МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

ФИЗИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА ИНФОРМАТИКИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ИНФОРМАТИКЕ

Методика изучения темы «Информация» в школе в условиях реализации ФГОС ООО

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

«Информатика. Английский язык»

Проверка на объем заимствований:
72,55 % авторского текста

Работа рекомендована к защите
рекомендована/не рекомендована
«25» мая 20 18 г.
зав. кафедрой И, ИТ и МОИ
_____ Рузаков А.А.

Выполнила:
Студентка группы ОФ-513/093-5-1
Королева Яна Васильевна

Научный руководитель:
к.п.н., доцент кафедры ИИТиМОИ
_____
Носова Людмила Сергеевна.

Челябинск
2018

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

ФИЗИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА ИНФОРМАТИКИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ИНФОРМАТИКЕ

Методика изучения темы «Информация» в школе в условиях реализации ФГОС ООО

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

«Информатика. Английский язык»

Проверка на объем заимствований:
_____% авторского текста

Работа_____к защите
рекомендована/не рекомендована

«____»_____20___г.
зав. кафедрой И, ИТ и МОИ

_____Рузаков А.А.

Выполнила:
Студентка группы ОФ-513/093-5-1
Королева Яна Васильевна

Научный руководитель:
к.п.н., доцент кафедры ИИТиМОИ

_____
Носова Людмила Сергеевна.

Челябинск

2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В наше время упорного развития информационных технологий важным достижением любого человека является его умение качественно работать с информацией, его способность к анализу информации, а также к принятию обоснованных и своевременных решений на основе имеющейся информации. Этому надо учить, начиная с первых шагов в школе на уроках информатики.

Преподавание темы «Информация» на уроках информатики является ключевой, содержит базовые понятия предмета информатики. Без преподавания данной темы изучение дальнейшего материала является бессмысленным.

Одной из актуальных тем, связанных с информацией, является возрастающий уровень проблемы информационной безопасности, несмотря на развитие технологий для защиты информации. В условиях информатизации общества, всех его структур, высокая информационная культура, обеспечивающая информационную безопасность личности, является необходимостью для успешной деятельности в любой сфере. Поэтому детям нужно прививать знания об информационной безопасности со школы. Для изучения детьми информационной безопасности больше подходят факультативы.

Цель работы – разработка факультативного курса для обучения школьников информационной безопасности.

Объект исследования – методика преподавания темы «Информация» и процесс обучения школьников на факультативных занятиях по информационной безопасности.

Предмет исследования – разработка факультативного курса «Информационная безопасность».

Гипотеза исследования: если использовать разработанный курс в рамках факультатива «Информационная безопасность», то это повысит уровень знаний по информационной безопасности и сформирует умение работы с информацией.

Задачи исследования:

1. Изучить теоретические аспекты информации и информационной безопасности.
2. Изучить и проанализировать ФГОС по информатике, учебники по информатике и ИКТ для 5-9 классов.
3. Разработать факультативный курс «Информационная безопасность» для учащихся 7-9 классов.
4. Разработать программно-методическую поддержку факультативного курса в виде электронного пособия «Информационная безопасность».

ГЛАВА 1. ПРЕДСТАВЛЕНИЕ ТЕМЫ «ИНФОРМАЦИЯ» В ШКОЛЬНОМ КУРСЕ ИНФОРМАТИКИ

1.1. Понятие информации

Термин «информация» происходит от латинского слова «informatio», который означает сведения, разъяснения, изложение.

По российскому федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Статья 2): Информация – сведения (сообщения, данные) независимо от формы их представления [21].

Разнообразие информационных процессов и широкий интерес к ним в разных областях знаний породили много толкований и определений этого понятия, а также подходов к его определению. С точки зрения информационного взаимодействия объектов можно выделить следующие подходы: физический, сигнальный, лингвистический, семантический, прагматический. Первые три подхода направлены на количественное описание сложности объекта или явления. Четвертый – описывает содержательность и новизну передаваемого сообщения для получателя сообщения. Наконец, пятый вид обращает внимание на полезность полученного сообщения для пользователя [23].

Информация и ее свойства являются объектом исследования целого ряда научных дисциплин, таких как теория информации (математическая теория систем передачи информации), кибернетика (наука о связи и управлении в машинах и животных, а также в обществе и человеческих существах), семиотика (наука о знаках и знаковых системах), теория массовой коммуникации (исследование средств массовой информации и их влияния на общество), информатика (изучение процессов сбора, преобразования, хранения, защиты, поиска и передачи всех видов информации и средств их автоматизированной обработки) и ряде других [23].

В информатике наиболее часто используется следующее определение этого термина:

Информация – это осознанные сведения об окружающем мире, которые являются объектом хранения, преобразования, передачи и использования.

Основные виды информации по ее форме представления, способам ее кодирования и хранения, что имеет наибольшее значение для информатики, это [23]:

Графическая или изобразительная – первый вид, для которого был реализован способ хранения информации об окружающем мире в виде наскальных рисунков, а позднее в виде картин, фотографий, схем, чертежей на бумаге, холсте, мраморе и др. материалах, изображающих картины реального мира;

Звуковая – мир вокруг нас полон звуков и задача их хранения и тиражирования была решена с изобретение звукозаписывающих устройств в 1877 г.; ее разновидностью является музыкальная информация – для этого вида был изобретен способ кодирования с использованием специальных символов, что делает возможным хранение ее аналогично графической информации;

Текстовая – способ кодирования речи человека специальными символами – буквами, причем разные народы имеют разные языки и используют различные наборы букв для отображения речи; особенно большое значение этот способ приобрел после изобретения бумаги и книгопечатания;

Числовая – количественная мера объектов и их свойств в окружающем мире; особенно большое значение приобрела с развитием торговли, экономики и денежного обмена; аналогично текстовой информации для ее отображения используется метод кодирования специальными символами – цифрами, причем системы кодирования могут быть разными;

Видеоинформация – способ сохранения «живых» картин окружающего мира, появившийся с изобретением кино.

Существуют также виды информации, для которых до сих пор не изобретено способов их кодирования и хранения – это тактильная информация, передаваемая ощущениями, органолептическая, передаваемая запахами и вкусами и др.

Как и всякий объект, информация обладает свойствами. Характерной отличительной особенностью информации от других объектов права информации влияют как свойства исходных данных, составляющих ее содержательную часть, так и свойства методов, фиксирующих эту информацию.

С точки зрения информатики, наиболее важными представляются следующие общие качественные свойств [23]:

Субъективность информации. Информация существует только во взаимосвязи с субъектом, передающим эту информацию и зависит от человеческого сознания. Информация – это субъективное отражение внешнего объективного мира. Информация зависит от методов ее фиксации и оценки.

Достоверность информации. Информация достоверна, если она отражает истинное положение дел. Достоверная информация помогает принять нам правильное решение. Недостоверной информация может быть по следующим причинам:

Преднамеренное искажение (дезинформация) или непреднамеренное искажение субъективного свойства;

Искажение в результате воздействия помех («испорченный телефон») и недостаточно точных средств ее фиксации.

Полнота информации. Информацию можно назвать полной, если ее достаточно для понимания и принятия решений. Неполная информация может привести к ошибочному выводу или решению.

Точность информации определяется степенью ее близости к реальному состоянию объекта, процесса, явления и т. п.

Актуальность информации – важность для настоящего времени, злободневность, насущность. Только вовремя полученная информация может быть полезна.

Полезность (ценность) информации. Полезность может быть оценена применительно к нуждам конкретных ее потребителей и оценивается по тем задачам, которые можно решить с ее помощью.

В средней школе понятие информация дается как такое определение: «Информация – это знания, получаемые вами в школе; сведения, которые вы черпаете из книг, телепередач; новости, которые вы слышите по радио или от других людей» [5]. Далее информация изучается более подробно, изучаются виды и свойства информации, также понятие «информация для человека» и как человек воспринимает информацию.

1.2. Понятие информационной безопасности

Термин «информационная безопасность» появился с развитием информационных технологий, вычислительной техники и ЭВМ. Словосочетание «информационная безопасность» в разных контекстах может подразумевать различный смысл. Ниже приведены два широко распространенных определения информационной безопасности.

Информационная безопасность – это состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [4].

Информационная безопасность – защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре [11].

В Доктрине информационной безопасности Российской Федерации от 5 декабря 2016 г. № 646 под термином «информационная безопасность» понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства [16].

Само понятие информационной безопасности базируется на трех основных положениях: доступность, целостность и конфиденциальности информации. Под «доступностью» понимается обеспечение доступа к информации. «Целостность» – это обеспечение достоверности и полноты информации. «Конфиденциальность» подразумевает под собой обеспечение доступа к информации только авторизованным пользователям [1].

Информационная безопасность включает в себя безопасность используемого ПО, безопасность аппаратных и технических средств и многое другое. Обеспечение информационной безопасности включает перечень мероприятий и образует систему обеспечения информационной безопасности.

Субъекты информационных отношений заинтересованы в обеспечении своей информационной безопасности, а именно: своевременного доступа к необходимой информации и автоматизированным службам; достоверности информации; конфиденциальности информации и ее целостности; защиты от дезинформации (навязывания им ложной информации) и т.д. [1].

Ущерб субъектам информационных отношений может быть нанесен не только со стороны локальных и глобальных сетей, но и через определенную информацию с носителей. Поэтому в качестве объектов, подлежащих защите в целях обеспечения безопасности информационных отношений должны рассматриваться информация, любые носители, средства хранения и процессы ее обработки [1].

1.3. Особенности изучения темы «Информация» в средней школе

Анализ ФГОС основного общего образования позволил выдвинуть требования к выпускникам по изучению темы «Информация» [18]:

На базовом уровне выпускник должен:

- Знать научное представление об информации, информационных процессов;
- Знать виды информационных процессов;
- Уметь работать с различными видами информации с помощью компьютера и других средств информационных и коммуникационных технологий;
- Уметь избирательно относиться к полученной информации;
- Уметь оперировать различными видами информационных объектов, в том числе с помощью компьютера;
- Уметь структурировать информацию.

На углубленном уровне выпускник должен:

- Уметь выделять информационный аспект в деятельности человека; информационное взаимодействие в простейших социальных, биологических и технических системах;
- Уметь организовывать собственную информационную деятельность и планировать ее результаты;
- Использовать приобретённые знания и умения в практической деятельности и повседневной жизни для поиска и отбора информации, в частности, связанной с личными познавательными интересами, самообразованием и профессиональной ориентацией.

Тема «Информация» в основной школе начинается изучаться с пятого класса и в дальнейшем продолжает более подробно раскрываться в 7 и 9 классах.

