Онлайн-спор, в который вовлечены определённое сообщество или группа в Интернете.
    B. Травля, оскорбления и угрозы в условиях интернет-коммуникации.

C. Написание обидных комментариев к фотографиям, обвинение в непрофессионализме.

8. Какие данные хотят узнать фишеры(мошенники)?

A. Паспортные данные.

B. Номер школы.

C. Телефон.

D. Номер школьной карты.

E. Проверочный код от карты.

F. Пароль от учётной записи в социальной сети.

G. Пароль от онлайн-банкинга.

H. Номер банковской карты.

I. Логин и пароль от входа в дневник.

J. Логин и пароль от почты.

9. Какие программы(коды) можно назвать вредоносными?

A. Программы, ворующие регистрационные данные.

B. Программы, использующие ресурсы других компьютеров.

C. Программы, дающие несанкционированный доступ к ключевым файлам различных программных продуктов.

D. Программы, предлогающие посетить платные веб-ресурсы.

E. Программы, принудительно демонстрирующие рекламную информацию.

F. Программы, исправляющие ошибки и недоработки в новых версиях приложений.

G. Программы, шифрующие персональные файлы пользователей.

10. Проанализируйте и отметьте истинные(верные) высказывания.

A. Трояны распространяются самостоятельно, а вирусы распространяют люди.

B. Трояны распространият люди, п вирусы распространяются самостоятельно.

C. Трояны, распространяются так же, как и вирусы.

D. Черви распространяются так же, как и вирусы.

E. Червы распространяют люди.

11. Как распространяются вредоносные программы?

A. С помощью вложенных в письма файлов.
B. Ппри скачивании приложений.
C. При авторизации в социальных сетях.
D. При посещений популярных сайтов.
E. С помощью файлообменных сетей и торрентов.
F. С помощью методов социальной инженерии.
G. При переходе по ссылке для подтверждения регистрации.
H. При использовании зараженной интернет-страницы.
I. Компаниями, которые создают и продают защиту от вредоносных программ.
J. Передаются телефонным провайдером.

12. Выделите действия, которые связанны с целью установления обновлений и являются обязательными для защиты от проникновения вредоносных программ:

A. Обновлять операционную систему для устранения в новых версиях ошибок и уязвимостей.
B. Не обновлять операционную систему, потому что обновления тоже могут содержать ошибки, которые представляют опасность.
C. Не обновлять лицензионную операционную систему, потому что она достаточно безопасная.
D. Обновлять браузер, потому что в новых версиях исправляют уязвимости и недостатки предыдущих версий.
E. Не обновлять браузер, игнорировать информацию о необходимости обновления потому, что она бессмысленна.
F. Не обновлять браузер потому, что при обновлении могут быть занесены вредоносные программы.
G. Обновлять антивирусное программное обеспечение для детектирования и блокирования вновь появившихся вредоносных программ.
H. Не обновлять антивирусные программные обеспечения, потому что оно лишь добавит новые функции и изменит интерфейс и будет платным.
I. Не обновлять антивирусное программное обеспечение до истечения платной лицензии.

13. При работе с поисковыми браузерами вы находите известный вам сайт, но появляется предупреждение об опасности. Ваши действия.

A. Не буду заходить на сайт, даже проверенный сайт может быть заражён.
B. Не буду обращать внимания на предупреждение, потому что уже заходил на этот сайт неоднократно, и перейду на сайт.

C. По ищу информацию о заражении этого сайта, и если не найду, то перейду на сайт.

14. Выберите самое точное определение человека не застрахованного от проникновения разного рода вредоносных программ на устройства, которыми он пользуется.

A. Внимательный аккуратный человек.
B. Невнимательный и неаккуратный человек.
C. Человек, следящий за обновлениями браузера, операционной системы и антивирусного обеспечения.
D. Человек, не следящий за обновлениями браузера, операционной системы и антивирусного обеспечения.
E. Не разбирающийся в устройствах и программах человек.
F. Разбирающийся в устройствах и программах человек.
G. Любой человек.

15. На какие параметры антивирусных программ следует обращать внимание при покупке?

