МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ФИЗИКО-МАТЕМАТИЧЕКИЙ ФАКУЛЬТЕТ

КАФЕДРА ИНФОРМАТИКИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ИНФОРМАТИКЕ

Разработка дидактического обеспечения изучения темы «Информационная безопасность» в школе

Выпускная квалификационная работа
по направлению 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность программы бакалавриата

«Информатика. Английский язык»

Выполнил:
Студент группы ОФ-513/093-5-1
Губанов Евгений Александрович

Научный руководитель:
К.п.н., доцент кафедры ИИТиМОИ
Паршукова Наталья Борисовна

Проверка на объем заимствований:
55,9 % авторского текста

Работа рекомендована к защите
рекомендована/не рекомендована
«20» мая 2017 г.
и.о. зав. кафедрой И, ИТ и МОИ
_____ Рузаков А.А.

Челябинск
2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ФИЗИКО-МАТЕМАТИЧЕКИЙ ФАКУЛЬТЕТ

КАФЕДРА ИНФОРМАТИКИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ИНФОРМАТИКЕ

Разработка дидактического обеспечения изучения темы «Информационная безопасность» в школе

Выпускная квалификационная работа
по направлению 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность программы бакалавриата

«Информатика. Английский язык»

Выполнил:
Студент группы ОФ-513/093-5-1
Губанов Евгений Александрович

Научный руководитель:
К.п.н., доцент кафедры ИИТиМОИ
Паршукова Наталья Борисовна

Проверка на объем заимствований:
_____% авторского текста

Работа _____ к защите
рекомендована/не рекомендована

« ___ » _____ 20__ г.
и.о. зав. кафедрой И, ИТ и МОИ

_____ Рузаков А.А.

Челябинск
2017

Содержание

Введение

Актуальность исследования основана на значительных изменениях во многих сферах жизни. Подобные изменения основаны на влиянии развития информационных технологий в современном мире. В данный момент можно наблюдать процесс перехода общества к новому состоянию, которое ученые называют информационным обществом.

В этом состоянии общества ключевую роль играет информация и информационная деятельность. Сами технологии не всегда оказывают воздействие на социальную сферу, включая образование. Изменения, которые оказываются наиболее важными для общества, обычно происходят под действием развивающихся технологий.

Образование в информационном обществе не является способом усвоения готовых знаний, образование становится способом обмена информацией между ребёнком и окружающими его людьми. Также образование в информационном обществе является способом генерирования новой информации в обмен на информацию полученную.

В связи с переходом к информационному обществу и внедрением инновационных компьютерных технологий в образовательный процесс, с изменением целей обучения, его направленности на развитие творческой активности учеников возрастает роль самостоятельной деятельности учащихся в обучении с использованием возможностей сети Интернет. Учитывая вышесказанное, нельзя рассматривать Интернет как благоприятную образовательную среду. К опасностям в информационной сфере можно отнести следующие угрозы:

- доступность, неконтролируемость, неограниченный объем поступления информации для учеников школы;
- наличие в сети Интернет специфических элементов, которые специально направлены на изменение психофизиологического состояние школьника;

- наличие в сети Интернет информации, которая имеет манипулятивный характер, дезориентирующие школьников, ограничивая их возможность в условиях слабой правовой образованности.

Таким образом, актуализация качественно новых угроз безопасности учащихся, затрагивающих сущность информационной связи общества и человека в системе образования, свидетельствует об актуальности данной работы.

Цель исследования: Определить уровень соответствия учебных комплексов школьного курса «Информационная безопасность» требованиям и разработать методику изучения курса для учеников 8-11 классов.

Объект исследования: изучение вопросов информационной безопасности в школьном курсе информатики.

Предмет исследования: методика преподавания темы информационной безопасности в курсе Информатики и ИКТ для учеников 8-11 классов.

Задачи:

1. Изучить теоретические основы по теме «Информационная безопасность»
2. Провести анализ изложения темы в учебных комплексах и учебно-методической литературе
3. Разработать уроки по теме «Информационная безопасность»
4. Разработать ЭОР в поддержку темы «Информационная безопасность»

Методы исследования: педагогический эксперимент и анализ литературных источников и методической литературы.

Гипотеза исследования состоит в том, что, если методические материалы темы «Информационная безопасность» будут своевременно дополняться актуальной информацией.

ГЛАВА 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1 Теоретические основы обучения информационной безопасности школьником в школьном курсе информатики 8-11 классов

Прежде чем говорить об информационной безопасности как о предмете в курсе «Информатика и ИКТ», необходимо определить, что такое информация и информационная безопасность.

Информация – абстрактное понятие в предмете «Информатика и ИКТ», которое рассматривается как объем данных [1].

Информационная безопасность – состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной среде [1].

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации [1].

Конфиденциальность информации – процесс обеспечения доступа к информации только авторизованным пользователям [1].

Целостность информации – обеспечение достоверности и полноты информации и методов её обработки [1].

Доступность информации – обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости [1].

Информационная безопасность состоит из нескольких аспектов:

- информационная безопасность человека заключается в невозможности нанесения ему вреда как личности, социальная деятельность которой во много базируется на осмыслении получаемой информации, информационных взаимодействиях с другими индивидами и часто имеет информацию в качестве предмета деятельности;

- информационная безопасность детей – состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;
- безопасность личности в информационной сфере обеспечивается путем создания условий для свободной реализации и защиты информационных прав граждан, обеспечения защиты личной тайны и иной принадлежащей гражданам конфиденциальной информации, защиты от правонарушений в области информационной безопасности, включая защиту от злоупотребления правами в информационной сфере;
- информационная безопасность личности – состояние и условия жизнедеятельности личности, при которых реализуются её информационные права и свободы;
- информационная безопасность общества заключается в невозможности нанесения вреда его духовной сфере, культурным ценностям, социальным регуляторам поведения людей, информационной инфраструктуре и передаваемым с ее помощью сообщениям.

Информационная безопасность личности – это: а) состояние защищенности, при котором отсутствует угроза (минимален риск) причинения вреда информации, которой владеет личность; б) состояние и условие жизнедеятельности личности, при которых отсутствует угроза (минимален риск) нанесения вреда личности информацией [2].

Понятие «Информационная безопасность» сегодня трактуется как в широком, так и в узком смысле. В широком смысле данное понятие трактуется как состояние общества, при котором обеспечена надёжная и всесторонняя защита личности, общества и государства от воздействия на них особого вида угроз, выступающих в форме организованных

информационных потоков и направленных на деформацию общественного и индивидуального сознания. В узком смысле это состояние безопасности информации и каналов передачи и приёма, а также организация защиты от применения противником информационного оружия в ходе боевых действий. Примечательно, что понятие в узком смысле трактуется с технической точки зрения, и является организационным средством обеспечения информационной безопасности в широком смысле.

Необходимо рассматривать понятие информационной безопасности как информационную безопасность личности, которая включает в себя два этапа: безопасности формирующейся личности (информационную безопасность детей и учеников школы) и безопасность сформированной личности. Возможно также расширение состава информационной безопасности за счёт межгосударственной информационной безопасности.

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

Несмотря на то, что в образовательных стандартах, как для основной, так и для старшей школы явным образом указано понятие «информационная безопасность», в школьных учебниках информатики авторы, как правило, определяют и концентрируют внимание обучающихся на термине «защита информации», который в школьном стандарте в явном виде не приводится. Этот термин упоминается только в примерной программе для основной школы применительно к средствам защиты личной информации и примерной учебной программе по предмету «Информатика и ИКТ» применительно к защите от вредоносного программного обеспечения и защите персональных данных.

Информационная безопасность личности состоит из трёх аспектов безопасности: информационно техническая безопасность, информационно – идеологическая безопасность и информационно – психологическая безопасность. Под информационно – технической информационной безопасностью личности необходимо понимать защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба личности. Под информационно – идеологической информационной безопасностью необходимо понимать защищенность личности от преднамеренного или непреднамеренного информационного воздействия. Результатом подобного воздействия может быть нарушение прав и свобод в области создания, потребления и распространения информации, пользования информационной инфраструктурой и ресурсами, противоречащих нравственно – этическим нормам, оказывающих деструктивное воздействие на личность, имеющих негласный (внечувственно – неосознанный) характер, внедряющих в общественное сознание антисоциальные установки. Под информационно – психологической информационной безопасностью следует понимать состояние защищенности отдельных лиц и (или) группы лиц от негативного информационно – психологического воздействия и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере.

Безопасность информации — состояние защищенности данных, при котором обеспечиваются их конфиденциальность, доступность и целостность. Безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе [2].

Угрозы информационной безопасности – совокупность условий, факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [2].

Атакой называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, называется злоумышленником. Потенциальные злоумышленники называются источниками угроз [2].

Угроза является следствием наличия уязвимых мест или уязвимостей в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ [2].

Угрозы можно классифицировать по нескольким критериям:

- по свойствам информации (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход. Выделяют следующие уровни защиты информации:

1) законодательный уровень – законы, нормативные акты и прочие документы РФ и международного сообщества;
2) административный уровень – комплекс мер, предпринимаемых локально руководством организации;
3) процедурный уровень – меры безопасности, реализуемые людьми;

4) программно-технический уровень – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) отношение к людям, нарушающим информационную безопасность.

Интернет – гигантская всемирная компьютерная сеть, объединяющая десятки тысяч сетей всего мира. Её назначение — обеспечить любому желающему постоянный доступ к любой информации. Интернет предлагает практически неограниченные информационные ресурсы, полезные сведения, учёбу, развлечения, возможность общения с компетентными людьми, услуги удалённого доступа, передачи файлов, электронной почты и многое другое. Интернет обеспечивает принципиально новый способ общения людей, не имеющий аналогов в мире.

Для создания ресурса, которые поможет в обучении теме «Информационная безопасность» я создал веб-ресурс, который был создан при помощи базы данных MySQL и языка программирования PHP.

База данных – это совокупность связанных между собой таблиц. Например, в одной таблице может храниться информация о пользователе, зарегистрированном на сайте, а в другой – информация о комментариях, которые оставил пользователь на сайте.

MySQL – это один из множества средств персонального обеспечения для работы с SQL базами данных [6].

SQL – это структурированный язык запросов, созданный для управления реляционными БД. Он обладает широким перечнем возможностей, например, создать таблицу, редактировать и удалять данные, производить запросы из таблиц и многое другое [6].

PHP – это широко используемый язык сценариев общего назначения с открытым исходным кодом [6].

PHP – это язык программирования, специально разработанный для написания web-приложений (сценариев), исполняющихся на Web-сервере [6].

1.2 Основные аспекты информационной безопасности в школьной программе предмета «Информатика и ИКТ» 8-11 классов

Обилие угроз в современном мире делает самой важной характеристикой качества жизни безопасность жизнедеятельности и, прежде всего, такую её составляющую, как информационная безопасность. При обучении информационной безопасности, необходимо обратить особое внимание на формирование компетентности школьников во время непрерывного обучения, которое будет соответствовать, и способствовать благоприятному прохождению этапов становления личности.