Подход к понятию информации, которое является ключевым в данной теме, в школьных учебниках неоднозначный. Одна из причин такой сложившейся ситуации – сложность самого понятия информации. Понятие «информация» относится к числу фундаментальных для всей науки и носит общенаучный, а также философский характер, поэтому данное понятие является предметом постоянных дискуссий.

Выбор учебника по информатике, где присутствует тема «Информация», также играет большую роль при изучении понятия информации. Например, в учебнике 7 класса по информатике Босовой Л.Л. объясняется понятие информации и информации для человека, а в учебнике 7 класса по информатике и ИКТ Семакина И.Г. дополнительно рассматривается философский подход к понятию информации [6, 7].

В таблице 1 приведен результат анализа учебников, рекомендованных министерством образования на 2017-2018 гг, и их содержание, связанное с темой «Информация»: Босова Л.Л., Семакин И.Г., Угринович Н.Д., Быкадоров Ю.А. [5-8].

Таблица 1

Анализ учебников по теме «Информация»

Учебник	Тема	Аннотация
Информатика. Учебник для 5 класса. Босова Л.Л.	§ 1. Информация вокруг нас	
	Как человек получает информацию	Объясняется само понятие информации и как человек получает информацию.
	Виды информации по форме представления	Представляются виды информации по способу получения.
	Действия с информацией	Действия человека с информацией,

		связанные с получение, передачей, хранением и обработкой информации (более подробно эти действия расписаны в параграфах «Хранение информации», «Передача информации», «Обработка информации»)
Информатика. Учебник для 7 класса. Босова Л.Л.	Глава 1. Информация и информационные процессы	
	§1.1 Информация и ее свойства	
	1.1.1. Информация и сигнал	Объясняется понятие информации и информации для человека, а также классификация сигналов (сообщений), воспринимаемых человеком как информация.
	1.1.2. Виды информации	Разъясняются виды информации, по способу восприятия человеком.
	1.1.3. Свойства информации	Приводятся свойства информации, а

		также субъективные характеристики информации, зависящие от личности получателя информации и обстоятельств получения информации: важность, своевременность, достоверность, актуальность и т.п.
Информатика и ИКТ. 7 класс. Семакин И.Г. и др.	Глава 1. Человек и информация.	
	§ 1. Информация и знания.	Объясняется понятие информации для человека. Рассматривается философский подход к понятию информации.
	§ 2. Восприятие и представление информации.	Объясняется с помощью каких органов чувств человек получает информацию, формы представления информации.
	§3Информационные процессы	В данном параграфе рассказывается об основных информационных

		процессах: хранение, передача, обработка информации.
Информатика и ИКТ. Учебник для 8 класса. Угринович Н.Д.	Глава 1. Информация и информационные процессы.	
	1.1. Информация в природе, обществе и технике	
	1.1.1. Информация и информационные процессы в неживой природе.	Рассматривается переход от хаоса к порядку (увеличение информации) в окружающем мире.
	1.1.2. Информация и информационные процессы в живой природе.	Рассматриваются переход от хаоса к порядку (увеличение информации) в живой природе; получение, передача и использование информации живыми организмами.
	1.1.3. Человек: информация и информационные процессы.	Способы восприятия информации человеком органами чувств, информация в форме сообщений и знаний, субъективные характеристики информации, зависящие от личности получателя

		информации и обстоятельств получения информации: важность, своевременность, достоверность, актуальность и т.п.
	1.1.4. Информация и информационные процессы в технике.	Связь с информационными процессами функционирования систем управления техническими устройствами, как роботы могут воспринимать информацию.
Информатика и ИКТ. 8 класс. Быкадоров Ю.А.	Глава 1. Компьютер и информация.	
	§ 3. Информация в природе и обществе	Рассматривается роль информации в живой природе, в жизни человека и общества.
	§ 4. Содержание и форма представления информации	Рассматривается, как человек воспринимает информацию, основные формы представления информации.

	§ 5. Информационные процессы.	Информационные процессы: хранение, передача, обработка информации. Различные способы хранения информации.
	§ 6. Язык как способ представления информации	Рассматриваются естественные, формальные и искусственные языки для передачи, хранения информации.

Как видно в средней школе, начиная с 5 класса, тема «Информация» изучается с нуля, то есть даются понятие информации, виды информации и действия человека с информацией. В 7 и 8 классах данная тема рассматривается более подробно, то есть дополнительно изучаются свойства информации, информационные процессы, восприятие человеком информации и языки как способы сохранения и передачи информации.

1.4. Особенности курса в средней школе

В XXI веке, во времена информатизации общества человека окружает большой объем информации. Каждый день человеку приходится получать все новую и новую информацию, но не всегда эта информация является актуальной и достоверной. Поэтому в связи с нарастающим процессом активного использования информационных ресурсов особое значение приобретает информационная безопасность для детей и подростков. Таким образом на уроках информатики или в рамках школьного курса ставится цель просвещения детей в части использования различных информационных ресурсов, знания правил отбора достоверной информации и ее использования, которая способствует развитию системы защиты прав несовершеннолетних в информационной среде и их нормальному развитию.

Обеспечение государством информационной безопасности детей во всех ресурсах, предоставляющих информацию – требование международного права. Международные стандарты в области информационной безопасности детей отразились в российском законодательстве. Федеральный закон Российской Федерации № 436-ФЗ от 29 декабря 2010 года «О защите детей от информации, причиняющей вред их здоровью и развитию» регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и развитию, в том числе от такой информации, содержащейся в информационной продукции. Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью, физическому, психическому, духовному и нравственному развитию [22].

Федеральный закон Российской Федерации от 21 июля 2011 г. № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», направленный на защиту детей от разрушительного, травмирующего их психику

информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки. Закон запрещает размещение рекламы в учебниках, учебных пособиях, другой учебной литературе, предназначенных для обучения детей, а также распространение рекламы, содержащей информацию, запрещенную для распространения среди детей, в детских образовательных организациях [20].

Незнание законов об информационной безопасности и мер безопасности в Интернете, а также неумение обезопасить себя от деструктивной информации может привести к необратимым последствиям. Особенно это актуально сейчас, в век информационного прогресса современный ребенок живет в мире, где постоянно увеличиваются темпы роста информации. Главная роль для распространения информации теперь принадлежит глобальным сетям. В Интернете на ребенка оказывать влияние может любой человек, группы людей, а также организации. Средства влияния и возможности виртуального воздействия постоянно усиливаются и усложняются.

Всероссийское исследование «Дети России онлайн», проведенное в 2013 г. в рамках проекта EU Kid Online II, охватившее 1025 детей в возрасте от 9 до 16 лет и 1025 их родителей из одиннадцати разных регионов России, выявило более рискованное и, следовательно, более беззащитное поведение российских школьников в Интернете, нежели у их сверстников, живущих в развитых европейских странах. Среди особенностей использования интернет-технологий можно обозначить следующие [25]:

– дети в России начинают впервые осваивать Интернет в возрасте 8-10 лет;

– 70% школьников ежедневно пользуются Интернетом, 56% выходят в сеть с мобильных устройств и компьютера в своей комнате, 26% проводят более 2-3 часов в Сети каждый день;

– дети часто встречают опасный контент (например, почти треть опрошенных детей сталкивались за последний год с изображениями сексуального характера в Интернете);

– не все родители достаточно осведомлены о существующих рисках в Интернете и способах защиты от них, многие зачастую недооценивают проблему безопасности.

Исходя из результатов исследования, можно выявить острую необходимость в просвещении школьников по информационной безопасности в рамках дополнительного курса в средней школе, так как в этом возрасте дети начинают более активно пользоваться различными Интернет-ресурсами, а в рамках учебной программы по информатике невозможно полностью освятить данную проблему из-за того, что в учебной программе по информатике не предусмотрено детальное освещение темы по информационной безопасности. Поэтому главная задача преподавателя информатики по данному вопросу – это объяснить школьникам, как обезопасить себя при проведении своего времени в Интернете и проверять достоверность полученной информации только в рамках школьного курса.

Все выше перечисленные особенности в какой-то степени влияют на планирование, подготовку и ход проведения занятия. Главной задачей учителя информатики основной школы является особое внимание ко всем составляющим: возрастные особенности школьников, тематика внеклассного занятия и способы подачи материала для большего проявления интереса учащихся к данному курсу. Только все в совокупности может привести к продуктивной деятельности школьника во время внеурочной деятельности.

1.5. Анализ программных средств обучения

Для повышения грамотности школьников по информационной безопасности были разработаны Интернет-ресурсы, которые в игровой форме объясняют детям основы безопасного времяпровождения в Интернете. Такие ресурсы можно использовать в рамках курса по информационной безопасности.

Перечислим некоторые из них:

1. Прогулка через Wild Web Woods (Дикий Интернет Лес). Данная онлайн-игра была разработана в рамках программы Совета Европы «Строим Европу для детей и вместе с детьми» и призвана помочь детям в возрасте от 8 до 13 приобрести навыки правильного использования Интернета в личных целях. Игра также направлена на то, чтобы помочь детям узнать о правах человека, свои собственные права, а также как уважать права других, к тому же эта онлайн-игра поможет детям приобрести достаточные знания для защиты от домогательств и насилия в виртуальном мире.

Цель игры – попасть игровому персонажу в электронный город. Для того чтобы попасть в этот электронный город, персонажу нужно пройти через Дикий Интернет Лес, где расположены четыре города, через которые нужно и собрать монеты, позволяющие перейти на следующий уровень. Каждый раз, когда игроки получают монету, им предоставляется важная информация о компьютерной безопасности и правах детей [12].

Рис. 1 Прогулка через Wild Web Woods (Дикий Интернет Лес)

2. Интерактивная онлайн-игра «Путешествие на Астерикс». Данная игра разработана для проекта «Разбираем Интернет», в котором рассказывается об устройстве электронного мозга сетевого пространства. Игра подходит для школьников в возрасте 14-16 лет. При прохождении игры, школьник может проверить свои знания в получении доступа к знаниям, нахождении нужной информации, критически оценивании контента, общении в Интернете, но при этом соблюдая правила безопасности. В ходе игры персонаж собирает баллы, которые могут открыть дополнительные возможности игры [13].

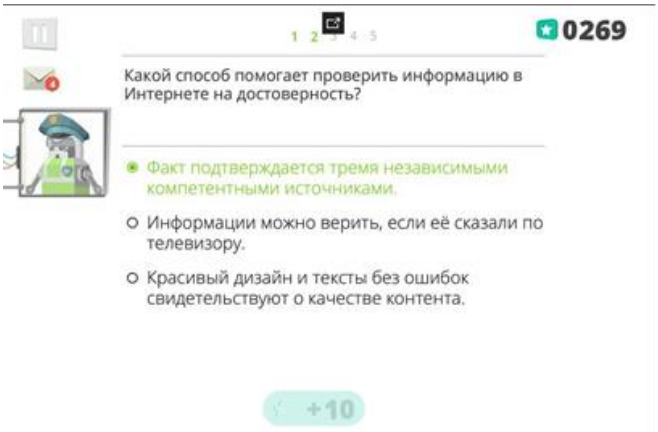


Рис. 2 Путешествие на Астерикс

3. Интерактивный рассказ «Римская группа» для детей 11-16 лет разработана для рассмотрения вопросов авторского права, защиты компьютера и значение паролей в личной безопасности. В рассказе ведется повествование о девушке Эмме, которая получает сценарий от неизвестного друга по чату. А дальше история ведет к необычному повороту [14].