A. Разнообразие функций.
B. Уровень детектирования.
C. Бесплатность.
D. Платность.
E. Влияние на скорость работы компьютера.
F. Уровень ложных срабатываний.
G. Доставка обновлений.
H. Наличие лицензии.
I. Продление лицензии

16. Отметьте виды программы которые всегда вредоносны.

A. Вирусы.
B. Черви.
C. Трояны.
D. Скрипты.
E. Макросы.
F. Архиваторы
G. Бэкдоры.
H. Буткиты.
I. Утилиты.

17. Отметьте, что необходимо использовать на компьютере, чтобы предотвратить заражение вирусами.

A. Регулярное обновление браузера.
B. Регулярное обновление операционной системы.
C. Регуляторное обновление антивирусной базы.
D. Проверку адресов сайтов.
E. Отказ от перехода по ссылкам из всплывающих окон.
F. Использование диспетчера задач для закрытия браузера в случае заражения.

G. Загрузку программного обеспечения только с официальных сайтов разработчиков.

H. Выбор зарекомендовавших себя антивирусных программ.

I. Установку только лицензионных версий программного обеспечения.

J. Установку проактивного и поведенческого анализа в антивирусной базе.

K. Проверку почтовых сообщений и их вложений.

L. Полное сканирование компьютера и подключаемых устройств не реже одного раза в неделю.

M. Установку на компьютер сразу нескольких средств защиты.

18. Подберите синонимичныеприлагательные на русском языке и объясните следующие понятия:

1) Фейковые новости.
2) Фейковая программа.
3) Фейковый номер телефона.
4) Фейковый аккаунт.
5) Фейковая страница в социальной сети.
6) Фейковая кредитная карта.
7) Фейковый профиль.
8) Фейковый контроль.

A. Фальшивые новости, ложно смонтированное видео

B. Приложение, которое имеет дизайн и функционал, напоминающий переделываемую программу.

C. Виртуальный номер телефона.

D. Любой аккаунт с недостоверной информацией - имя, контакты, фотографии.

E. Фиктивная страница в интернет ресурсах.

F. Банковская карта, оформленная на человека, который в рельности не существует.

G. Профиль, содержащий ложную информацию о владельце либо не содержащий её вовсе.

H. Фальсифицированный сайт, копия главной страницы которого напоминает известный.

19. Выберите правильный ответ.

Социальная инженерия - это.

A. Привлечение пользователей к действиям, способствующим заражению вредоносными программами.

B. Метод управления действиями яеловека без использования технических средств.

C. Технология внедрения вредоносных программ, использующая управление действиями пользователя.

20. Отметье места, в которых можно безопасно подключиться к общественной сети Wi-Fi.

A. Кафе.
B. Школа.
C. Общественный транспорт.
D. Такси.
E. Ресторан.
F. Торговый центр.
G. Поликлиника.
H. Вуз.

21. Какое шифрование сети, предназначенное для её защиты, легко взломать?
A. WPA.
B. WPA2.
C. WEP.

22. Каковы дополнительные признаки безопасности публичной Wi-Fi сети?
A. Рядом со значком Wi-Fi находится замочек.
B. Для входа в сеть требуетсяавторизация.
C. Для входа в сеть необходимо ввести пароль.
D. Название сети совпадает с названием учреждения или места расположения.

23. Какие меры безопасности необходимы для проведения онлайн-платежей?
A. Операционная система обновлена.
B. Версия браузера обновлена.
C. Двухфакторная онлайн-транзакция.
D. Компьютер друзей.
E. Свой компьютер.
F. Антивирус, установленный на устройстве, с которого производится транзакция.
G. Правильный адрес в адресной строке.
H. Банковское приложение, скачанное с официального сайта банка.
I. Банковское приложение, скачанное из магазина приложений.
J. Ссылка на страницу из электронного письма или другого источника онлайн-банкинг.

ПРИЛОЖЕНИЕ Б

Конспект урока «Что такое вредоносный код?»

Тип урока: Открытие новых знаний

Цель урока: познакомить учащихся с понятием вредоносного кода, видами вредоносного кода, признаками вредоносного кода.

Задачи урока:

1. Образовательная: знакомство учащихся с понятием вредоносного кода, их видами и признаками.
2. Воспитательная: воспитание информационной культуры учащихся, внимательности, усидчивости, дисциплинированности.