Целью обучения информационной безопасности школьников является приобретенные ими после окончания школы компетенции в области информационной безопасности, которые позволят им с успехом социализироваться в современном информационном обществе. Для этого, соответственно, нужно, чтобы у выпускников было сформировано целостное представление о предметной области обеспечения информационной безопасности. Следовательно, необходимо сформировать у выпускников целостное представление об информационной безопасности и её составляющие (информационная безопасность детей, личности, государства, общества и международная информационная безопасность). Всё это должно происходить в условиях информатизации общества, в момент, когда развитие информационных и коммуникационных технологий делает средства массовой информации главным институтом социализации, который начинает выполнять функции многих традиционных социальных институтов (школы, групп сверстников, семьи и государства).

Именно по этой причине школьники старших классов являются наиболее восприимчивыми к пропаганде в СМИ и сети Интернет. Они активно пытаются найти своё место в социуме, а СМИ предлагают свои модели развития, эталоны поведения, выступая в качестве

информационных фильтров, выделяющих и усиливающих одни контексты и приглушающих, иногда и вовсе замалчивающих другие.

Одной из составляющих школьного обучения является подготовка к важному этапу социализации выпускников средней общеобразовательной школы в информационном пространстве после школы. Это предполагает, что формирование нового мышления и понимания мира и себя в нём будет означать активное использование школьниками информационных коммуникационных технологий в процессе их возрастного развития как личности.

Однако развитие умений свободной ориентации в современной информационной среде, организации поисковой деятельности, использования различных стратегий познания увеличивает степень информационных угроз, с которыми может столкнуться школьник. Сложностью в выявлении таких угроз является то, что старшеклассники вступают во взаимодействие с информационным пространством больших масштабов, которое, к тому же, неоднородно. При этом приоритеты информационного взаимодействия учащихся старшего школьного возраста определяются динамикой их возрастного развития в процессе и в структуре их информационной и общей социализации.

Исходя из этого, необходимо не просто научить подростков уметь оценивать и объективно анализировать информацию, учитывая возможные поступающие угрозы, но сформировать у него умения, которые обеспечат его информационную безопасность как личности, интегрированной в социальную структуру, в комплексном понимании им различных аспектов информационной безопасности как предмета.

Рассмотрим имеющиеся представления об информационной безопасности. Так, в Доктрине информационной безопасности под таковой понимается «состояние защищенности национальных интересов государства в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

В Доктрине раскрывается содержание и таких сопутствующих понятий, как интересы личности, интересы общества и интересы государства в информационной сфере:

− интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

− интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

− интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры. Это необходимо для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Однако частично эти интересы были затронуты в понятии информационной безопасности Российской Федерации, отдельных определений, касающихся обеспечения информационной безопасности личности, общества, государства, данная Доктрина не содержит. Между тем, обеспечение комплексной информационной безопасности в Российской Федерации, на мой взгляд, требует уточнения данных

определений и детализации роли отдельных составляющих информационной безопасности.

В тех малочисленных случаях, когда в учебниках по предмету «Информатика и ИКТ» упоминается понятие «информационная безопасность», оно, как правило, применяется только в узком его смысле. Например, в учебнике А.Г. Гейн и А.И. Сенокосова «Информатика и ИКТ» [4] под информационной безопасностью понимается: «состояние защищенности информации и поддерживающей инфраструктуры информационной системы от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб субъектам информационных отношений, имеющих место в рамках данной информационной системы». А в учебнике «Информатика и ИКТ» для 11 класса под редакцией профессора Н.В. Макаровой (2009) [8] «информационная безопасность – это совокупность мер по защите информационной среды общества и человека». В обоих приведённых примерах делается акцент на защите информации: в первом случае – в рамках информационной системы, а во втором – в информационной среде. Следует отметить, что в Доктрине об информационной безопасности главным определение этого понятия является «сбалансированность интересов личности, общества и государства».

Исходя из анализа, следует определять понятие информационной безопасности, исходя из широкого смысла, то есть, говоря о формировании системных знаний в столь значимой в современном информационном обществе области, как обеспечение информационной безопасности.

Рассматривая ФГОС по Информатике и ИКТ среднего (общего) и хотелось бы отметить, что целью обучения Информационной безопасности в ходе освоения основной общеобразовательной программы заключается в формировании у старшеклассников умения использовать средства коммуникационных и информационных технологий в решении заданных

задач с соблюдением всех необходимых норм информационной безопасности.

Достижение цели обучения информационной безопасности помогает и программа воспитания и социализации школьников, которая, в том числе, включает в себя цели, задачи, планируемые результаты духовно-нравственного развития, воспитания и социализации обучающихся, основные направления и ценностные основы духовно – нравственного развития, воспитания и социализации. Эта цель находит своё отражение и в требованиях к метапредметным результатам обучения основной образовательной программы среднего (полного) общего образования. Которые, к тому же, должны показывать готовность и способность к самостоятельной информационно-познавательной деятельности, содержа в себе умение быстро ориентироваться в различных источниках информации, умение критически оценивать и переформулировать информацию, получаемую из разных источников информации.

Таблица 1

Требование стандартов для основной и старшей школы по вопросам обеспечения информационной безопасности

<table>
<tr><td>Стандарт
2 ступень (средняя школа)</td><td colspan="2">Стандарт
3 ступень (старшая школа)</td></tr>
<tr><td rowspan="2">Предметные результаты изучения предметной области «Математика и информатика» должны отражать: формирование навыков и умений безопасного и</td><td>Базовый уровень</td><td>Профильный уровень</td></tr>
<tr><td>Метапредметные результаты освоения основной образовательной программы должны отражать: умение использовать средства</td><td>Метапредметные результаты освоения основной образовательной программы должны отражать развитие умений</td></tr>
</table>

целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права. Программа развития универсальных учебных действий (программа формирования обще учебных умений и навыков) на ступени основного общего образования (далее – Программа) должна быть направлена на: *формирование и развитие компетенции обучающихся в области использования информационно-коммуникационных технологий на уровне общего пользования, включая владение основами информационной*	*ИКТ в решении когнитивных, коммуникативных и организационных задач с соблюдением требований правовых и этических норм, норм ИБ.* Изучение предметной области «Математика и информатика» должно обеспечить: *принятие этических аспектов Информационных технологий; осознание ответственности людей, вовлечённых в создание и использование информационных систем, распространение информации.* «Информатика» (базовый уровень) – требования к предметным результатам освоения базового курса	*использовать средства ИКТ в решении коммуникативных и организационных задач с соблюдением требований правовых и этических норм, норм ИБ.* Изучение предметной области «Математика и информатика» должно обеспечить: *Принятие этических аспектов информационных технологий; осознание ответственности людей, вовлечённых в создание и использование информационных систем,*

безопасности, умением безопасного использования средств ИКТ и сети Интернет.	информатики должны отражать: *сформированность понимания основ правовых аспектов использования компьютерных программ и работы в Интернете.*	*распространение информации*. «Информатика» (углубленный уровень) – требования к предметным результатам освоения курса информатики должны включать требования к результатам освоения курса и дополнительно отражать *сформированность знаний базовых принципов норм информационной этики, принципов обеспечения информационной безопасности, способов и средств обеспечения надёжного функционирования средств ИКТ.*

1.3 Анализ учебной литературы курса «Информатики и ИКТ» для 8-11 классов

Выполнив полный анализ содержания учебников на предмет содержания в них требований стандартов и примерных образовательных программ в области обучения вопросам информационной безопасности учащихся основной и старшей школы, хотелось бы отметить, что авторы включают в содержание учебника практически все понятия стандарта. Но многие из этих авторов не вводят понятие «информационная безопасность», несмотря на то, что оно указано в требованиях ФГОС как для основной, так и для старшей школы. При этом авторы учебников по информатике предпочитают использовать концентрический принцип в преподавании разделов, относящихся к данной проблематике, часто повторяя содержание по данному разделу в неизменном виде, как в основной школе, так и в старшей.

Для примера, подтверждающего использование подобного подхода в школьных учебниках по предмету «Информатика и ИКТ» рассмотрим содержание параграфа 35 «Этика интернета. Безопасность в Интернете» учебника для 9 класса А.Г. Гейн «Информатика и информационные технологии» [4]. Оно почти полностью повторяет содержание параграфа 44 с таким же названием «Этика интернета. Безопасность в Интернете» в учебнике по предмету «Информатика и ИКТ» для 11 класса А.Г. Гейн [3]. Та же ситуация складывается и с параграфом 36 «Защита информации» учебника для 9 класса. Параграф 36 повторяется с незначительными изменениями в учебнике для 11 класса, только порядковый номер стал 46.

Для подтверждения своих слов, хотелось бы рассмотреть содержание раздела «Защита информации» в учебнике Н.Д. Угриновича для 8 класса «Информатика и ИКТ» [16]. Информация в параграфе дублируется с незначительными изменениями в разделе «Защита от

несанкционированного доступа к информации» в учебниках этого же автора, только за 10 класс [11].

В вопросах изучения информационной безопасности в средней и старшей школах необходимо использовать спиральный принцип обучения для обеспечения соответствия уровня сложности материала возрастным особенностям учеников. Необходимо углубленное содержание раскрываемых понятий. Школьники при таком подходе получат увеличенный интерес к вопросам информационной безопасности, смогут расширить свой кругозор, улучшат мотивацию к восприятию нового материала.

Так же анализ учебных материалов различных авторов для 8-11 классов привёл к выводу, что некоторые авторы учебников, приводя конкретные примеры, не дают определения основным понятия по информационной безопасности, ограничиваясь примерами и отсылая обучающегося к Интернет – источникам, которые зачастую даже не рассчитаны на аудиторию этого возраста.

Например, в учебнике Л.Ф. Соловьевой для 8 класса «Информатика и ИКТ» [17] приводятся следующие рекомендации по работе с основными понятиями в области информационной безопасности: «Основные понятия и термины, используемые в сфере информационной безопасности при работе в интернете можно найти, например, в справочной системе обозревателя Internet Explorer». И далее: «в Интернете нет недостатка в сведениях, касающихся информационной безопасности при работе в сети. На сайте http://www.securitylab.ru, например, можно найти подробный обзор существующих угроз и дополнительных средств обеспечения информационной безопасности». Или, например, «Пользуясь справочной службой операционной системы Windows, можно найти необходимые для обеспечения информационной безопасности сведения». Это не позволяет сформировать системные знания учащихся о данной предметной области.

Модель содержания обучения учащихся средней и старшей школ предполагает преемственность знаний по информационной безопасности с предыдущими ступенями обучения, систематизацию понятий в этой области знания.

Примером систематизации понятий отдельных тем по информационной безопасности может быть материал учебника И.Г. Семакина для 10–11 классов «Информатика и ИКТ (базовый уровень)» [10] (параграф 12 второй главы «Информационные процессы и системы»). Авторами систематизированы основные понятия в области защиты цифровой информации и представлены в виде иерархической схемы под названием Система основных понятий (рис. 1).