Рис. 3. Римская группа

4. Сборник интерактивных рассказов для учеников 11-16 лет «Конфликты и происшествия» – это сборник, в котором рассматриваются вопросы достоверности информации в Интернете, ответственности, связанной с публикаций фотографий и текстов, а также вопросы знакомства с пользователями в Интернете и одноранговых сетях [10].

Рис. 4 Конфликты и происшествия

Исходя из анализа программных средств обучения информационной безопасности можно сделать вывод, что у каждой программы есть свои достоинства в предоставлении материала. Но следует сказать, что каждый из этих программных средств помогает при изучении определенных тем в курсе информационной безопасности и является игровым, что необходимо для повышения интереса учащихся при прохождении данного курса.

ВЫВОДЫ ПО ГЛАВЕ 1

В данной главе были рассмотрены основные теоретические сведения понятия информации и информационной безопасности, а также особенности изучения темы «Информации» в средней школе и как данная тема представлена в учебниках по информатике в средней школе.

В ходе данной главы был проанализирован ряд программных средств для изучения темы «Информационная безопасность» в средней школе: Прогулка через Wild Web Woods (Дикий Интернет Лес), Путешествие на Астерикс, Римская группа, Конфликты и происшествия [10, 12-14].

Рассмотренный в первой главе теоретический минимум служит основной составляющей разработки курса «Информационная безопасность» в средней школе для внеклассного обучения.

ГЛАВА 2. РАЗРАБОТКА ФАКУЛЬТАТИВНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОТЬ»

2.1. Анализ нормативных документов

Федеральные государственные образовательные стандарты (ФГОС) представляют собой совокупность требований, обязательных при реализации основных образовательных программ начального общего, основного общего, среднего (полного) общего, начального профессионального, среднего профессионального и высшего профессионального образования образовательными учреждениями, имеющими государственную аккредитацию.

Федеральные государственные образовательные стандарты обеспечивают:

1) единство образовательного пространства Российской Федерации;

2) преемственность основных образовательных программ;

3) вариативность содержания образовательных программ соответствующего уровня образования, возможность формирования образовательных программ различных уровня сложности и направленности с учетом образовательных потребностей и способностей обучающихся [19].

В ходе подготовки курса для 7-9 классов был проанализирован ФГОС основного общего образования.

ФГОС ООО устанавливает требования к результатам освоения основной образовательной программы основного общего образования:

Метапредметные результаты:

формирование и развитие компетентности в области использования информационно-коммуникационных технологий.

Предметные результаты:

Изучение предметной области «Информатика» должно обеспечить:

- осознание значения информатики в повседневной жизни человека;

- понимание роли информационных процессов в современном мире.

В результате изучения предметной области «Информатика», обучающиеся получают представление об основных информационных процессах в реальных ситуациях [18].

Предметные результаты изучения предметной области «Информатика» должны отражать [18]:

- формирование информационной и алгоритмической культуры; формирование представления о компьютере как универсальном устройстве обработки информации; развитие основных навыков и умений использования компьютерных устройств;
- формирование умений формализации и структурирования информации, умения выбирать способ представления данных в соответствии с поставленной задачей – таблицы, схемы, графики, диаграммы, с использованием соответствующих программных средств обработки данных;
- формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

Из анализа ФГОС следует вывод о том, что тема «Информационная безопасность» не представлена.

Из анализа примерной программы учебного предмета «Информатика» видно, что идет направление на развитие навыков использования компьютерных устройств.

Предмет «Информатика» на базовом уровне в ФГОС среднего общего образования призван сформировать [17]:

– представление о роли информации и информационных процессов в социальных, биологических и технических системах;

– владение алгоритмическим мышлением, понимание необходимости формального описания алгоритмов;

– владение умением понимать программы, написанные на выбранном для изучения универсальном алгоритмическом языке высокого уровня; знание основных конструкций программирования (ветвление, цикл, подпрограмма);

– владение стандартными приемами написания на алгоритмическом языке программы для решения стандартной задачи с использованием основных конструкций программирования; отладки таких программ; использование готовых прикладных компьютерных программ по выбранной специализации;

– представление о компьютерно-математических моделях и необходимости анализа соответствия модели и моделируемого объекта (процесса), о способах хранения и простейшей обработке данных; понятие о базах данных и средствах доступа к ним; умение просматривать, создавать, редактировать, сохранять записи в базах данных, получать необходимую информацию по запросу пользователя;

– владение компьютерными средствами представления и анализа данных (электронные таблицы, средства построения графиков и диаграмм, гипертекст, мультимедиа);

– навыки и умения по соблюдению требований техники безопасности, гигиены, эргономики и ресурсосбережения при работе со средствами информатизации; понимание основ правовых аспектов использования компьютерных программ и работы в сети Интернет.

Анализ УМК по информатике и ИКТ для ФГОС ООО на предмет изучения информационной безопасности позволяет сделать вывод о том, что на уровне основного общего образования в рамках предмета «Информатика» акцент в соответствии с требованиями ФГОС делается на формировании навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

В УМК по предмету «Информатика» 7-9 класс, автором которого является Угринович Н. Д. информационная безопасность рассматривается в теме «Информационное общество и информационная безопасность». Всего на нее уделяется 3 часа: 1 час в 7 классе и 2 часа в 9 классе [24].

В содержание данной темы, при ее изучении в 9 классе, входят: Информационное общество. Информационная культура. Перспективы развития информационных и коммуникационных технологий. Правовая охрана программ, данных и информации. Защита информации. Лицензионные, условно бесплатные и свободно распространяемые программы.

В поурочном планировании для учебника 7 класса по информатике под авторством Угриновича Н.Д. в конце изучения главы «Коммуникационные технологии» дается 1 час для изучения темы «Личная безопасность в сети Интернет», которое может быть проведено в виде итогового семинарского занятия [24].

Таблица 2

Анализ учебника по информатике Н.Д. Угринович 9 кл.

№	**Раздел**	**Тема**	**Основные понятия**	**Практикум**
1.	Информационное общество и информационная безопасность	Информационное общество	Доиндустриальное, индустриальное, информационное общество	
		Информационная культура	Информационная и коммуникативная культура.	

		Правовая охрана программ и данных	Авторское право, электронная подпись.	Ознакомиться с законом «Об электронной подписи» и частью 4 Гражданского кодекса Российской Федерации

В УМК «Информатика»7-9 класс, автором которого является Босова Л.Л. формируются такие предметные результаты, как формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права, при изучении тем в 7 классе «Всемирная паутина» и «Программное обеспечение компьютера», а также в 9 классе при изучении темы «Информационные ресурсы и сервисы Интернета» [2].

Таблица 3

Анализ учебника по информатике Босовой Л.Л. 7 и 9 кл.

№	**Раздел**	**Тема**	**Основные понятия**	**Практикум**
7 класс				
1	Информация и информационные процессы	Всемирная паутина	WWW – Всемирная паутина, web-страница, web-сайт, браузер, поисковая система,	Найти в Интернете заданную информацию.

			поисковый запрос.	
2	Компьютер как универсальное устройство для работы с информацией	Программное обеспечение компьютера	Антивирусная система.	Ответить на вопросы с помощью сети Интернет.
9 класс				
3	Коммуникационные технологии	Информационные ресурсы и сервисы Интернета	Всемирная паутина, электронная почта, форум, телеконференция, чат, социальная сеть, логин, пароль.	

В УМК «Информатика» 7-9 класс, под авторством Семакина И.Г. и др. аспекты информационной безопасности рассматриваются в 7 и 9 классах в рамках тем «Компьютер: устройство и программное обеспечение» и «Информационные технологии и общество». В содержание темы «Компьютер: устройство и программное обеспечение» входят: использование антивирусных программ, а в содержание темы «Информационные технологии и общество»: проблемы безопасности информации, этические и правовые нормы в информационной сфере [15].

Таблица 4

Анализ учебника по информатике Семакин И.Г. и др. 7 и 9 кл.

№	**Раздел**	**Тема**	**Основные понятия**	**Практикум**
7 класс				

1	Компьютер: устройство и программное обеспечение	О системном ПО и системах программирования	Операционная система, антивирусная программа, система программирования.	
9 класс				
3	Информационные технологии и общество	Информационная безопасность	Информационное общество, информатизация, задачи информатизации.	Подготовить сообщение по каким признакам можно судить о наступлении эпохи информационного общества.

Таким образом, анализ показал, что все авторские коллективы УМК по информатике уделяют внимание вопросам по информационной безопасности, в основном аспектам безопасного поведения в Интернете и защите от компьютерных вирусов. В основном такие уроки запланированы авторами в начале 7 класса и в конце 9 класса. А в 5, 6, 8 классах эта тема отсутствует, однако именно в возрасте 12 лет дети становятся активными участниками сетевых сообществ и ведут активную деятельность в Интернете. Поэтому на этом этапе необходимо рассказывать им о защите персональных данных, о признаках компьютерной зависимости, о мошенничестве в Интернете и т.д. Поэтому выявляется острая необходимость введения дополнительного курса по информационной безопасности в средней школе.

2.2. Факультативный курс «Информационная безопасность»

Пояснительная записка

В настоящее время происходит глобальное развитие процесса информатизации общества, который, охватывая все страны мира, приводит к формированию новой информационной среды и профессиональной деятельности. Но при этом пропорционально разрастается уязвимость личных данных, а также общественных и государственных информационных ресурсов.

Таким образом, проблема обеспечения информационной безопасности становится актуальной на сегодняшний день. Решение данной проблемы невозможно как без достаточного количества высококвалифицированных профессионалов в области информационной безопасности, так и обычных пользователей, компетентных в сфере информационной безопасности.

Важнейшей составляющей обеспечения личной безопасности человека является его защита от поступающей к нему информации. Человек должен уметь защищаться от возможных информационных атак и манипуляций. Поэтому существует острая необходимость в организации информационного образования, который должен обеспечить формирование информационной культуры и информационной безопасности личности и общества в целом.

Формируя информационную безопасность человека необходимо выработать систему, при которой личность сможет защититься от возможных информационных манипуляций, а также воспитать чувство ответственности за распространение и производство любой информации, понимание ее последствий, а также ее влияния на личность и общество.