3. Развивающая: развитие познавательных интересов.

Планируемые образовательные результаты:

Предметные:

1) знакомство с понятием вредоносного кода;

2) формирование навыков распознания вредоносного кода;

3) приобретение навыков отличия разных видов вредоносного кода.

Метапредметные:

1) умение соотносить свои действия с планируемыми результатами;

2) осуществлять контроль своей деятельности в процессе достижения результата;

3) определять способы действий в рамках предложенных условий и требований;

4) корректировать свои действия в соответствии с изменяющейся ситуацией.

Личностные:

1) формирование интереса к изучению информатики через творческие задания;

2) стремление использовать полученные знания в процессе обучения другим предметам и в жизни;

3) осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов.

Оборудование: ПК, интерактивная доска, проектор, рабочие тетради.

План урока:

1. Организационный момент

2. Постановка целей и задач

3. Изучение нового материала

4. Самостоятельная работа учеников

5. Подведение итогов

Содержание теоретической и практической частей урока:

Все люди подвержены различным воздействиям окружающей среды, заболеваниям, которые возникают из-за вирусов и бактерий.

Вирусы - это мельчайшие микроорганизмы, которые увидеть без специальных увеличительных средств невозможно. Они проникают в организм человека из внешней среды, вследствие этого человек начинает болеть. Подобно людям, компьютер подвержен своего рода заболеваниям - вредоносному коду. Сходство вируса человека и компьютера мы видим с вам на рисунке Б1.

Рисунок Б1. Сходство вирусов

Действительно, довольно часто дети изображают компьютерный вирус, как фантастическое и не дружелюбное существо зелёного

цвета. На самом деле, компьютерный вирус - это всего лишь компьютерная программа, которая является разновидностью большой группы вредоносных программ, или, как ещё говорят, вредоносных кодов. У вредоносных кодов есть общий признак - они способны совершать на компьютерах пользователей разные несанкционированные и при этом вредоносные(«деструктивные») действия.

В «Лаборатории Касперского» принято разделять вредоносные коды на следующие виды:

1. Вирус - Это код, который копирует сам себя и внедряется в установленные программы без согласия пользователя. При этом вирус может выполнять множество разных задач, направленных на нанесение вреда операционной системе.
2. Червь. Черви созданы на основе саморазмножающихся программ. Однако они не могут заражать существующие файлы. Червь «поселяется» в компьютере и ищет способы дальнейшего распространения себя.
3. Троян - по своему действия является противоположностью вирусам и червям; трояны не самовоспроизводятся и не распространяются сами по себе; самые известные трояны – шифровальщики блокировщики (блокеры).
4. Загрузчик - небольшая часть кода, используемая для дальнейшей загрузки и установки полной версии вредоносной программы.

Это лишь часть классификации вредоносных кодов. Существуют и другие виды вредоносных программ, например, Бэкдор и Руткиты.

Бэкдор, тайный вход — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом.

Руткит - под этим термином понимается набор утилит или специальный модуль ядра , которые злоумышленник устанавливает на взломанной им компьютерной системе сразу после получения прав суперпользователя. Этот набор, как правило, включает в себя разнообразные

утилиты для «заметания следов» вторжения в систему, делает незаметными снифферы , сканеры, кейлоггеры , троянские программы , замещающие основные утилиты UNIX (в случае не ядерного руткита). Rootkit позволяет взломщику закрепиться во взломанной системе и скрыть следы своей деятельности путём скрытия файлов, процессов, а также самого присутствия руткита в системе.

Первая «эпидемия» компьютерного вируса произошла в 1986 году.

Рассмотрим 4 самых страшных вируса в истории:

1. Brain (1986 год).

По праву является родоначальником всех компьютерных вирусов, но для этих целей он вовсе и не задумывался. Был разработан братьями-программистами Амджатом и Базитом Алви из Пакистана. Brain создавался как оружие против местных пиратов, ворующих созданное братьями ПО, однако всё пошло не по плану (прям фильм можно снимать). Только в США было заражено порядка 18 тыс. компьютеров. Вирус распространялся, записывая свое тело в загрузочные сектора дискет. Если их пытались сканировать, он подставлял вместо зараженного сектора его специально созданную нейтральную копию. Сегодня подобные программы, пытающиеся скрыть свое присутствие в системе, именуют стелс-вирусами и они считаются опаснее прочих.