Система основных понятий

<table>
<tr><td colspan="4">Защита цифровой информации</td></tr>
<tr><td colspan="4">Цифровая информация —
информация, хранение, передача и обработка которой осуществляются средствами ИКТ</td></tr>
<tr><td colspan="4">Защищаемая информация —
информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.</td></tr>
<tr><td colspan="2">Угроза утечки</td><td colspan="2">Угроза разрушения</td></tr>
<tr><td colspan="2">Преднамеренная кража, копирование, прослушивание и пр.</td><td>Несанкционированное разрушение</td><td>Непреднамеренное разрушение</td></tr>
<tr><td>Проникновение в память компьютера, в базы данных информационных систем</td><td>Перехват в каналах передачи данных, искажение, подлог данных</td><td>Вредоносные программные коды-вирусы; деятельность хакеров, атаки</td><td>Ошибки пользователя, сбои оборудования, ошибки и сбои в работе ПО, форс-мажорные обстоятельства</td></tr>
<tr><td colspan="4">Меры защиты информации</td></tr>
<tr><td colspan="2">Физическая защита каналов; криптографические шифры; цифровая подпись и сертификаты</td><td>Антивирусные программы; брандмауэры; межсетевые экраны</td><td>Резервное копирование; использование ББП; контроль и профилактика оборудования; разграничение доступа</td></tr>
</table>

Рис. 1. Система основных понятий

Так же анализ содержания учебников по предмету «Информатика и ИКТ» показал взаимосвязь технологических научных понятий в области информационной безопасности и более широкого круга понятий, которые относятся к информационной культуре: информационная этика, этика интернета, компьютерная этика, сетевой этикет, этика сетевого общения, нормы поведения при использовании информации. Наверняка это связано с тем, что информационная безопасность связана со всеми сферами жизни школьников.

Следует отметить, что зачастую, у школьников возникают трудности при изучении таких абстрактных понятий, как «информационная культура» и «информационная этика», и устранение этих трудностей требует, чтобы были применены необходимые технологии обучения, которые позволят упростить и конкретизировать смысл этих понятий и сделать их смысл доступным для ребенка.

Например, в учебник А.Г. Гейн для восьмого класса «Информатика и информационные технологии» [5] устанавливается важная связь понятия «информационная культура» и аспектов информационной безопасности: «Информационная культура каждого человека подразумевает готовность человека к жизни и деятельности в высокоразвитой информационной среде, умение эффективно использовать ее возможности и защищаться от ее негативных воздействий». В характеристике составляющих элементов информационной культуры указаны, в том числе, имеющие непосредственное отношение к области информационной безопасности поступающей информации и этичное поведение при использовании информации», что также указывает на соподчиненность понятия «информационной этики» понятию «информационная культура».

И.Г. Семакин же делает в своём учебнике для 9 класса «Информатика и ИКТ» [10] акцент на соблюдении правовых норм как важной части информационной культуры: «Необходимой составляющей общей культуры современного человека становится информационная

культура. Это понятие включает в себя не только умение использовать средства информационно-коммуникационных технологий, но и соблюдение правовых норм в своей информационной деятельности».

Н.Д. Угринович в своём учебник «Информатика и ИКТ» для 9 класса [16] считает, что «информационная культура состоит не только в овладении определенным комплексом знаний и умений в области информационных и коммуникационных технологий, но и предполагает знание и соблюдение юридических и этических норм и правил».

Подобным образом, авторы создают предпосылки для конкретизации и систематизации, на первый взгляд, достаточно абстрактных культурологических понятий, которые непосредственно связанны с областью информационной безопасности. С другой стороны, необходимо при обучении информационной безопасности избегать излишней конкретики и обеспечивать учеников правдивой информации на момент её приобретения. Например, утверждение Н.Д. Угриновича в своём учебнике «Информатика и ИКТ» для 8 класса [15] о том, что «наиболее надёжную защиту от вирусов обеспечивают российские антивирусные системы DrWeb и Антивирус Касперского» кажутся слишком категоричными и не совсем отражают действительность.

Анализируя преемственность содержания обучения в вопросах информационной безопасности было установлено, что имеет место быть достаточно большой дисбаланс в равномерности распределения материала для каждого класса, последовательность выдачи материала происходит без учета важных внутрипредметных связей.

Так, в учебнике Н.Д. Угриновича «Информатика и ИКТ (базовый уровень)» для 10 класса [14] рассматриваются такие важные темы обеспечения информационной безопасности, как общение в интернете в режиме реального времени, системы мгновенных сообщений, серверы общения в режиме реального времени, Интернет – телефония, IP-

телефония, SMS- и MMS-сообщения. Сами вопросы информационной безопасности в этом учебнике остаются практически без внимания.

Аналогичным образом, в учебнике М.Е. Фиошин для 11 класса «Информатика и ИКТ (Профильный уровень)» [18] вопросы, тесно связанные с информационной безопасности почти не упоминаются, потому что автор их полностью выносит для обучения в 10 классе.

Также анализ выявил, что в вопросах раскрытия «принципов обеспечения информационной безопасности» реализуются не до конца. В лучшем случае приводятся ссылки на нормативные документы и частично отражены принципы антивирусной защиты. Разделы, которые связаны с вредоносным программным обеспечением, значительно преувеличены по сравнению с остальными рассматриваемыми проблемами области обеспечения информационной безопасности. Подобное наблюдается, например, в учебнике Н.Д. Угриновича «Информатика и ИКТ (Профильный уровень)» для 10 класса [14].

Так же хотелось бы отметить, что в учебнике Л.Ф. Соловьевой «Информатика и ИКТ» для 8 класса [17] дана важная оценка аспектов информационной безопасности, приобретающих широкое распространение облачных сервисов. Наглядно показаны недостатки в обеспечении информационной безопасности при работе с «облачными» технологиями.

Интересно и то, что, например, понятие «фишинг» встречается только в учебнике Н.Д. Угриновича «Информатика и ИКТ (Профильный уровень)» для 10 класса [14], а понятия «троллинг» и «кибербуллинг» в учебниках совсем отсутствуют. По моему мнению, данные понятия являются необходимыми к изучению, так как эти угрозы неотвратимо будут встречены учениками в информационном пространстве. Поэтому необходимо обучать школьников противодействию данным угрозам сети Интернет.

Выводы по главе 1

Высокую актуальность данной темы косвенно подтверждает и тот факт, что информационная безопасность важна не только как личностные результаты, которых школьнику необходимо достигнуть, но и как одна из важнейших составляющих государственной безопасности, что подтверждается большим количеством нормативных документов. Все эти документы обосновывают необходимость наличия высокого уровня информационной безопасности для обеспечения безопасной жизни граждан во всех сферах жизнедеятельности, в том числе и в информационной сфере.

Федеральный государственный стандарт образования описывает далеко не все необходимые результаты, так как не успевает включать в себя новообразованные угрозы, а также их самые различные модификации. Необходимо разработать основные элементы стандарта таким образом, чтобы он соответствовал большинству требований информационной безопасности.

Для того чтобы достигнуть желаемых результатов, нужно создать актуальные методические комплексы. Они должны включать в себя современную учебно-методическую литературу, отражающие современную информацию на тему информационной безопасности, которая будет успевать за актуальными киберугрозами.

Анализ учебных комплексов по Информатики и ИКТ для 7-11 классов таких авторов как: Гейн А.А., Угринович Н.Д., Семакин И.Г., Босова Л.Л., Босова А.Ю. и др., на предмет наличия там конкретных знаний об информационной безопасности, выявил недостаточное содержание актуальной информации на тему информационной безопасности, которая в состоянии научить их адекватному ответу на угрозу информационной безопасности. Методики, применяемые для обучения учеников 7-11 классов основам информационной безопасности,

не могут угнаться за столь быстро развивающимися технологиями мошенничества, и не в состоянии обеспечить высокий уровень грамотности в этой сфере. Учебный комплекс должен научить учащихся адекватному и действенному ответу на большую часть киберугроз, с которой он может встретиться в информационной сфере.

ГЛАВА 2. РАЗРАБОТКА МЕТОДИКИ ОБУЧЕНИЯ ТЕМЕ: «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

2.1 Методическая разработка интегрированных уроков по теме «Информационная безопасность» по предмету «Информатика и ИКТ»

Развитие мобильных и переносных устройств сделало проникновение в интернет еще более масштабным. Развиваются мобильные сети, растут скорости передачи данных, увеличиваются зоны покрытия. Следовательно, с каждым годом трафик интернета увеличивается, и рост будет продолжаться. Но это лишь положительная сторона этого развития. Существует и отрицательная сторона – вместе с развивающимися мобильными технологиями параллельно развиваются и технологии мошенничества, различные вирусы и троянские программы, от которых, зачастую, наши устройства оказываются беззащитны.

Вся проблема в том, что антивирусные программы и различные сетевые экраны – это лишь инструмент для защиты от угроз в сфере информационной безопасности. Необходимо уметь этими инструментами правильно пользоваться. Для того чтобы научить школьников пользоваться этими инструментами, нужно создать актуальные методические комплексы. Они должны включать в себя современную учебно-методическую литературу, отражающие современную информацию на тему информационной безопасности, которая будет успевать за актуальными киберугрозами. Учебный комплекс должен научить учащихся адекватному и действенному ответу на большую часть киберугроз, с которой он может встретиться в информационной сфере.

Мною было разработано содержание нескольких учебных занятий для учащихся 8-11 классов по изучению вопросов информационной безопасности и способов противостояния угроз. Известно, что изучение информатики особенно эффективно при получении информации в форме цикличности, так называемой дидактической спирали. Поэтому вопросы

информационной безопасности следует также рассматривать циклично – посвящать 1-2 урока в каждом классе с 8 по 11. С учетом возрастных особенностей и уровня знаний учащихся целесообразно ввести следующее содержание таких уроков.