Актуальность проблемы воспитания информационной безопасности обусловлена необходимостью получения знаний, навыков и умений, которыми должен владеть каждый человек в современном мире в условиях глобальной информатизации общества.

Факультативный курс «Информационная безопасность» разработан для расширения кругозора и повышения уровня знаний и умений в безопасности учащихся в Интернете и окружающей его информационной среде.

Данная программа курса предназначена для учащихся 7-9 классов с базовым уровнем знаний, умений и навыков.

Объем курса составляет 17 часов.

Предложенный материал дополняет предмет «Информатика» и способствует формированию информационной безопасности личности, а также созданию условий для повышения готовности подростков к сознательному, профессиональному и культурному самоопределению в целом.

Цель курса – содействие формированию компетенций по безопасному использованию различных информационных ресурсов среди учащихся.

Задачи программы:

- повысить уровень информационной компетентности подростков;
- сформировать: информационную, коммуникативную, потребительскую и техническую компетентности;
- научить способам защиты информации;
- расширить представление о законодательстве Российской федерации в области защиты информации и авторского права;
- сформировать навыки ответственного поведения в сети Интернет с целью обеспечения информационной безопасности;

Формы проведения занятий: беседы, беседы с элементами дискуссий, работа в малых группах, практические работы.

Форма итогового контроля: проект.

Перед данным элективным курсом ставятся следующие задачи:

Образовательные:

- освоение учащимися знаний об информационной безопасности и их систематизации;

Развивающие:

- повышение интереса учащихся к изучению предмета «Информатика»;
- развитие у учащихся способностей к научно-исследовательской деятельности;

Воспитательные:

- воспитание у учащихся культуры в области применения информационных технологий в различных сферах современной жизни;
- воспитание у учащихся установки на позитивную социальную деятельность в информационном обществе, недопустимость действий, нарушающих правовые и этические нормы работы с информацией.

Ожидаемые результаты обучения

После прохождения курса «Информационная безопасность» учащиеся должны:

знать:

- понятие и угрозы информационной безопасности;
- уровни и меры защиты информации;
- правовые акты и нормы по защите информации и авторского права;
- принципы и приемы Интернет-безопасности;
- требования безопасного использования информационных ресурсов, в том числе и информационных ресурсов сети Интернет.

уметь:

- грамотно использовать возможности программного обеспечения для снижения рисков от несанкционированного доступа и от вирусного заражения компьютера;
- применять на практике меры профилактики и защиты информации;
- получать, обрабатывать, анализировать и прогнозировать полученную информацию.

Таблица 5

Учебно-тематический план

Номер урока	Тема урока	Количество часов	В том числе	
			Теория	Практика
Введение в информационную безопасность. Проблема информационной безопасности общества – 1 час.				
1	Введение в информационную безопасность.	1	1	
Угрозы информационной безопасности. Классы угроз информационной безопасности – 1 час.				
2	Виды и источники угроз	1	0,5	0,5
Вредоносные компьютерные программы. Методы профилактики и защиты от них– 2 часа.				
3	Вирусы как угроза информационной безопасности	1	0,5	0,5
4	Методы защиты компьютеров от вредоносных программ	1	0,5	0,5
Правовые основы по обеспечению информационной безопасности – 2 часа				

5	Организационные законы и правовые акты в области защиты информации	1	0,5	0,5
6	Защита информации ограниченного доступа	1	0,5	0,5
Современные методы защиты информации в автоматизированных системах обработки данных – 4 часа.				
7	Идентификация и аутентификация.	1	0,5	0,5
8	Аппаратные средства по защите информации	1	0,5	0,5
9	Криптографические алгоритмы шифрования данных	1	0,5	0,5
10	Симметричный или асимметричный криптографический алгоритм	1	0,5	0,5
Технические и организационные методы хранения информации – 1 час.				
11	Программные средства защиты информации	1	1	
Защита информации в компьютерных сетях – 4 часа.				
12	Защита информации в компьютерных сетях	1	0,5	0,5
13	Безопасность в сети Интернет	1	0,5	0,5
14	Способы отделения интрасети от глобальных сетей	1	0,5	0,5
15	Программные средства по защите информации Firewall	1	0,5	0,5

Проблемы информационно–психологической безопасности личности –2 часа				
16	Информационно–психологическая безопасность личности в информационном обществе	1	0,5	0,5
17	Проектная работа «Безопасный интернет в каждый дом»	1		1
Итого:		17	9	8

Поурочное планирование курса

Урок 1. Введение в информационную безопасность.

Тип урока: урок усвоения новых знаний.

Цель урока: формирование представления об информационной безопасности

Задачи:

Образовательная: Знакомство с понятиями информации и информационной безопасности; с современными методами защиты информации.

Развивающая: Развитие познавательного интереса.

Воспитательная: Воспитание у учащихся интереса к предмету. Воспитание информационной культуры, коммуникационных качеств личности;

Основные понятия: Информационная безопасность, нарушитель информационной безопасности, защита информации, доступность, целостность, конфиденциальность информации

Краткое содержание урока: В ходе урока даются определения таким понятиям, как «информация», «информационная безопасность», «защита информации», «обнаружения угроз». Определяется смысл предупреждения возможных угроз и ликвидация последствий.

Вопросы для контроля:

1. Под информацией надо понимать?
2. В чем состоит сущность защиты информации?
3. Какие меры необходимо принимать для защиты информации?
4. Что такое «информационная безопасность» и «защита информации»?

Урок 2. Виды и источники угроз.

Тип урока: урок усвоения новых знаний.

Цель урока: создать условия для формирования у обучающихся представление о видах и источниках угроз.

Задачи:

Образовательная: Знакомство с понятием «компьютерные угрозы», а также с угрозами в сети и их источниками.

Развивающая: Развитие познавательного интереса.

Воспитательная: Воспитание у учащихся интереса к предмету.

Основные понятия: Угроза информационной безопасности, класс угроз информационной безопасности, канал несанкционированного доступа к информации, случайное воздействие, преднамеренное воздействие.

Краткое содержание урока: В ходе урока дается понятия о различных источниках угроз, классифицируется по способам воздействия на объекты, дается перечисление видов угроз.

Вопросы для контроля:

1. Какие источники внутренних угроз вы знаете?
2. Какие действия будут относиться к физическим угрозам информационной безопасности?
3. Какие действия будут относиться к программным? Приведите примеры.

Урок 3. Вирусы как угроза информационной безопасности.

Тип урока: урок усвоения новых знаний.

Цель урока: ознакомить учащихся с угрозами информационной безопасности, которые происходят из-за влияния компьютерных вирусов; изучить особенности и характерные черты компьютерных вирусов.

Задачи:

Образовательная: Знакомство с компьютерными вирусами, способами и формами распространения компьютерных вирусов.

Развивающая: Развитие познавательного интереса.

Воспитательная: Воспитание у учащихся аккуратности, добросовестному отношению к учебному труду.

Основные понятия: Компьютерный вирус, сетевые вирусы, файловые вирусы, загрузочные вирусы, файлово-загрузочные вирусы.

Краткое содержание урока: в ходе урока дается понятие «компьютерный вирус», перечисляются типы компьютерных вирусов и способы их распространения.

Вопросы для контроля:

1. Что такое «компьютерный вирус»?
2. Перечислите основные типы компьютерных вирусов.
3. Какие существуют антивирусные программы?
4. Как можно вылечить зараженный файл?

Урок 4. Методы защиты компьютеров от вредоносных программ.

Тип урока: комбинированный.

Цель урока: сформировать знания, умения и навыки о защите информации от вредоносных программ.

Задачи:

Образовательная: Знакомство с методами защиты информации от вирусов.

Развивающая: формирование компьютерную грамотность учащихся.

Воспитательная: Воспитание у учащихся информационной культуры, внимательности, дисциплинированности.

Основные понятия: Вредоносная программа, антивирусная программа, брандмауэр.

Краткое содержание урока: В ходе урока учащиеся изучают понятия «вредоносная программа», «антивирусная программа» и брандмауэр. После изучения теоретического материала учащиеся выполняют практическую работу по теме урока за компьютером.

Вопросы для контроля:

1. К каким последствиям может привести заражение компьютерными вирусами?
2. Назовите признаки заражения компьютера вирусом.
3. Что необходимо сделать в первую очередь в случае заражения компьютера вирусом?

Урок 5. Организационные законы и правовые акты в области защиты информации.

Тип урока: урок усвоения новых знаний.

Цель урока: ознакомить учащихся с основными видами правонарушений в информационной сфере.

Задачи:

Образовательная: Иметь представление о правовом обеспечении РФ и о четырех уровнях стандарта информационной безопасности РФ; понимать значение стандартов информационной безопасности РФ.

Развивающая: Развитие познавательного интереса у учащихся.

Воспитательная: Воспитание у учащихся информационной культуры.

Основные понятия: Защита информации, информационная безопасность, преступление, информационное законодательство РФ, информационное право.

Краткое содержание урока: В ходе урока учащиеся знакомятся с информационным законодательством РФ и с четырьмя стандартами информационной безопасности РФ. После ознакомления с законами и правовыми актами решают задачи на данную тему урока.

Вопросы для контроля:

1. Какие правонарушения в сфере информационных технологий вы знаете?
2. Что такое система информационного законодательства РФ?
3. Что такое «преступление»?
4. Что изучает информационное право?

Урок 6. Защита информации ограниченного доступа.

Тип урока: урок усвоения новых знаний.

Цель урока: ознакомить учащихся с понятием защиты информации, основными проблемами и средствами защиты информации.

Задачи:

Образовательная: познакомить учащихся с мерами защиты личной информации на ПК.

Развивающая: развитие умения обобщать и систематизировать знания.

Воспитательная: воспитание ответственного отношения к соблюдению этических и правовых норм информационной деятельности.

Основные понятия: коммерческая тайна персональные данные, профессиональная тайна, государственная служебная тайна, информация ограниченного доступа.

Краткое содержание урока: В ходе урока учащиеся знакомятся с информацией ограниченного доступа, после изучения теоретического материала выполняют практическую работу за компьютером по теме урока.

Вопросы для контроля:

1. В чем состоит различие между лицензионными, условно-бесплатными и бесплатными программами?
2. Как можно зафиксировать свое авторское право на программный продукт?
3. Почему компьютерное пиратство наносит ущерб обществу?
4. Какие существуют программные и аппаратные способы защиты информации?

Урок 7. Идентификация и аутентификация.

Тип урока: урок усвоения новых знаний.

Цель урока: ознакомить учащихся с содержанием и механизмами реализации сервисов безопасности «идентификация» и «аутентификация».

Задачи:

Образовательная: Знакомство с понятиями «идентификация» и «аутентификация», научить учащихся различать системы идентификации.

Развивающая: Развитие познавательного интереса.

Воспитательная: Воспитание у учащихся аккуратности, добросовестному отношению к учебному труду.