2. Jerusalem (1988 год)

Разработан в Израиле и запущен 13 мая 1988 года, вирус Jerusalem распространился на Ближнем Востоке, в Европе и США среди огромного числа пользователей. Антивирусы тогда ещё не были так распространены и пользователи как с ним бороться. Вреда Jerusalem приносил много, например, при попытке запуска зараженного файла он сразу удалял его. А если приход пятницы совпадал с наступлением 13-го числа, что случается не так уж редко, то вирус форматировал жёсткий диск, стирая все данные без разбора. Был написан Робертом Моррисом и запущен 2 ноября 1988 года. Стоит отметить, что в 1988 году размеры сети Интернет были куда как меньше

современных. И поэтому быстро и бесконтрольно размножающемуся червю Морриса не составило особого труда за короткий срок захватить его целиком. Вирус доводил компьютер до состояния отказа, постоянно копируя себя. Ноябрь 1988 года запомнился как месяц, когда один вирус парализовал работу всего Интернета, что обернулось прямыми и косвенными убытками на общую сумму около 100 млн. долл.

3. Michelangelo (1992 год)

Изначально вирус был абсолютно безобиден. Он проникал через дискеты в загрузочные сектора ПК, где он и находился, бездействуя. Однако 6 марта (день рождения Микеланджело), вирус запустился и стирал все данные на компьютере. В реальности количество зараженных систем не превысило 10 тыс., но пользователи уже вкусили удел потери данных и начали активно обращаться к разработчикам антивирусного ПО. Именно этот вирус дал неплохой задел для развития антивирусов во всём мире.

4. Win95.CIH (1998 год)

Разработан неким тайванским студентом, CIH (его инициалы). Для проникновения на компьютеры использовал все способы, включая распространение по электронной почте, на внешних носителях, просто через Интернет. При этом довольно умело прятался среди файлов других программ и никак себя не проявлял. Активизировался 26 апреля (дата аварии на ЧАЭС). Проснувшийся CIH не просто форматировал данные, но и стирал содержимое BIOS, нанося уже физический вред – после этого компьютер просто не включался.

Достоверно известно о 300 тыс. зараженных компьютеров, преимущественно в странах Восточной Азии. По некоторым оценкам, за всё время его существования он успел проникнуть на более чем полумиллиона систем во всем мире.

Самостоятельная работа:

Ребята, сейчас мы с вами проверим всё ли мы знаем о вредоносном коде. Сейчас вам нужно перейти на сайт по ссылке, которую вы видите на экране

(https://quizizz.com/admin/quiz/5dedb646d92d7c001d8a206b/что-такое-вредоносный-код?studentShare=true), ввести код игры и пройти тест. Результаты мы увидим в турнирной таблице(Рис. В1).

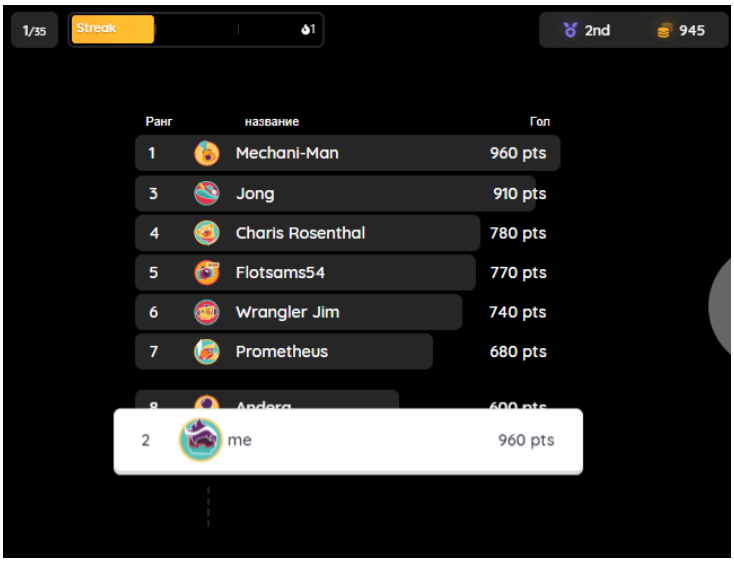


Рисунок В1. Пример турнирной таблицы.