Таблица 2

Краткое содержание занятий по информационной безопасности

Класс	Урок	Тема	Цели	Изучаемые вопросы
8 класс	1 урок	Введение в курс информационной безопасности.	Знакомство с понятием информационной безопасности, понятием вируса и антивируса.	1) Что такое вирус? 2) Основные правила защиты компьютера от вредоносных программ. 3) Что такое программы - трояны? 4) Что такое программы – шпионы?
	2 урок	Основные угрозы безопасности подросткам в сети Интернет	Знакомство с угрозами, которые могут нанести ущерб психологическому здоровью учеников.	1) Что такое кибербуллинг? 2) Как можно обезопасить себя от воздействия угрозы кибербуллинга? 3) Назовите признаки интернет – зависимости. 4) Перечислите способы фильтрации нежелательного контента (антивирусные программы, фаерволы, сетевые экраны)
9 класс	1 урок	Безопасность в социальных	Знакомство с угрозами,	1) Изучение основных угроз в

		сетях	подстерегающими учеников в социальных сетях. Изучение методов защиты от злоумышленников.	социальных сетях (появление частной информации о человеке в соцсети без его желания; взлом аккаунта соцсети и рассылка спама; получение сообщений от известного пользователя сомнительного содержания - спам). 2) Способы обеспечения информационной безопасности в социальных сетях (смена пароля, подтверждение действий по телефону, не открывать сомнительные сообщения; не использовать одинаковый пароль в разных соцсетях).
	2 урок	Обеспечение безопасности данных в общественных сетях	Знакомство с понятиями информационной безопасности в сетевом пространстве.	1) Как защитить своё WiFi соединение в незащищенной сети? 2) Решение практических заданий (как войти в интернет

				в анонимном режиме; что делать, если забыл выйти из аккаунта социальной сети при использовании компьютера в общественном месте; что нужно делать, если на почту пришло письмо о большом выигрыше; что делать, если на почту пришло письмо о блокировке денежных средств и просьбе ввести пароль с целью их возврата)
10-11 класс	1 урок	Информационная безопасность	Рассмотреть информационную безопасность как необходимую составляющую современного информационного общества.	1) Назовите стандартную модель информационной безопасности. 2) Дайте определение понятию хакер? 3) Назовите действия, которые могут нанести ущерб информационной безопасности.
	2 урок	Угрозы информационной безопасности	Рассмотреть угрозы, которые угрожают государственной информационной безопасности.	1) Что такое угроза информационной безопасности? 2) Назовите три разновидности угрозы.

				3) Что такое доступность информации? 4) Назовите угрозы исходя из Доктрины информационной безопасности РФ.
	3 урок	Методы обеспечения информационной безопасности	Рассмотрение методов обеспечения информационной безопасности. Тезис о том, что необходимо применять комплексную защиту для большей безопасности.	1) Перечислите методы обеспечения информационной безопасности. 2) Какие основные требования предъявляется к системам шифрования?

Урок №1.

Тема урока: Введение в курс информационной безопасности.

Класс: 8.

Цели урока: Знакомство с понятием информационной безопасности, понятием вируса и антивируса.

Тип урока: Объяснение и первичное закрепление знаний.

Основные понятия:

1. Программы – черви и вирусы

Вирусы – это вредоносные программы, обладающие способностью к несанкционированному пользователем саморазмножению в компьютерах или компьютерных сетях, при этом полученные копии также обладают этой возможностью.

2. Программы – трояны

Программы – трояны – вирусы, имитирующие полезные программы для уничтожения данных, повреждения компьютера и похищения личных данных.

3. Программы – шпионы

Программы – шпионы – это общее название для программного обеспечения, осуществляющего сбор информации на компьютере без согласия пользователя.

ЦОРы для урока: Для данного урока подготовлено приложение LearningApps. (рис. 2,3)

Рис. 2. Задание LearningApps для 8 класса

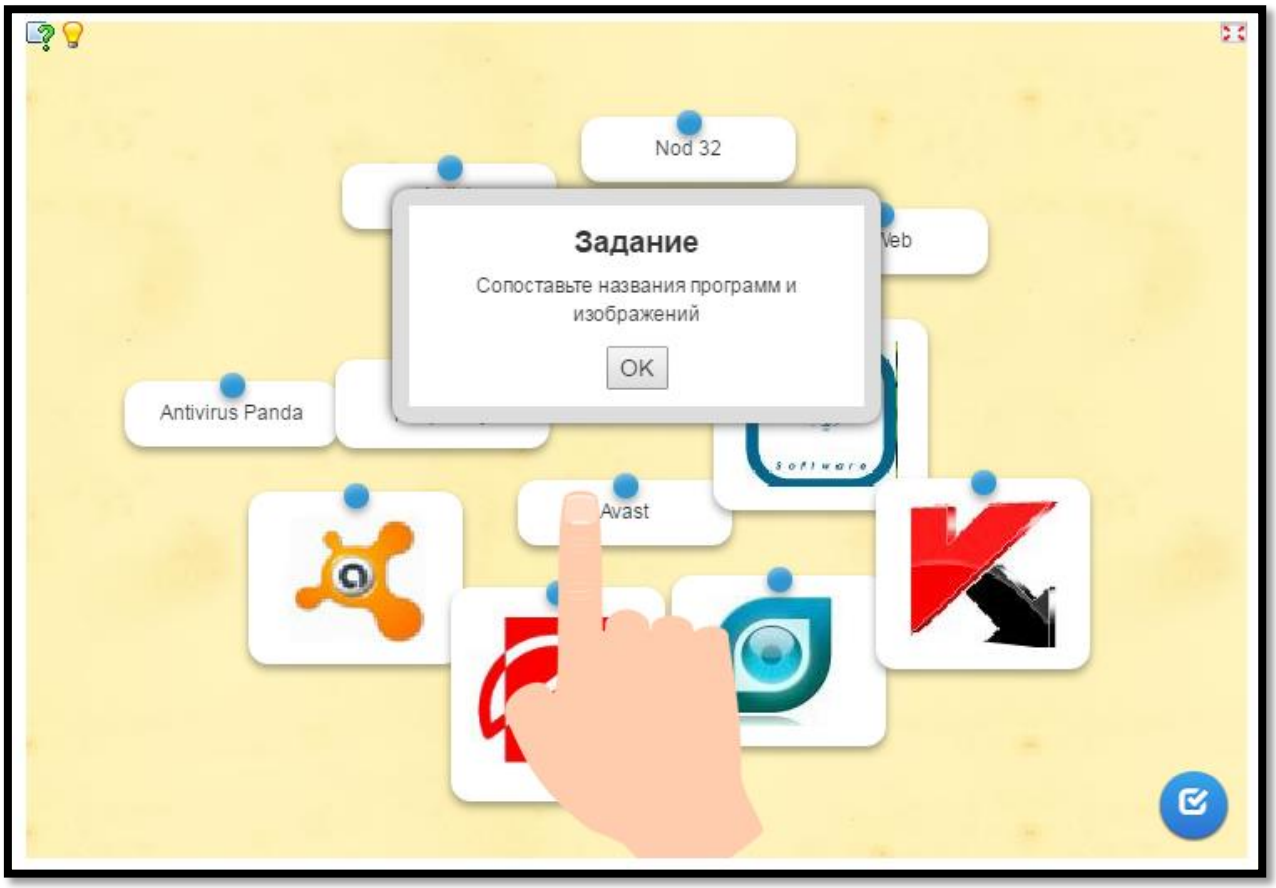


Рис. 3. Задание LearningApps для 8 класса

Методические рекомендации к уроку: Так как этот урок является основополагающим при изучении темы «Информационная безопасность», необходимо следить за тем, насколько успешно ученики усваивают новый материал.

Урок №2.

Тема урока: Основные угрозы безопасности подросткам в сети Интернет.

Класс: 8.

Цели урока: Знакомство с угрозами, которые могут нанести ущерб психологическому здоровью учеников.

Тип урока: Объяснение и первичное закрепление знаний.

Основные понятия:

- Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет — сервисов.
- Неприличный контент. Это информация, которая отрицательным образом влияет на психику подростка, развращая и извращая её. К счастью, существует достаточное количество способов фильтровать поступающий на наши компьютеры контент.
- Интернет-зависимость — навязчивое желание войти в интернет, находясь оффлайн и неспособность выйти из интернета, будучи онлайн.

ЦОРы для урока: Для данного урока подготовлено приложение LearningApps. (рис. 4)

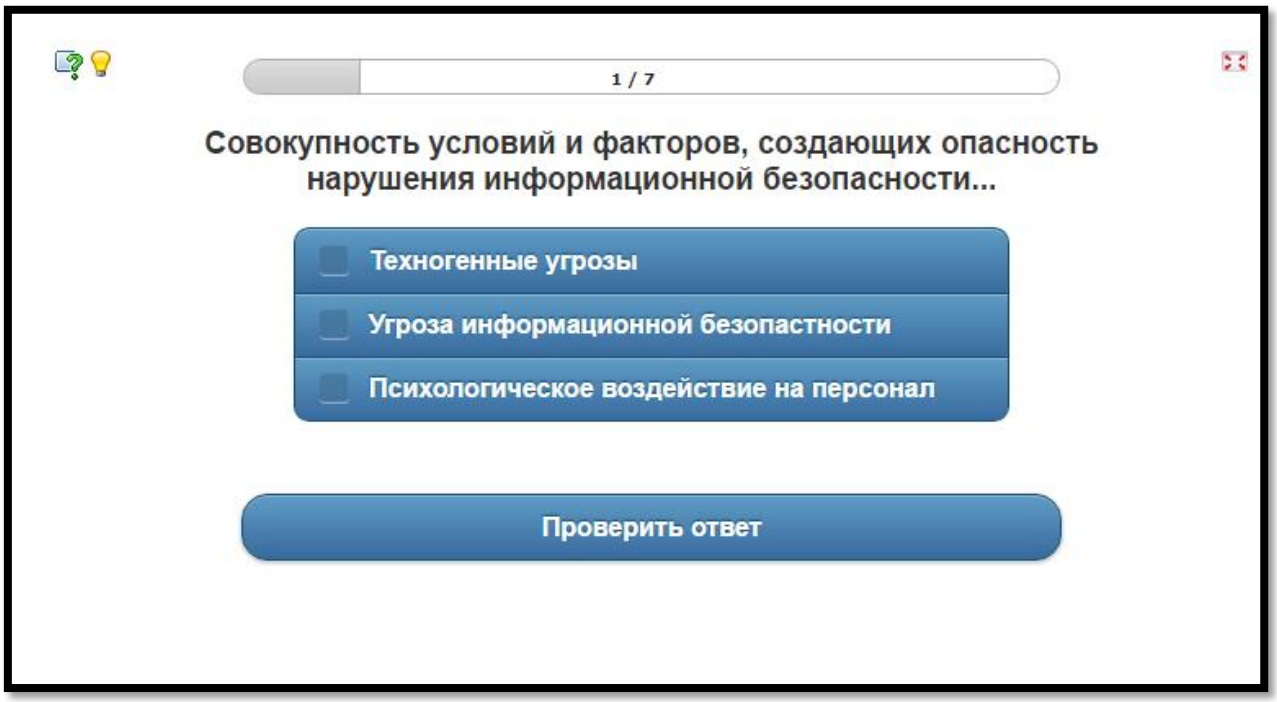


Рис. 4. Второе задание LearningApps для 8 класса

Методические рекомендации к уроку: Выполнение данного задания должно быть индивидуальным. Это задание также является проверочным для данного урока. После проведения второго урока ученики

должны хорошо разбираться в понятиях темы «Информационная безопасность».

Урок №3.

Тема урока: Информационная безопасность

Класс: 11.

Цели урока: Рассмотреть информационную безопасность как необходимую составляющую современного информационного общества.

Тип урока: Повторение и первичное закрепление знаний.