Основные понятия: Идентификация, аутентификация, авторизация.

Краткое содержание урока: В ходе урока учащиеся изучают понятия «идентификации», «аутентификации», «авторизации» и методы идентификации и аутентификации.

Вопросы для контроля:

1. Что такое идентификация и аутентификация?
2. Какие способы защиты информации от несанкционированного доступа существуют?

Урок 8. Аппаратные средства по защите информации.

Тип урока: Урок обобщение с применением ИКТ.

Цель урока: закрепить у учащихся умение обеспечивать защиту информации, используя паролирование и архивирование.

Задачи:

Образовательная: формирование представления учащихся о том, что паролирование и архивирование применяются при решении жизненно важных задач.

Развивающая: развитие навыков самостоятельной работы за компьютером.

Воспитательная: Воспитание у учащихся самостоятельности, добросовестному отношению к учебному труду.

Основные понятия: Аппаратные средства по защите информации.

Краткое содержание урока: В ходе урока учащиеся знакомятся с аппаратные средствами по защите информации и после изучения теоретического материала выполняют практическую работу для закрепления темы урока.

Вопросы для контроля:

1. Что нового вы узнал на уроке?
2. Какие можно защитить файл от несанкционированного доступа?

Урок 9. Криптографические алгоритмы шифрования данных

Тип урока: урок усвоения новых знаний.

Цель урока: ознакомить учащихся с назначением, методами шифрования данных.

Задачи:

Образовательная: познакомить учащихся с основными видами кодирования; сформировать умения шифрования и декодирования информации.

Развивающая: Развитие познавательного интереса у учащихся.

Воспитательная: Воспитание у учащихся познавательный интерес к изучению информатики, аккуратность, культуру общения.

Основные понятия: Криптография, шифрование, дешифровка, алгоритм шифрования.

Краткое содержание урока: В ходе урока учащиеся изучают краткую историю криптографии, понятиями «шифрование» и «дешифровка», алгоритмы шифрования. После изучения теоретического материала учащиеся решают задачи по кодированию информации с помощью алгоритмов шифрования.

Вопросы для контроля:

1. Что такое криптография?
2. Что такое алгоритм шифрования?
3. Как с помощью шифрования защищаются данные?

4. Какие бывают алгоритмы шифрования?

Урок 10. Симметричный или асимметричный криптографический алгоритм.

Тип урока: урок усвоения новых знаний.

Цель урока: ознакомить учащихся с симметричным или асимметричным криптографическими алгоритмами.

Задачи:

Образовательная: Знакомство с симметричным или асимметричным криптографическими алгоритмами.

Развивающая: Развитие познавательного интереса.

Воспитательная: Воспитание у учащихся аккуратности, добросовестному отношению к учебному труду.

Основные понятия: Симметричный и асимметричный криптографический алгоритм.

Краткое содержание урока: В ходе урока дается понятия симметричного и асимметричного криптографического алгоритмов, учащиеся знакомятся со стандартом ассиметричного шифрования RSA и выполняют практику по шифровке и расшифровке.

Вопросы для контроля:

1. Что такое ассиметричный криптографический алгоритм?
2. Что такое симметричный криптографический алгоритм?

Урок 11. Программные средства защиты информации.

Тип урока: урок усвоения новых знаний.

Цель урока: ознакомить учащихся с программными средствами защиты информации.

Задачи:

Образовательная: Знакомство с программными средствами защиты информации.

Развивающая: Развитие познавательного интереса.

Воспитательная: Воспитание у учащихся аккуратности, добросовестному отношению к учебному труду.

Основные понятия: Программные средства защиты информации, встроенные средства защиты информации, антивирусные программы.

Краткое содержание урока: В ходе урока учащиеся изучают программные средства защиты информации, а также как ими пользоваться.

Вопросы для контроля:

1. Какие источники программные средства защиты информации вы знаете?
2. Какие антивирусные программы вы знаете?
3. Что такое VPN и для каких целей используется?

Урок 12. Защита информации в компьютерных сетях.

Тип урока: урок повторение.

Цель урока: Создание условий для усвоения учащимися приемов и принципов защиты информации.

Задачи:

Образовательная: способствовать формированию у учащихся знаний о приемах и методах защиты информации во время транспортировки по электронным сетям; формировать умения применять знания на практике.

Развивающая: Развитие познавательного интереса.

Воспитательная: содействовать воспитанию организованности, внимательности, культуры общения в группе, самостоятельности.

Основные понятия: цифровая информация, несанкционированное воздействие, непреднамеренное воздействие, цифровая подпись, цифровой сертификат, приемы и принципы защиты информации.

Краткое содержание урока: В ходе урока учащиеся повторяют способы защиты информации в компьютерных сетях.

Вопросы для контроля:

1. Что такое цифровая подпись?
2. Что такое закрытый ключ?

3. Перечислите основные типы компьютерных вирусов.

Урок 13. Безопасность в сети Интернет.

Тип урока: урок усвоения новых знаний.

Цель урока: обеспечение информационной безопасности несовершеннолетних обучающихся путем привития им навыков ответственного и безопасного поведения в Интернете.

Задачи:

Образовательная: Знакомство с правилами ответственного и безопасного поведения в современной информационной среде.

Развивающая: Развитие познавательного интереса.

Воспитательная: Воспитание у учащихся познавательный интерес к изучению информатики, аккуратность, культуру общения.

Основные понятия: интернет, угроза, безопасность, информация, угроза информационной безопасности.

Краткое содержание урока: В ходе урока учащиеся знакомятся с безопасным поведением в Интернете и сетевой этикой.

Вопросы для контроля:

1. Какую информацию нельзя разглашать в Интернете?
2. Чем опасны социальные сети?
3. Что в Интернете запрещено законом?
4. Действуют ли правила этикета в Интернете?

Урок 14. Способы отделения интрасети от глобальных сетей.

Тип урока: урок усвоения новых знаний.

Цель урока: Поиск оптимального решения при построении интрасети.

Задачи:

Образовательная: сформировать знания о назначении, принципах построения и функционирования интрасети.

Развивающая: Развитие дружеского и делового общение учащихся в совместной работе.

Воспитательная: Воспитание у учащихся дисциплинированности, целеустремленности и трудолюбия.

Основные понятия: Интрасеть, глобальная сеть, компьютерная сеть.

Краткое содержание урока: В ходе урока учащиеся знакомятся с принципами построения и функционирования интрасети и поиском оптимального решение при построении интрасети.

Вопросы для контроля:

1. Что такое глобальная сеть?
2. Чем отличается интрасеть от глобальной сети?

Урок 15. Программные средства по защите информации Firewall

Тип урока: комбинированный урок.

Цель урока: формирования знаний учащихся по теме «Программные средства по защите информации Firewall».

Задачи:

Образовательная: Знакомство учащихся с межсетевым и сетевым экраном.

Развивающая: Развитие познавательного интереса к предмету.

Воспитательная: Воспитание у учащихся информационной культуры, внимательности, дисциплинированности.

Основные понятия: Межсетевой экран, сетевой экран, сеть.

Краткое содержание урока: В ходе урока учащиеся изучают межсетевой экран, особенно рассматривают Firewall. После изучения теоретического материала выполняют практическую работу для закрепления темы урока.

Вопросы для контроля:

1. Что такое Firewall?
2. Основная задача Firewall?
3. Перечислите виды Firewall?

Урок 16. Информационно–психологическая безопасность личности в информационном обществе.

Тип урока: комбинированный урок.

Цель урока: ознакомить учащихся с методами, которые могут обезопасить личность в информационном обществе.

Задачи:

Образовательная: Знакомство с понятиями «информационное общество», а также с методами информационно–психологической безопасности личности.

Развивающая: Развитие познавательного интереса учащихся к предмету.

Воспитательная: Воспитание у учащихся информационной культуры.

Основные понятия: Информационное общество, информационная революция.

Краткое содержание урока: В ходе урока учащиеся изучают информационное общество, с его особенностью и характеристиками, а также с методами информационно–психологической безопасности личности.

Вопросы для контроля:

1. Что такое информационное общество?
2. Перечислите основные особенности информационного общества.
3. Как обезопасить себя в информационном обществе?

Урок 17. Проектная работа «Безопасный интернет в каждый дом».

Тип урока: урок применения знаний, умений и навыков с элементами творчества.

Цель урока: Определить уровень знаний по прохождению курса: «Информационная безопасность» и умений по созданию презентации на заданную тему.

Задачи:

Образовательная: формирование навыков использования разных типов объектов при создании презентаций или буклетов, умения демонстрировать презентацию.

Развивающая: Развитие познавательного интереса к предмету, внимательности, мышления и творческих способностей учащихся при реализации индивидуального проекта.

Воспитательная: воспитание информационной культуры учащихся, самостоятельности, внимательности, аккуратности, дисциплинированности, усидчивости, формирование интереса к изучению информационной безопасности.

Краткое содержание урока: В ходе урока учащиеся защищают свои проекты по заданной теме.

Вопросы для контроля:

1. Что нового вы узнали на этом курсе?
2. Что вы начали использовать для достижения личной безопасности в Интернете?

2.3. Программно-методическая поддержка курса

В качестве программно-методической поддержки факультативного курса «Информационная безопасность» для 7-9 классов был разработан сайт с помощью WordPress. Учебное пособие располагается по адресу http://z92275kk.beget.tech/.

На рисунке представлена главная страница программно-методической поддержки курса.

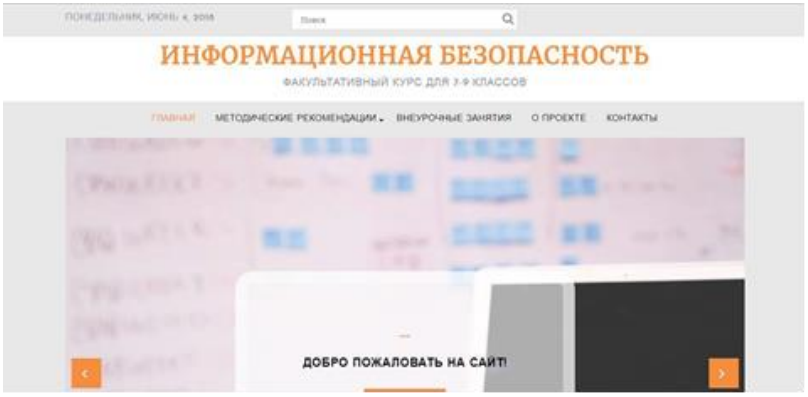


Рис. 5. Главная страница

На сайте представлены разделы как главная, о проекте, контакты, методические рекомендации и внеурочные занятия.

В разделе «Контакты» пользователь сайта может узнать, где нас можно найти и как связаться, дополнительно он может отправить нам сообщение с помощью контактной формы на сайте.