Подведение итогов:

Сегодня ученики узнали что такое вредоносный код, его схожие черты с вирусом человека, узнали новое понятия руткит и бэкдор, а также узнали топ 4 самых страшных компьютерных вирусов человечества.

ПРИЛОЖЕНИЕ В

Конспект урока «Методы защиты от вредоносных программ: Антивирус»

Тип урока: Открытие новых знаний

Цель урока: познакомить учащихся с понятием антивирусной программы, их основными характеристиками, признаками заражения компьютера, а также познакомиться с видами антивирусов.

Задачи урока:

3. Образовательная: знакомство учащихся с понятием антивирусной программы, их основными характеристиками и т.д.
4. Воспитательная: воспитание информационной культуры учащихся, внимательности, усидчивости, дисциплинированности.

3. Развивающая: развитие познавательных интересов.

Планируемые образовательные результаты:

Предметные:

1) знакомство с понятием антивирусной программы;

2) формирование навыков распознания признаков заражения компьютера;

3) приобретение навыков работы с антивирусными программами.

Метапредметные:

1) умение соотносить свои действия с планируемыми результатами;

2) осуществлять контроль своей деятельности в процессе достижения результата;

3) определять способы действий в рамках предложенных условий и требований;

4) корректировать свои действия в соответствии с изменяющейся ситуацией.

Личностные:

1) формирование интереса к изучению информатики через творческие задания;

2) стремление использовать полученные знания в процессе обучения другим предметам и в жизни;

3) осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов.

Оборудование: ПК, интерактивная доска, проектор, рабочие тетради.

План урока:

1. Организационный момент

2. Постановка целей и задач

3. Изучение нового материала

4. Самостоятельная работа учеников

5. Подведение итогов

Содержание теоретической и практической частей урока:

В настоящее время, технически вредоносный код может совершать всё тоже самое, что и стандартное программное обеспечение на ваших устройствах:

- видеть и сохранять пароли от различных сервисов;
- получать доступ к файлам на вашем устройстве;
- получать доступ к различным данным, сервисы и функционалу устройства, например к веб-камере и микрофону.

Для того чтобы избежать заражения вирусом, нам необходима антивирусная программа.

Антивирусная программа (антивирус) – это программное обеспечение, защищающее устройство от действий и проникновения вредоносного кода.

Основные характеристики антивирусных программ:

- платность и бесплатность;
- уровень детектирования;
- уровень ложных срабатываний;
- разнообразие функций;
- влияние на скорость работы компьютера.

Как же распознать, что наш компьютер заражен? Для этого мы должны помнить признаки заражения компьютера.

Признаки заражения компьютера:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- частые зависания и сбои в работе компьютера;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов.

Теперь мы с вами знаем признаки заражения компьютера, но какие тогда существуют виды антивирусных программ, раз вирусов так много?

Виды антивирусных программ: Avast!, Антивирус Касперского, Agnitum, Dr.Web, Bitdefender, ESET NOD32 и т.д. На самом деле их очень много и все они разные.

Самостоятельная работа:

1. Ребята, для вас следующее задание! Вам нужно найти ответы на эти вопросы:
2. Когда появились антивирусные программы?
3. Как они называли?
4. Чем отличается антивирус, появившийся в 1985 году, от предыдущих антивирусных программ?
5. Для чего нужны и как работают следующие защитные программы: Антиспам; Антифишинг; Антибаннер; Веб-фильтр?

Сейчас вы можете просмотреть видео-ролик «Приключения робота Каспера-Опасности на надёжных сайтах». А после этого, вам необходимо пройти игровой тест на Quizizz, с результатами которого мы ознакомимся после в турнирной таблице.

Подведение итогов:

Сегодня мы узнали что такое антивирусная программа, какие виды антивирусных программ бывают, познакомились с признаками заражения копьютера и узнали, какие опасности на сайтах нас ожидают.