Основные понятия:

- под информационной безопасностью понимается защищённость информации и поддерживающей её инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам или поддерживающей инфраструктуре;
- хакер — квалифицированный ИТ-специалист, который разбирается в работе компьютерных систем;
- отдельная категория электронных методов воздействия — компьютерные вирусы и другие вредоносные программы. Они представляют собой реальную опасность для современного бизнеса, широко использующего компьютерные сети, Интернет и электронную почту;
- спам — в изначальном значении нежелательные рекламные электронные письма;
- «Естественные» угрозы. На информационную безопасность компании могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства и т.д;

ЦОРы для урока: Для данного урока подготовлено приложение LearningApps. (рис. 5)

Рис. 5. Задание LearningApps для 10-11 классов

Методические рекомендации к уроку: При изучении темы «Информационная безопасность» необходимо повторять ранее полученные знания, актуализировать их и дополнять новыми данными. Данный урок поможет повторить пройденный в 8 классе материал и углубит познания учеников.

Урок №4.

Тема урока: Методы обеспечения информационной безопасности.

Класс: 11.

Цели урока: Рассмотрение методов обеспечения информационной безопасности. Тезис о том, что необходимо применять комплексную защиту для большей безопасности.

Тип урока: Повторение и первичное закрепление знаний.

Контрольные вопросы:

- Что такое межсетевой экран?
- Какие основные требования, предъявляемые к системам шифрования, существуют?
- Какие бывают средства защиты информационной безопасности?

ЦОРы для урока: Для данного урока подготовлено приложение LearningApps. (рис. 6,7)

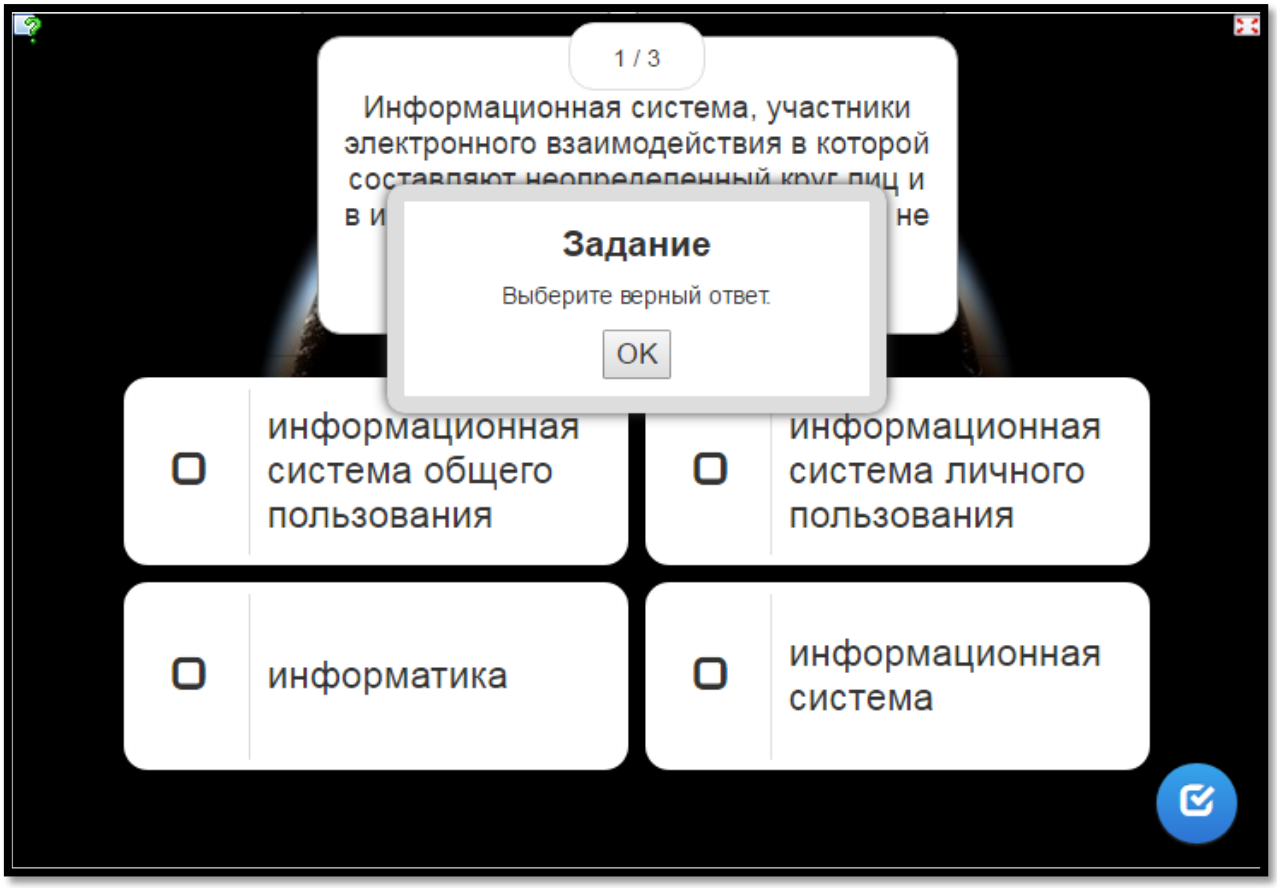


Рис. 6. Задание LearningApps для 10-11 классов

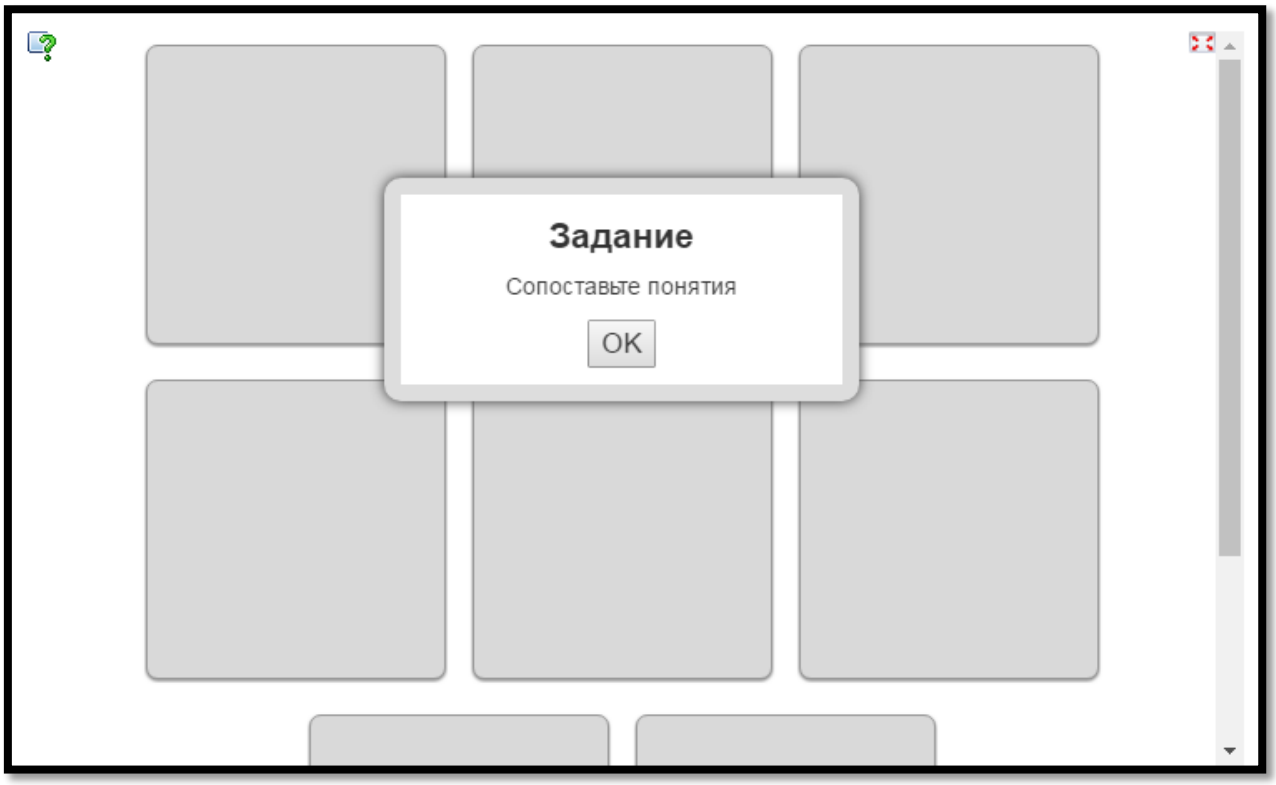


Рис. 7. Второе задание LearningApps для 10-11 классов

Методические рекомендации к уроку: Данный урок является заключительным в курсе «Информационной безопасности» в школе, после завершения данного урока, ученики должны хорошо разбираться в определениях информационной безопасности, знать угрозы, которые им угрожают, и уметь защищать свой компьютер от этих угроз.

2.2 Программно-методическая поддержка методической разработки интегрированных уроков по теме «Информационная безопасность»

Для программно – методической поддержки моих методических разработок мною была выбрана система управления сайтов с открытым исходным кодом, которая написана на языке программирования PHP, которая называется WordPress.

WordPress – популярная и очень удобная программа для управления контентом (CMS). Она задумывалась и создавалась как система управления содержимым блогов, но спустя короткий промежуток времени обрела большую популярность не только у пользователей блогов, но и у владельцев небольших интернет – проектов. Над программой долгое время упорно работали многие программисты, и в настоящее время она распространяется на бесплатной основе. Программа имеет открытый исходный код, благодаря чему, многие пользователи, в том числе и начинающие, могут на собственном опыте понять, что такое WordPress.

WordPress подходит не только для создания простых персональных блогов, но и для создания несложных интернет – проектов, таких как: персональных страничек, сайтов-визиток компаний, портфолио, информационных сайтов, малобюджетных интернет-магазинов. С помощью предоставленных средств для разработки сайтов, разобраться в этой системе может даже человек, который не имел опыта разработки сайтов.

Но и для опытных пользователей, WordPress приготовил много новых функциональных возможностей, которые позволяют использовать различные плагины, необходимые в конкретных ситуациях и для конкретного сайта. Основной частью системы WordPress являются «темы», которые включают в себя уже готовые изображения, макеты веб-страниц и таблицы стиля CSS. С помощь них обладатель сайта может очень быстро и без особых усилий легко изменять внешний вид своего проекта и

наполнять сайт с помощью средств WordPress. Неправильно утверждать, что сайты, которые были созданы по шаблонам этого простого движка, будут выглядеть невзрачно или похоже друг на друга. Программа позволяет размещать логотип компании вверху страницы.

Также WordPress включает в себя всё необходимое программное обеспечение, поэтому для создания сайта на этом движке потребуется только браузер. Раньше для создания сайта требовалось обязательное знание языка HTML, то WordPress отменяет необходимость этих знаний и с созданием простого сайта справится даже не подготовленный человек.