В разделе «О проекте» находится информация о том, что пользователь может найти для себя на этом сайте.

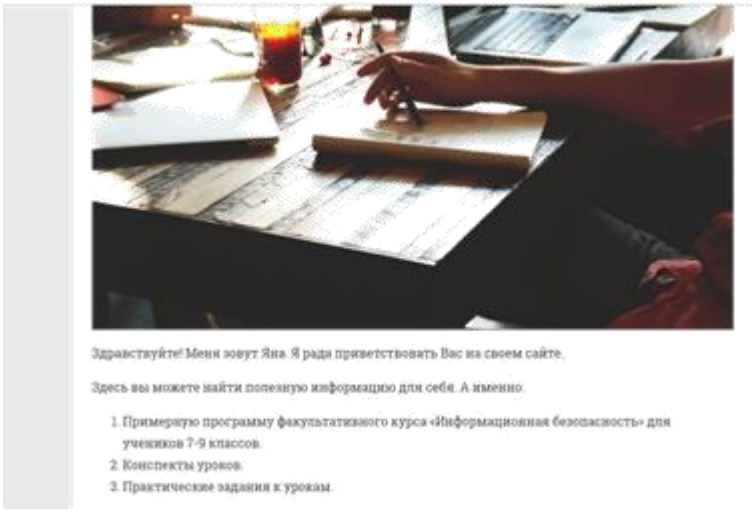
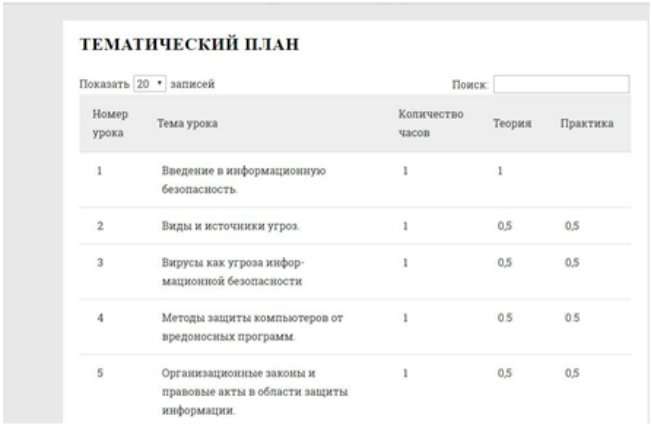


Рис. 6. Раздел «О проекте»

В разделе «Методические рекомендации» расположены анализы нормативных документов и учебников по информатике 7 и 9 классов. В дополнение к этому в разделе существуют пояснительная записка к факультативному курсу, его тематический план и содержание программы.



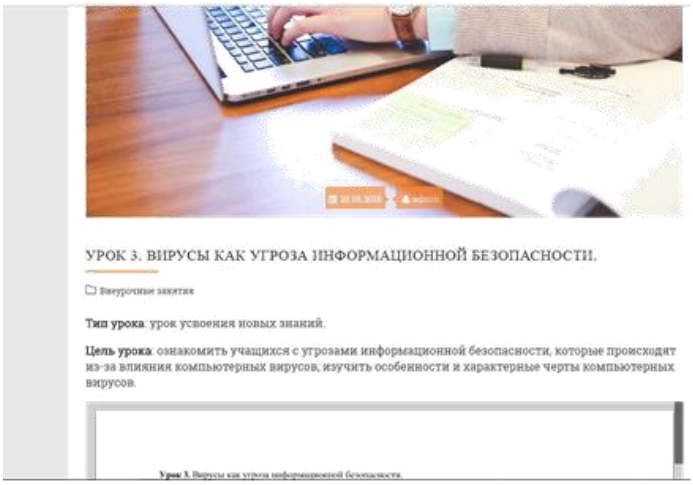
ТЕМАТИЧЕСКИЙ ПЛАН

Показать 20 записей Поиск:

Номер урока	Тема урока	Количество часов	Теория	Практика
1	Введение в информационную безопасность.	1	1	
2	Виды и источники угроз.	1	0,5	0,5
3	Вирусы как угроза информационной безопасности	1	0,5	0,5
4	Методы защиты компьютеров от вредоносных программ.	1	0.5	0.5
5	Организационные законы и правовые акты в области защиты информации.	1	0,5	0,5

Рис. 7. Тематический план

Во «Внеурочных занятиях» размещены конспекты уроков к данному курсу, а также презентации к ним и вспомогательные материалы для практических занятий или приложения для контроля по прохождению темы урока.



УРОК 3. ВИРУСЫ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Внеурочные занятия

Тип урока: урок усвоения новых знаний.

Цель урока: ознакомить учащихся с угрозами информационной безопасности, которые происходят из-за влияния компьютерных вирусов, изучить особенности и характерные черты компьютерных вирусов.

Рис. 8. Страница урока

2.4. Апробация результатов исследования в школе

Педагогическая апробация проводилась в рамках научно-исследовательской практики в МБОУ СОШ № 12 г. Верхнего Уфалея. Курс изучался в 9-ом классе. В течении одного занятия была рассмотрена тема информационной безопасности.

Апробация была проведена успешно. Способствовала этому правильная мотивация, цели и задачи для изучения темы.

Тема курса оказалась частично знакома для учащихся, но они быстро включились в работу, заинтересовавшись темой.

ВЫВОДЫ ПО ГЛАВЕ 2

Во второй главе были рассмотрены образовательные стандарты, описан факультативный курс «Информационная безопасность» и программно-методическая поддержка, в виде образовательного портала.

Проведенное исследование было направлено на изучение теоретических положений по изучению информационной безопасности в средней школе и разработку факультативного курса и программно-методической поддержки курса. В конце работы была достигнута цель, разработан факультативный курс по теме «Информационная безопасность».

Была проведена апробация курса, которая проводилась в рамках научно-исследовательской практики в МБОУ СОШ № 12 г. Верхнего Уфалея.

В процессе исследования были решены поставленные задачи и получены следующие результаты:

1. Изучены теоретические положения по проблеме исследования, в школьном курсе данная тема узко рассматривается.
2. Разработан 17-часовой факультативный курс как школьный факультативный курс по изучению информационной безопасности в школе для 7-9 классов.
3. Разработана программно-методическая поддержка факультативного курса в виде электронного пособия «Информационная безопасность».

В подтверждение гипотезы можно сказать, что данный курс позволяет повысить уровень компетентности в области изучения информационной безопасности у учащихся.

Поставленные задачи можно считать выполненными и можно сделать вывод о верности поставленной гипотезы.

ЗАКЛЮЧЕНИЕ

Проведенное исследование было направлено на изучение теоретических положений по изучению информации и информационной безопасности и разработку факультативного курса «Информационная безопасность», а также его программно-методической поддержки, используя возможности внеурочной деятельности по информатике в средней школе.

В процессе исследования были решены поставленные задачи и получены следующие результаты:

1. Изучены теоретические положения по проблеме исследования, в школьном курсе тема информационной безопасности рассматривается недостаточно широко.
2. Разработан 17-часовой факультативный курс по изучению информационной безопасности в школе для 7-9 классов.
3. Разработана программно-методическая поддержка факультативного курса в виде образовательного портала «Информационная безопасность».

В подтверждение гипотезы можно сказать, что данный курс позволяет повысить уровень компетентности в области изучения информационной безопасности.

Поставленные задачи можно считать выполненными и можно сделать вывод о верности поставленной гипотезы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е. Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015, 98 с.
2. Бородин М.Н. Информатика. УМК для основной школы: 5–6 классы. 7—9 классы. Методическое пособие / Автор-составитель: М. Н. Бородин. — Эл. изд. — М.: БИНОМ. Лаборатория знаний, 2013. — 108 с. : ил.
3. Грошев А. С. Г89 Информатика: Учебник для вузов / А.С. Грошев. – Архангельск, Арханг. гос. техн. ун-т, 2010. – 470 с.
4. Доктрина информационной безопасности РФ от 09.09.2000 №Пр-1895. Доступ из справ.-правовой системы «КонсультантПлюс».
5. Информатика: учебник для 5 класса / Л.Л.Босова, А.Ю.Босова – 3-е изд.– М.: БИНОМ. Лаборатория знаний 2015. – 184 с.
6. Информатика: учебник для 7 класса / Л.Л.Босова, А.Ю.Босова – 3-е изд.– М.: БИНОМ. Лаборатория знаний 2013. – 224 с.
7. Информатика: учебник для 7 класса / И.Г.Семакин, Л.А. Залогова, С.В.Русаков, Л.В.Шестакова. – М.: БИНОМ. Лаборатория знаний 2012. – 167 с.
8. Информатика и ИКТ. 8 кл.:учебник/ Ю.А.Быкадоров. – 4-е изд., стереотип. – М.: Дрофа, 2016. – 288 с.
9. Информатика: учебник для 8 класса / Н.Д. Угринович. – 4-е изд. – М.БИНОМ. Лаборатория знаний 2013. – 178 с.
10. Конфликты и происшествия [Электронный ресурс], – http://laste.arvutikaitse.ee/rus/solmuja_ja_sattumuksia.html – мультимедиа-приложение (дата обращения: 18.01.2018)
11. Приходько, А. Я. Словарь - справочник по информационной безопасности / А. Я. Приходько. – М.: СИНТЕГ, 2001. – 120 с. – (Сер. "Информационная безопасность")

12. Прогулка через Wild Web Woods [Электронный ресурс]. – http://www.wildwebwoods.org/ – мультимедиа-приложение (дата обращения: 18.01.2018)

13. Путешествие на Астерикс [Электронный ресурс]. – http://www.разбираеминтернет.рф/game – мультимедиа-приложение (дата обращения: 18.01.2018)

14. Римская группа [Электронный ресурс]. – http://laste.arvutikaitse.ee/rus/ryhma_rooma.html – мультимедиа-приложение (дата обращения: 18.01.2018)

15. Семакин И. Г. Информатика : методическое пособие для 7–9 классов / И. Г. Семакин, М. С. Цветкова. — М. : БИНОМ. Лаборатория знаний, 2016. — 160 с.

16. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646. Доступ из справ.-правовой системы «КонсультантПлюс».

17. Федеральный государственный образовательный стандарт основного общего образования от 6 октября 2009 г. № 413

18. Федеральный государственный образовательный стандарт основного общего образования от 17.12.2010 г. №1897

19. Об образовании в Российской Федерации: федер. закон от 29.12.2012 № 273-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

20. О внесении изменений в отдельные законодательные акты российской федерации в связи с принятием федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию": федер. закон от 21.07.2011 № 252-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

21. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ: ред. от 18.06.2017. Доступ из справ.-правовой системы «КонсультантПлюс».