Высокую безопасность WordPress обеспечивает его самодостаточность, так как при использовании различных программ для разработки и создания сайта часто приводит к дырам в системе безопасности сайта. Разработчики системы WordPress постоянно следят за уязвимостями их системы и иногда предлагают установить обновления – необходимо дать только своё согласие на установку. Система авторизации сайта может предоставить доступ к редактированию сайта только ограниченному числу человек, которые будут выбраны администратором сайта, поэтому перехват доступа у администратора не возможен.

Преимущества данной платформы для создания сайтов следующие:

- бесплатность. WordPress — это бесплатная система. Для новичка, который хочет создать свой блог или небольшой проект, это немаловажный момент и огромное преимущество;
- простота установки и использования. Весь процесс установки занимает не более 5-ти минут, и для этого не нужно быть программистом, разбираться в коде и технических нюансах. Разработчики постарались сделать систему максимально простой и дружелюбной к пользователю, чтобы в ней смогли максимально быстро разобраться даже абсолютные новички;
- кроссплатформенность. WordPress устанавливается и используется непосредственно на вашем сайте (сервере). На компьютер не нужно

ничего дополнительно устанавливать. Это значит, что вы можете управлять своим сайтом с любого компьютера из-под любой операционной системы. Единственное необходимое условие — это подключение к Интернету. Даже в транспорте с одним лишь мобильным телефоном в руках вы можете добавить новую статью на сайте и прикрепить картинку;

- встроенный редактор. Пользоваться WordPress-ом очень просто и легко в основном благодаря интуитивно понятному встроенному редактору. Если вы хоть раз работали в Microsoft Word, освоить редактор будет детской задачей. Форматирование текста, ссылки, вставка картинок и видео — все это делается в пару кликов;
- популярность. WordPress — это самая популярная в мире система управления содержимым сайта. Согласно официальной статистике, доля рынка WordPress среди других конкурентов превышает 55%. Более 58 миллионов сайтов в мире существуют на WordPress. Более 297 миллионов людей просматривают ежемесячно 2,5 миллиарда страниц на WordPress. Каждый 7-ой сайт в мире создан и работает на WordPress. Если вам нужен какой-либо плагин, их больше 15 тысяч. В Интернете вы найдете огромное количество бесплатных тем, шаблонов и плагинов. А если у вас возникнут какие-то вопросы, вы легко сможете найти ответ в Интернете.

Сервер базы данных – MySQL. MySQL – это одна из самых популярных и самых распространенных СУБД (система управления базами данных) в интернете. Она не предназначена для работы с большими объемами информации, но ее применение идеально для интернет-сайтов, как небольших, так и достаточно крупных.

MySQL отличатся хорошей скоростью работы, надежностью, гибкостью. Работа с ней, как правило, не вызывает больших трудностей. Поддержка сервера MySQL автоматически включается в поставку PHP.

Немаловажным фактором является ее бесплатность. MySQL распространяется на условиях общей лицензии GNU (GPL, GNU Public License).

Ранее для долговременного хранения информации приходилось работать с файлами: помещать в них некоторое количество строчек, а затем извлекать их для последующей работы. Задача длительного хранения информации очень часто встречается в программировании Web-приложений: подсчёт посетителей в счётчике, хранение сообщений в форуме, удалённое управление содержанием информации на сайте и т.д.

Между тем, профессиональные приёмы работы с файлами очень трудоёмки. Необходимо заботится о помещении в них информации, о её сортировке, извлечении, при этом не нужно забывать, что все эти действия будут происходить на сервере хост-провайдера, где с очень большой вероятностью стоит один из вариантов Unix – следовательно, нужно так же заботиться о правах доступа к файлам и их размещении. При этом объём кода значительно возрастает, и совершить ошибку в программе очень просто.

Все эти проблемы решает использование базы данных. Базы данных сами заботятся о безопасности и сортировке информации и позволяют извлекать и размещать информацию при помощи одной строчки. Код с использованием базы данных получается более компактным, и отлаживать его гораздо легче. Кроме того, не нужно забывать и о скорости - выборка информации из базы данных происходит значительно быстрее, чем из файлов.

Приложение на PHP, использующее для хранения информации базу данных (в частности, MySQL) всегда работает быстрее приложения, построенного на файлах. Дело в том, что базы данных написаны на языке C++, и написать на PHP программу, которая работала бы с жёстким диском эффективнее базы данных - задача неразрешимая по определению,

поскольку программы на PHP в принципе работают медленнее, чем программы на C++, так как PHP - интерпретатор, а C++ это компилятор.

Таким образом, основное достоинство базы данных заключается в том, что она берёт на себя всю работу с жёстким диском и делает это очень эффективно.

Для проверки полученных знаний в результате обучения теме «Информационная безопасность» были созданы дидактические материалы при помощи технологий LearningApps.org.

Технология LearningApps позволяет в режиме онлайн создавать и использовать интерактивные задания самых разных видов: викторины, вставка пропусков в текст, кроссворды и игры с буквами на составление слов, пазлы, подобрать пару и многое другое. Задания, имеющиеся на сайте, рассортированы по категориям (тематике), уровням образования. Имеются ссылки, позволяющие поделиться заданиями и HTML-коды для встраивания на страницу сайта или блога. Для создания своих заданий необходимо зарегистрироваться на сайте LearningApps.org (регистрация бесплатна). Задания можно создать с нуля или на основе одного из понравившихся вам готовых вариантов.

Созданные задания можно встраивать в страницу сайта, скачивать для использования оффлайн.

Используя вышеописанные инструменты разработки баз данных и сайтов, был создан ЭОР (электронный образовательный ресурс), который расположен по адресу http://informbez.com для помощи в обучении темы информационной безопасности для учеников 8-11 классов. На рисунке 8 представлена главная страница сайта.

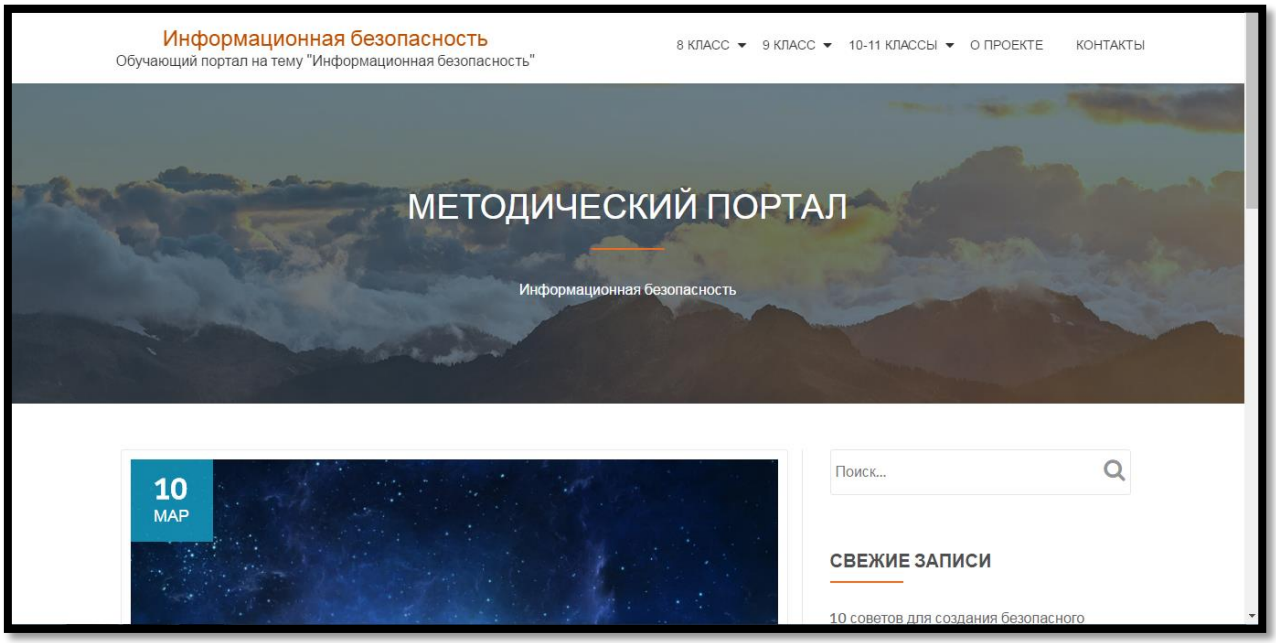


Рис. 8. Главная страница сайта

В верхнем меню сайта расположено меню с выпадающим списком (рис 9).

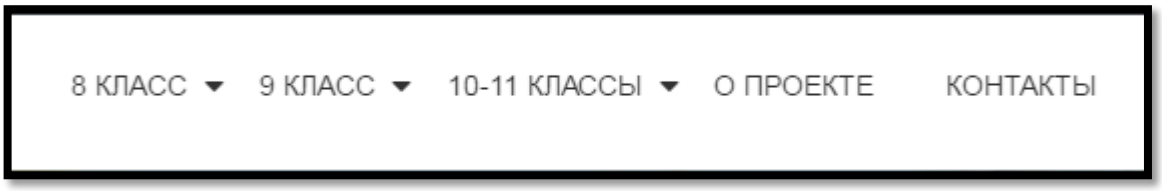


Рис. 9. Меню

Верхнее меню содержит в себе 5 разделов: «8 класс», «9 класс», «10-11 класс», «О проекте», «Контакты».

Во вкладке «8 класс» (рис. 10) содержатся пункты меню, которые содержат в себе вспомогательные материалы для 2 уроков на тему «Информационная безопасность». Они называются «Введение в курс информационной безопасности» и «Основные угрозы безопасности подросткам в сети Интернет», а также задания, которые используют технологию LearningApps.org.

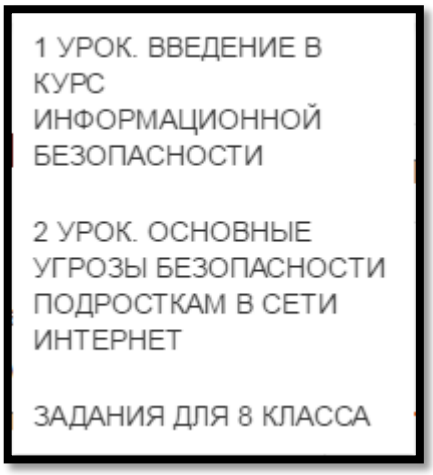


Рис. 10. Содержание раздела «8 класс»

Вкладка «9 класс» (рис. 11) содержит в себе пункты меню, в которой представлены вспомогательные материалы для уроков на тему «Безопасность в социальных сетях» и «Обеспечение безопасности данных в общественных местах» и задания, использующие технологию LearningApps.