22. О защите детей от информации, причиняющей вред их здоровью и развитию: федер. закон от 29.12.2010 № 436-ФЗ: ред. от 01.05.2017. Доступ из справ.-правовой системы «КонсультантПлюс».
23. Фурсов В. А.Ф 954 Теория информации: учеб. / В.А. Фурсов. - Самара: Изд-во Самар,гос. аэрокосм, ун-та, 2011. - 128 с.
24. Хлобыстова И. Ю. Информатика. УМК для основной школы: 7–9 классы. Методическое пособие для учителя / Авторы-составители: И. Ю. Хлобыстова, М. С. Цветкова. — Эл. изд. — М.: БИНОМ. Лаборатория знаний, 2013. — 91 с.
25. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. — М.: Фонд Развития Интернет, 2013. — 144 с.

ПРИЛОЖЕНИЕ

Урок №3

Тема урока. Вирусы как угроза информационной безопасности.

Тип урока: урок усвоения новых знаний.

Цель урока: ознакомить учащихся с угрозами информационной безопасности, которые происходят из-за влияния компьютерных вирусов; изучить особенности и характерные черты компьютерных вирусов.

Задачи:

Образовательная: Знакомство с компьютерными вирусами, способами и формами распространения компьютерных вирусов.

Развивающая: Развитие познавательного интереса.

Воспитательная: Воспитание у учащихся аккуратности, добросовестному отношению к учебному труду.

Обучающиеся должны знать:

1. Понятия компьютерный вирус, сетевые вирусы, файловые вирусы, загрузочные вирусы, файлово-загрузочные вирусы.
2. Методы аутентификации.

Обучающиеся должны уметь:

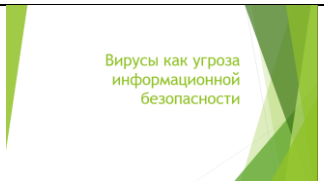
1. Грамотно придумывать безопасный пароль для интернет-сервисов.

Структура урока:

1. Организационный момент 1 мин.
2. Постановление цели урока 3 мин.
3. Объяснение нового материала 15 мин.
4. Практическая работа 15 мин.
5. Подведение итогов 6 мин.

Организационная структура урока

Деятельность учителя	Деятельность ученика	ЭОР	Время

1.<u>Организационный момент</u> Здравствуйте, ребята *(учитель приветствует учеников и отмечает в журнале посещаемость)!*	Приветствуют друг друга присутствующих уроке.		1 мин
<u>2. Постановление цели урока.</u> Ребята, как вы думаете компьютер может быть инфицирован? Приходилось ли встречаться с этой проблемой в процессе эксплуатации компьютера? Сегодня мы с Вами познакомимся с темой урока «Вирусы как угроза информационной безопасности». Данные сведения пригодятся для безопасной работы Интернете, с любыми носителями информации. А может ли компьютер заразится вирусом? Каким должен быть этот вирус по вашему представлению?	Участвуют в обсуждении. Слушают учителя. Отвечают на вопросы.		3 мин
<u>3.Объяснение нового материала</u> Давайте подведем итог, что компьютер может заразиться вирусами, только компьютерными. Это название пришло из биологии именно по признаку способности к самозаражению. Вирусы представляют собой небольшие вредоносные программы, которые запускаются на компьютере без ведома его владельца и могут	Записывают определения: компьютерный вирус, классификация вирусов.	 	15 мин

выполнять различные нежелательные действия. При этом вирусы могут быть как почти безвредными, так и весьма неприятными. Существует несколько видов классификации вредоносных программ: по среде обитания вируса и по особенностям построения вируса. По первому признаку вирусы бывают: сетевые, файловые, загрузочные и файлово-загрузочные. По второму – паразитические, черви, стелс-вирусы, мутанты, макро-вирусы, троянские программы. Как мы можем защитить наш компьютер от вируса? Да. Существуют специальные программы, которые смогут защитить ПК от заражения, а также удалить опасную программу, если заражение уже произошло. Особое место в этом списке занимают программные средства защиты-антивирусные программы. Рассмотрим несколько типов антивирусных программ, различающихся способами выполняемыми функциями. Существуют такие виды, как классический антивирус, антишпион, онлайн-сканер, сетевой экран, комплексная защита. Сделаем вывод, что ни один тип антивирусных программ по отдельности	Смотрят презентацию записывают классификацию вирусов. Отвечают на вопрос. Записывают определение: антивирусная программа Слушают про виды антивирусных программ. Записывают их отличия со слайда.	   	

защиты от вирусов. Поэтому современные программы работают в паре и не «конфликтуют собой».			
4.Практическая работа А теперь для закрепления ваших знаний об вирусах и антивирусах сделаем практическую работу за компьютером. Вам нужно зайти в папку вашего класса и найти там файлы, которые нужно проверить на наличие в них вируса.	Проверяют подготовленный электронный материал на наличие зараженного документа или носителя.		15 мин
5.Подведение итогов Выставление оценок за работу на уроке. Проверим ваши знания, поиграв в несколько игр.	Коллективно участвуют в решении приложения применяя полученные знания.		6 мин

Урок № 7

Тема: Идентификация и аутентификация

Тип урока: урок усвоения новых знаний.

Цель урока: ознакомить учащихся с содержанием и механизмами реализации сервисов безопасности “идентификация” и “аутентификация”.

Задачи:

Образовательная: Знакомство с понятиями “идентификация” и “аутентификация”, научить учащихся различать системы идентификации.

Развивающая: Развитие познавательного интереса.

Воспитательная: Воспитание у учащихся аккуратности, добросовестному отношению к учебному труду.

Обучающиеся должны знать:

1. Понятия аутентификации, идентификации и авторизации
2. Методы аутентификации.

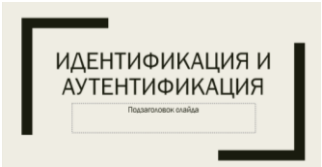
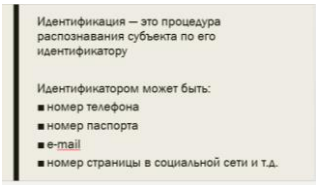
Обучающиеся должны уметь:

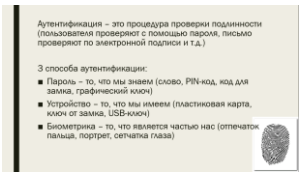
1. Грамотно придумывать безопасный пароль для интерне-сервисов.

Структура урока:

1. Организационный момент 1 мин.
2. Постановление цели урока 2 мин.
3. Объяснение нового материала 15 мин.
4. Практическая работа 15 мин.
5. Подведение итогов 7 мин.

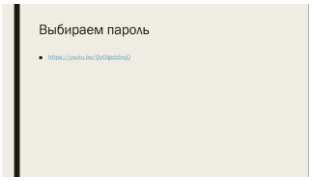
Ход урока

Деятельность учителя	Деятельность учеников	Экран	Время
1. Организационный момент Здравствуйте, ребята *(учитель приветствует учеников и отмечает в журнале посещаемость)!*	Приветствуют учителя		1 мин
2. Постановление цели урока. На сегодняшнем уроке мы узнаем, что такое идентификация, аутентификация, авторизация и в чем разница между этими понятиями. А также как создать безопасный пароль для личного пользования. Тема нашего урока: «Идентификация и аутентификация»			2 мин
3. Объяснение нового материала Для начала давайте дадим определение идентификации. Идентификация — это процедура распознавания субъекта по его идентификатору (проще говоря, это определение имени, логина или номера). Идентификация выполняется при попытке войти в какую-	Ученики дают определение Ученики предлагают варианты ответа		15 мин

либо систему (например, в операционную систему или в сервис электронной почты). Например, вашим идентификатором в социальной сети Вконтакте будет являться ваш id. Когда вам звонят с неизвестного номера, что вы делаете? Правильно, спрашиваем “Кто это”, т.е. узнаём имя. Имя в данном случае и есть идентификатор, а ответ вашего собеседника — это будет идентификация. Идентификатором может быть: 1. номер телефона 2. номер паспорта 3. e-mail 4. номер страницы в социальной сети и т.д. После идентификации производится аутентификация: Аутентификация – это процедура проверки подлинности (пользователя проверяют с помощью пароля, письмо проверяют по электронной подписи и т.д.) Чтобы определить чью-то подлинность, можно воспользоваться тремя факторами: 1. Пароль – то, что мы знаем (слово, PIN-код, код для замка, графический ключ) 2. Устройство – то, что мы имеем (пластиковая карта, ключ от замка, USB-ключ) 3. Биометрика – то, что является частью нас (отпечаток пальца, портрет, сетчатка глаза)	Слушают учителя Предлагают свои ответы Слушают учителя		

Получается, что каждый раз, когда вы вставляете ключ в замок, вводите пароль или прикладываете палец к сенсору отпечатков пальцев, вы проходите аутентификацию. Когда определили ID, проверили подлинность, уже можно предоставить и доступ, то есть, выполнить последний шаг - авторизацию. Авторизация – это предоставление доступа к какому-либо ресурсу (например, к электронной почте). В повседневной жизни примерами авторизации могут быть: 1. Открытие двери после проворачивания ключа в замке 2. Доступ к электронной почте после ввода пароля 3. Разблокировка смартфона после сканирования отпечатка пальца 4. Выдача средств в банке после проверки паспорта и данных о вашем счете Наверное, вы уже догадались, что все три процедуры взаимосвязаны: 1. Сначала определяют имя (логин или номер) – идентификация 2. Затем проверяют пароль (ключ или отпечаток пальца) – аутентификация 3. И в конце предоставляют доступ – авторизация Помните, сказку «Красная Шапочка»? Как в этой сказке бабушка разрешает внучке войти в дом? Правильно!		 	