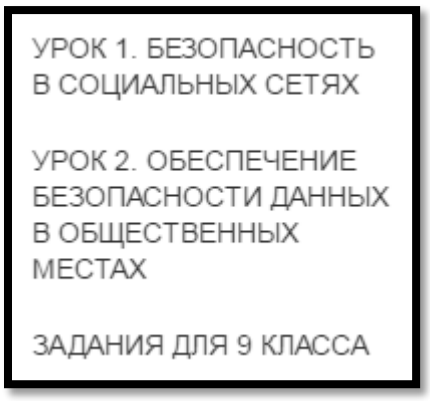


Рис. 11. Содержание раздела «9 класс»

Вкладка «10-11 класс» (рис. 12) содержит в себе пункты меню, в которых находятся вспомогательные материалы для уроков на такие темы как: «Информационная безопасность», «Угрозы информационной безопасности» и «Методы обеспечения информационной безопасности». Так же данная вкладка содержит задания, использующие технологию LearningApps.

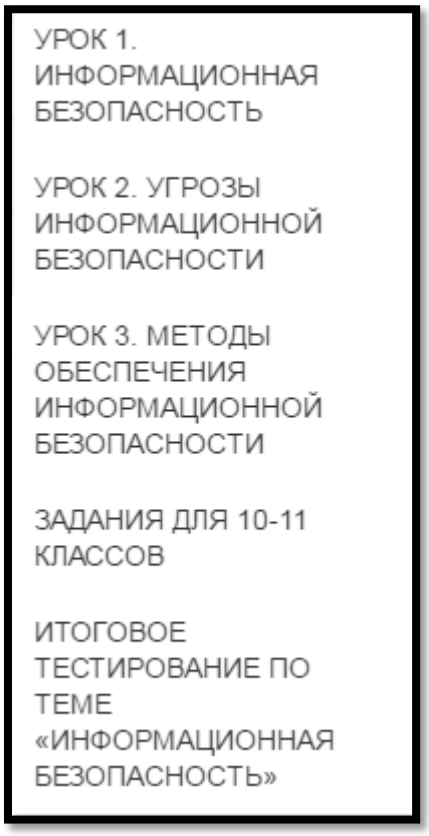


Рис. 12. Содержание раздела «10-11 класс»

Четвертая и пятая вкладка «Контакты» и «О проекте» содержат в себе контактную информацию и краткое описание проекта (рис. 13).

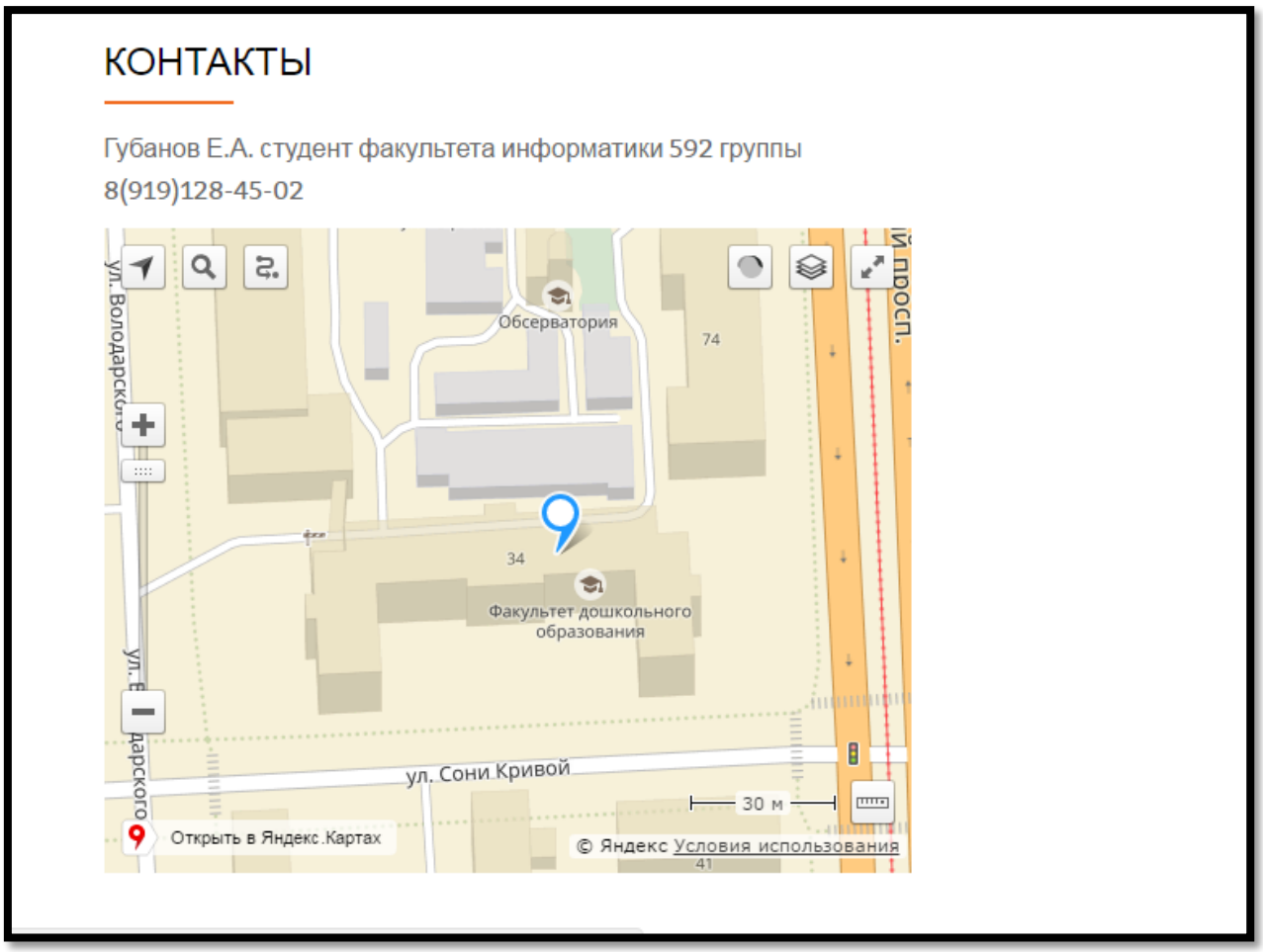


Рис. 13. Раздел меню «Контакты»

2.3 Апробация результатов исследования

Педагогическая апробация была проведена во время педагогической практики в МБОУ СОШ №151 г. Челябинска. Тема информационной безопасности впервые изучалась в 8 классах. В течении двух занятий были рассмотрены темы:

1. Урок №1 «Введение в курс информационной безопасности» - 1час.
2. Урок №2 «Основные угрозы безопасности подростка в сети Интернет» - 1час.

Апробация модуля прошла успешно. Помогло этому правильно заданные цели и задачи уроков. Также, на основе разработанного курса, была подготовлена статья для научной конференции [20].

Выводы по главе 2

Учитывая быстрое развитие угроз в информационной сфере, необходимо также быстро на них реагировать. Именно поэтому предпочтительно использовать для обучения школьников ЭОР (электронный образовательный ресурс). Используя технологии, которые позволяют быстро добавлять актуальные материалы для обучения школьников теме «Информационная безопасность», мы сможем своевременно и успешно подготавливать школьников к новообразованным угрозам.

Также, тема «Информационная безопасность» в школе, в которой была пройдена педагогическая практика, была интересна ученикам, и они с удовольствием получали новые знания, что способствовало изучению темы.

Таким образом, модуль и программно-методическая поддержка к нему были разработаны и апробированы на учениках.

Заключение

Подводя итоги данной работы, хотелось бы отметить, что проведенное исследование направлено на улучшение изучения темы информационной безопасности. Актуальность исследования обусловлена тем, что во время развития информационных технологий информационная безопасность имеют особое положение в курсе «Информатика и ИКТ».

В итоге работы были достигнуты цели и разработан ресурс к разделу «Информационная безопасность».

В процессе исследования были выполнены следующие задачи:

1.Изучены теоретические основы информационной безопасности.

2.Проведены анализы изложения темы в учебно-методических комплексах и дидактических материалах

3.Разработаны содержания уроков по теме «Информационная безопасность»

4.Разработана информационная поддержка для обучения учащихся теме «Информационная безопасность»

В подтверждении гипотезы можно сказать, что разработанный ресурс поможет своевременно и в краткие сроки доводить до учеников актуальную информацию, связанную с информационной безопасностью.

СПИСОК ЛИТЕРАТУРЫ

1. Анин Б. Ю. Защита компьютерной информации. – СПб.:"BHV-Санкт-Петербург" - 2000, 384 стр

2. Андреева Е. В., Босова Л. Л., Фалина И. Н Математические основы информатики. Элективный курс: Учебное пособие – М.: БИНОМ. Лаборатория знаний, 2005. – 328 с.

3. Галатенко В. А. Информационная безопасность. –М.: Финансы и статистика, 1997. –158 с.

4. Гейн А.Г. Информатика и ИКТ. 11 класс: Учеб. для общеобразоват. учреждений: базовый и профил. уровни / А.Г. Гейн, А.И. Сенокосов. М.: Просвещение, 2012.

5. Гейн А.Г. Информатика и информационные технологии. 9 класс: Учеб. для общеобразоват. учреждений / А.Г. Гейн, А.И. Сенокосов. М.: Просвещение, 2010.

6. Гейн А.Г. Информатика и информационные технологии: Учеб. для 8 кл. общеобразоват. учреждений / А.Г. Гейн, А.И. Сенокосов, Н.А. Юнерман. М.: Просвещение, 2009. 175 с.

7. Голицына, О.Л. Базы данных / О.Л. Голицына, Н.В. Максимов, И.И. Попов. - М.: Форум, 2004. - 352 с.

8. Лапчик М.П. и др. Методика преподавания информатики: Учеб. пособие для студ. пед. Вузов [Текст] / М.П. Лапчик, И.Г. Семакин, Е.К. Хеннер; Под общей ред. М. П. Лапчика. — М.: Издательский центр «Академия», 2012. Режим доступа http://businessfor.ru/m/frtyh/metodika_prepodavanija_informatiki_-_lapchik.html

9. Информатика и ИКТ. 11 класс. Базовый уровень / Под ред. проф. Н.В. Макаровой. СПб.: Питер, 2009.

10. Семакин И.Г. Информатика и ИКТ. Базовый уровень: Учебник для 10–11 классов / И.Г. Семакин, Е.К. Хеннер. 4-е изд., испр. М.: БИНОМ. Лаборатория знаний, 2008.

11. Семакин И.Г. Информатика и ИКТ: Учебник для 9 класса / И.Г. Семакин, Л.А. Залогова, С.В. Русаков, Л.В. Шестакова. 2-е изд., испр. М.: БИНОМ. Лаборатория знаний, 2009. 341 с.

12. Угринович Н.Д. Информатика и ИКТ. Базовый уровень: Учебник для 10 класса. 4-е изд. М.: БИНОМ. Лаборатория знаний, 2008. 212 с.

13. Угринович Н.Д. Информатика и ИКТ. Базовый уровень: Учебник для 11 класса. 2-е изд., испр. М.: БИНОМ. Лаборатория знаний, 2009. 187 с.

14. Угринович Н.Д. Информатика и ИКТ. Профильный уровень: Учебник для 10 класса. 3-е изд., испр. М.: БИНОМ. Лаборатория знаний, 2008. 387 с.

15. Угринович Н.Д. Информатика и ИКТ. Профильный уровень: Учебник для 10 класса. 3-е изд., испр. М.: БИНОМ. Лаборатория знаний, 2008. 387 с.

16. Угринович Н.Д. Информатика и ИКТ: Учебник для 8 класса. 2-е изд., испр. М.: БИНОМ. Лаборатория знаний, 2009. 178 с.

17. Угринович Н.Д. Информатика и ИКТ: Учебник для 9 класса. 2-е изд., испр. М.: БИНОМ. Лаборатория знаний, 2009. 295 с.

18. Соловьева Л.Ф. Информатика и ИКТ: Учебник для 9 класса. 2-е изд., испр. М.: БИНОМ. Лаборатория знаний, 2009. 295 с.

19. М.Е. Фиошин. Информатика и ИКТ. Учебник для 11 класса. (Профильный уровень).

20. Е.А. Губанов. XIX Всероссийская студенческая научно-практическая конференция Нижневартовского Государственного Университета.

Приложение 1

Разработка урока по теме «Информационная безопасность»

ПЛАН-КОНСПЕКТ УРОКА

Предмет: Информатика и ИКТ.

Класс: 8.

Тема урока: Информационная безопасность.

Учитель Губанов Е.А.

Дата:

Тип урока: Объяснение и первичное закрепление знаний.

Цель урока: Знакомство с понятием информационной безопасности, понятием вируса и антивируса.

Формы работы:

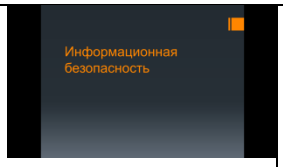
- Актуализация знаний – фронтальная работа
- Объяснение нового материала - лекция

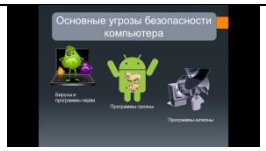
Задачи

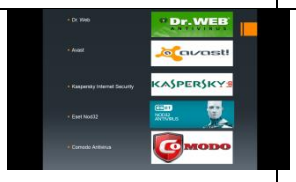
- *Образовательная:*
    - Дать ученикам представление о средствах защиты их персональных данных
    - Познакомить учащихся с понятиями информационной безопасности
    - Научить пользоваться антивирусными программами

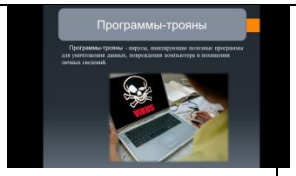
- *Развивающая:*
    - развивать алгоритмическое мышление учащихся, развивать мировоззрение;
    - развитие таких познавательных процессов, как восприятие, внимание, память.
- *Воспитательная:*
    - воспитывать устойчивый познавательный интерес к информационным технологиям через показ практического применения темы;
    - воспитывать такие качества личности, как активность, самостоятельность и аккуратность в работе;
    - воспитывать у учащихся стремление к реализации себя в обществе и общении.

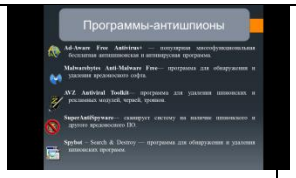
СТРУКТУРА И ХОД УРОКА

Деятельность учителя	**Деятельность учащихся**	**Интерактивная доска**	Тетрадь
Этап 1. Организационный момент 1 мин			
Приветствие. Здравствуйте, сегодня мы с вами поговорим об информационной безопасности. темой. Но сначала давайте вспомним			

Тема сегодняшнего урока “Информационная безопасность”. Запишите её в свои тетради.			
Этап 2 Объяснение нового материала 35 мин			
Теперь давайте с вами вспомним, что же такое информационная безопасность? Что угрожает нам в сети Интернет каждый день?	Отвечают на вопросы (в сети Интернет нам каждый день угрожают вирусы и программы – черви, программы – трояны, программы – шпионы, киберхулиганы(тролли), неприличный контент, фейки, интернет – зависимость, мошенничество) Записывают число и тему урока.		

Хорошо, давайте рассмотрим каждую из угроз поподробнее. Начнем с программ – червей и вирусов. Что же это такое?	Вирусы - это вредоносные программы, обладающие способностью к несанкционированному пользователем саморазмножению в компьютерах или компьютерных сетях, при этом полученные копии также обладают этой возможностью.		
Хорошо, как мы можем защитить себя от воздействия подобных программ?	Использовать антивирусные программы		
А какие вы знаете?	Dr Web, Avast, Kaspersky Internet Security, Eset NOD32, Comodo Antivirus.		

Как вы думаете, какие программы называют программами троянами?	Программы-трояны - вирусы, имитирующие полезные программы для уничтожения данных, повреждения компьютера и похищения личных сведений.		
А теперь скажите мне, с какими программами троянами вы в своей жизни сталкивались? Слышали о таковых?	Блокировщик WINDOWS, шифратор данных и тд		
А что вы скажете о программах шпионах? Сталкивались ли вы с ними? Какие проблемы они могут доставить пользователю?	Программы-шпионы (Spyware) – это общее название для программного обеспечения, осуществляющего сбор информации на компьютере без согласия пользователя.		

А как мы можем защитить свой компьютер от подобных программ? всей матрицы.	Мы можем использовать программы анти-шпионы.		
Этап 5. Домашнее задание, рефлексия 1 мин			
Что такое информационная безопасность? Какие вирусы вы знаете? Какие виды вирусов существуют? С помощью каких программ мы можем себя обезопасить от вирусов? Домашнее задание: Выучить конспект			

Разработка урока по теме «Основные угрозы безопасности подросткам с сети Интернет»

ПЛАН-КОНСПЕКТ УРОКА

Предмет: Информатика и ИКТ.

Класс: 8.

Тема урока: Основные угрозы безопасности подросткам в сети Интернет.

Учитель Губанов Е.А.

Дата:

Тип урока: Объяснение и первичное закрепление знаний.

Цель урока: Знакомство с угрозами, которые могут нанести ущерб психологическому здоровью учеников.

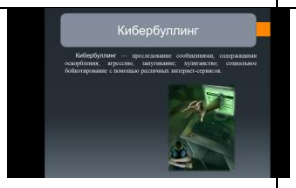
Формы работы:

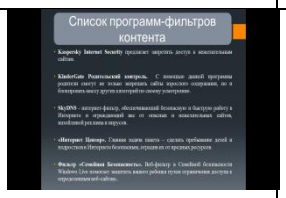
- Актуализация знаний – фронтальная работа
- Объяснение нового материала - лекция

Задачи

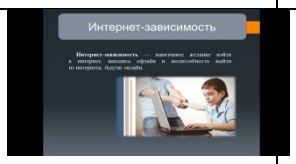
- *Образовательная:*
    - Дать ученикам представление о средствах защиты их персональных данных
    - Познакомить учащихся с понятиями информационной безопасности
    - Научить пользоваться антивирусными программами
- *Развивающая:*
    - развивать алгоритмическое мышление учащихся, развивать мировоззрение;
    - развитие таких познавательных процессов, как восприятие, внимание, память.
- *Воспитательная:*
    - воспитывать устойчивый познавательный интерес к информационным технологиям через показ практического применения темы;
    - воспитывать такие качества личности, как активность, самостоятельность и аккуратность в работе;
    - воспитывать у учащихся стремление к реализации себя в обществе и общении.

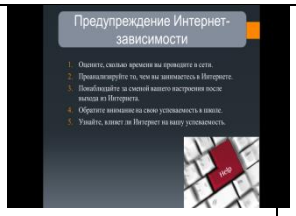
Ход урока:

Деятельность учителя	Деятельность учащихся	Интерактивная доска	Тетрадь
Этап 1. Организационный момент 1 мин			
Приветствие. Здравствуйте, сегодня мы с вами поговорим об основных угрозах в сети Интернет.			
Этап 2 Объяснение нового материала 35 мин			
Какие основные угрозы в сети Интернет вы знаете? С какими вы или ваши родственники, или знакомые сталкивались? ?	Киберхулиганы, неприличный контент, интернет-зависимость. Записывают число и тему урока.		
Давайте теперь подробнее рассмотрим эти угрозы. Что же такое киберхулиганство (кибербуллинг)?	Кибербуллинг — преследование сообщениями,		

	содержащим и оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.		
Все мы, рано или поздно, сталкиваемся с неприличным контентом в интернете, он отрицательно влияет на психику подростков. Существуют способы фильтрации этого контента. Какие из них вы знаете?	**Kaspersky Internet Security** предлагает запретить доступ к нежелательным сайтам. **KinderGate. Родительский контроль.** С помощью данной программы родители смогут не только запрещать сайты взрослого содержания, но и		

	блокировать массу других категорий по своему усмотрению. **SkyDNS** - интернет-фильтр, обеспечивающий безопасную и быструю работу в Интернете и ограждающий вас от опасных и нежелательных сайтов, назойливой рекламы и вирусов. **«Интернет Цензор».** Главная задача пакета – сделать пребывание детей и подростков в Интернете безопасным, оградив их от вредных ресурсов. Фильтр «Семейная Безопасность		

	». Веб-фильтр в Семейной безопасности **Windows Live** помогает защитить вашего ребенка путем ограничения доступа к определенным веб-сайтам.		
А что вы можете сказать об интернет зависимости? Сталкивались ли вы с этим?	Интернет – зависимость - это навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн.		

Есть ли у вас Интернет – зависимость? Давайте узнаем, ответим на эти простые вопросы себе. 1) Сколько времени вы проводите в сети? 2) Чем вы занимаетесь в сети Интернет? 3) Как меняется ваше настроение, после того, как вы выходите из Интернета? 4) Как влияет интернет на вашу успеваемость в школе? Теперь давайте сделаем выводы, есть ли у вас интернет зависимость или нет. Что скажете?	Да есть. / Нет, нету.		
Для того чтобы сеть Интернет для вас была безопасна, нужно соблюдать некоторые правила, а именно: 1) Будьте ответственны в сети! 2) Не распространяйте опасные и вредоносные файлы, сообщения, изображения и другой потенциально опасный контент! 3) Делись изображениями с людьми, которым вы доверяете! 4) Научитесь блокировать незнакомых людей и нежелательные контакты!	Блокировщик WINDOWS, шифратор данных и тд		

5) Не открывайте подозрительные ссылки, даже от ваших друзей и родственников, их аккаунты могут быть взломаны! 6) Будьте осторожны при встрече с людьми, с которыми вы познакомились в сети Интернет! 7) Необходимо выбирать надежный пароль для электронной почты и аккаунтов в ваших социальных сетях! 8) Меняйте пароли хотя бы раз в полгода, чтобы злоумышленники не смогли их подобрать !			
Этап 5. Домашнее задание, рефлексия 1 мин			
Какие существуют угрозы в сети Интернет? Что такое кибербуллинг? Как защитить себя от воздействия киберхулиганов? Назовите средства фильтрации нежелательного контента. Домашнее задание: Выучить конспект			