Сначала бабушка спрашивает, кто за дверью, затем говорит Красной Шапочке, как открыть дверь. Волку же оказалось достаточным узнать имя внучки и расположение дома, чтобы пробраться в дом. Какой вывод можно сделать из этой истории? Каждый этап авторизации должен быть тщательно продуман, а идентификатор, пароль и сам принцип авторизации нужно держать в секрете. Поэтому нам очень важно продумать свой пароль к доступу на различные сайты или сервисы. Надежность пароля напрямую зависит от его длины и сложности. Разнообразие предполагает использование разных паролей для разных учетных записей и регулярное изменение пароля. Необходимо также обеспечивать защиту записанных паролей и особенно внимательно относиться к защите аккаунта в электронной почте, через которую происходит регистрация на других ресурсах. Существуют автоматизированные службы, помогающие генерировать и хранить пароли от разных сервисов. Рекомендации для надежности пароля 1. Надежный пароль — это важный элементы защиты, который позволяет значительно повысить безопасность онлайн-	Отвечают на вопросы		

транзакций. Ключевые элементы надежности пароля — длина и сложность. Идеальный пароль — это длинная комбинация различных знаков, которая включает в себя буквы и цифры, а также знаки пунктуации и символы. Если это возможно, старайтесь использовать восемь и более знаков. 2. Не используйте один и тот же пароль везде. Злоумышленники крадут учетные данные на сайтах со слабой безопасностью, а затем пытаются использовать те же пароли и имена пользователя, чтобы получить доступ к более защищенным ресурсам, например, банковским сайтам. 3. Старайтесь регулярно менять свои пароли. Установите автоматическое напоминание, которое будет уведомлять вас о необходимости сменить пароли на используемых вами ресурсах. 4. Чем больше разнообразных символов вы используете в пароле, тем лучше. Тем не менее, помните, что программы для подбора паролей автоматически проверяют их на замену распространенных комбинаций букв на символы, например «to» на «2». 5. Обеспечьте защиту для записанных паролей. Будьте внимательны к тому, где вы храните или записываете пароли. Вместо того чтобы придумывать пароли, а тем более их помнить, можно			

использовать автоматизированные средства генерации и хранения паролей. 6.Будьте аккуратны с паролем к своему почтовому ящику. Именно он, как правило, служит ключом для несанкционированного доступа к разным сайтам от имени пользователя, поскольку через email производится регистрация практически на любых сервисах. Перед практической работой давайте посмотрим ролик о создании пароля.			
<u>4.Практическая работа</u> А теперь давайте поиграем в игру. Один из вас будет пользователем сети, который придумал 4-значный пароль для почты, а остальные - хакерами, которые хотят взломать его аккаунт. Так, пароль создан. А теперь, уважаемые хакеры, вы должны угадать какие цифры в данном пароле и их порядок. Молодцы! Вы отгадали пароль! Как вы думаете, легко ли настоящим злоумышленникам взломать простой пароль? Можно ли придумать такой пароль, который очень сложно взломать? Данный метод подбора паролей является очень распространенным способом взлома аккаунта и его применяют настоящие злоумышленники. Специально созданные для этого программы, которые способны	Один ученик выходит к доске и пишет 4 цифры для пароля, а затем закрывает пароль. Остальные ученики не должны видеть, что написал ведущий. Ученики угадывают пароль ведущего. Отвечают на вопросы учителя.		15 мин

перебирать большое количество комбинаций символов за короткий промежуток времени, делают это намного быстрее человека. Чем проще пароль, тем легче его взломать, поэтому необходимо знать ключевые правила создания, использования и хранения паролей, чтобы сократить риск взлома аккаунта.			
4. Подведение итогов Давайте подведем итоги. А точнее еще раз повторим, как нужно создавать безопасный пароль. Молодцы. Теперь вы сможете обезопасить себя и свою деятельность в интернете. До свидания.	Ученики предлагают свои ответы. Прощаются с учителем.		7 мин

Урок № 13

Тема: Безопасность в сети Интернет

Тип урока: комбинированный.

Цель урока: обеспечение информационной безопасности несовершеннолетних обучающихся путем привития им навыков ответственного и безопасного поведения в Интернете.

Задачи:

Образовательная: Знакомство с правилами ответственного и безопасного поведения в современной информационной среде.

Развивающая: Развитие познавательного интереса.

Воспитательная: Воспитание у учащихся познавательный интерес к изучению информатики, аккуратность, культуру общения.

Обучающиеся должны знать:

1. Перечень информационных услуг сети интернет;
2. Правила безопасной работы в сети интернет;
3. Опасности глобальной компьютерной сети.

Обучающиеся должны уметь:

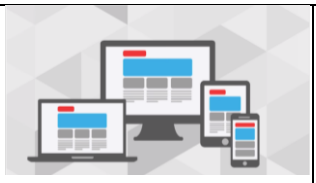
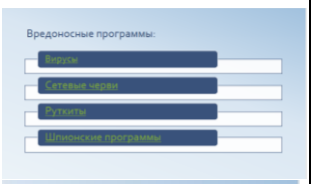
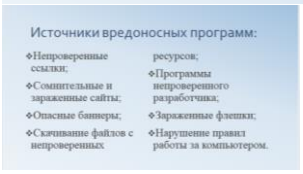
1. Ответственно относиться к использованию on-line-технологий.

Структура урока:

1. Организационный момент 1 мин.
2. Постановление цели урока 2 мин.
3. Объяснение нового материала 15 мин.
4. Практическая работа 20 мин.
5. Подведение итогов 2 мин.

Ход урока

Деятельность учителя	Деятельность учеников	Экран	Время
1. Организационный момент Здравствуйте, ребята *(учитель приветствует учеников и отмечает в журнале посещаемость)!*	Приветствуют учителя		1 мин
2. Постановление цели урока. Хотелось бы вам узнать какая погода будет завтра, чтобы продумать свой гардероб или получить сведения об интересующих вас вопросах? Все это и многое другое можно узнать, не выходя из дома, если у вас есть Интернет. Но Интернет не только может быть полезным в различных вопросах, а еще и опасным. И о том, как обезопасить себя в Интернете мы и поговорим. Тема нашего урока: «Безопасность в сети Интернет»			2 мин
3. Объяснение нового материала А давайте выясним, что такое интернет? А знаете ли вы, когда возник Интернет? Прообразом интернета стало компьютерная сеть Arpanet разработана по заказу министерства	Ученики дают определение Ученики предлага		15 мин

обороны США. В далеком 1969 году был проведен первый сеанс связи по компьютерной сети на расстоянии 640 километров было передано слово логин при этом успешная передача каждого символа подтверждалось по телефону. Далее развитие компьютерных сетей стало расти стремительно. И в 1991 году всемирная паутина стала доступна в интернете. С тех пор для многих слова «Интернет» и «всемирная паутина» стали синонимами. Сегодня для работы в интернете можно использовать разные устройства. Компьютер, ноутбук, планшет, сотовый телефон. К интернету все чаще подключается и бытовая техника, и другие устройства. В данных устройствах мы пользуемся различными программами, разработанными для разных целей. Игры, мессенджеры, офисные программы и так далее. Но некоторые программы таят в себе угрозу, угрозой является внедрение вредоносных программ, которые мы часто называем просто вирусы. Говоря о вредоносных программах, обычно выделяют собственно вирусы сетевые черви, руткиты, шпионские программы. Вирус - вредоносный код, который нарушает работоспособность системы. Сетевые черви - это вирусы, которые могут самостоятельно распространяться, заражая все больше устройств. Руткиты - это вирусы, которые маскируют свое присутствие системе и могут самовосстанавливаться или	ют варианты ответа Слушают учителя	  	

заражать компьютер при определенных условиях. Шпионские программы - это вредоносные программы, целью которых является слежка и похищение информации. Давайте вспомним, каким образом мы можем занести вирус на свое устройство? Главными источниками вирусов и других вредоносных программ являются заражение при переходе по ссылкам из писем и сообщений с незнакомых адресов, посещение сомнительных и зараженных сайтов, клики по баннерам сомнительного содержания, скачивания программ и файлов с непроверенных ресурсов, установка программ ненадежного разработчика или сомнительных ресурсов, неосторожное использование чужих зараженных флешек, нарушение других правил безопасной работы с компьютером. А теперь кратко остановимся на безопасности линии связи, а именно на беспроводной связи, которые мы привычно называем wi-fi. На самом деле wi-fi - это товарный знак альянса производителей техники, поддерживающий беспроводную связь нескольких стандартов, некоторые считают, что wi-fi произошло от английского Wireless Fidelity, который переводится как беспроводная точность. Сети wi-fi становятся все более популярными многие торговые точки предоставляют бесплатный доступ для привлечения клиентов, и мы с удовольствием пользуемся такой возможностью, однако нужно	Ученики отвечают на вопрос Слушают учителя	 	

быть осторожными при работе в сети и нужно соблюдать правила для безопасной работы если в сетях wi-fi. Не передавай свою личную информацию через общедоступные wi-fi сети, работая в них желательно не вводить пароли доступа, логины и какие-то номера, чтобы сделать что-то важное нужно воспользоваться более защищенными каналами связи, обращая внимание на значок безопасного соединения. При доступе к важному сайту и проверки электронной почты при использовании wi-fi отключи функцию «общий доступ» к файлам и принтерам. Данная функция закрыта по умолчанию, однако некоторые пользователи активирует ее для удобства используем в работе или учебе в мобильном телефоне. Отключи функцию подключения к wi-fi автоматически, не допуская автоматического подключения устройства к сетям вай-фай. без твоего согласия в домашней сети wi-fi используй надёжные пароли и отключи ненужные функции сети. С развитием сети интернет стали появляться мошенники и главная задача получить лично данные, которые позволяют добраться до ваших реальных денег. В первую очередь к таким данным относится логины и пароли от различных сервисов, в том числе от банковских карточек, номера и пин-коды банковских карт, персональные данные. Рассмотрим самые распространенные методы.		 	

Фишинг - различными методами тебя заманивают на поддельный сайт, обычно эта ссылка в письме, баннер или ссылка на сайте, иногда вредоносная ссылка маскируется под правильную, но есть риск попасть на фишинговый сайт. Из-за опечатки в адресе сайта поддельный сайт очень похож на настоящий, например, сайт социальной сети или банка, тебе предлагают ввести логин и пароль или данные счета, часто после этого происходит перенаправление на реальный сайт, но данные уже попадают в руки мошенников. Вишинг - это разновидность фишинга, в которой используется телефон. Злоумышленники звонят потенциальной жертве от имени администрации банка или другого сервиса и просят подтвердить пароль пин-код или другую важную информацию. Фарминг или скрытое перенаправление - разновидность фишинга, когда на поддельный сайт себя направляет вирус или взломанная программа, противодействовать ему крайне сложно поскольку злоумышленники не обращаются к своей жертве напрямую, а вмешиваются в работу компьютера, при этом происходит переадресация обращение на сайт злоумышленников, являющиеся полной копии официального ресурса. Для противодействия фишинга и его разновидности нужно следовать простым рекомендациям: следи за своим аккаунтом, используй проверенные и безопасные веб-			

сайты, используй сложные и разные пароли, если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях о том что тебя взломали, не размещай личную информацию в интернете, даже маленькие кусочки личных данных могут быть использованы в преступных целях.			
4.Практическая работа А теперь давайте поиграем в игру. Для начала вам нужно поделиться на группы с помощью жеребьевки! Вы частные детективные агентства, которым нужно разоблачить сетевых мошенников. Вам будут даны карточки с перепиской и вам нужно внимательно изучить переписку и найти все доказательства, позволяющие уличить мошенников в их злых деяниях. На выполнение задания отводится 5 минут. Вопросы для выступления: Какие чувства пытаются затронуть авторы письма у своих адресатов? Какая информация в письмах вызывает наибольшее подозрение? Как, по-вашему, чем обычно заканчивается переписка с мошенниками?	Ученики вытягивают жребий, формируются в группы и придумывают название группы. Ученики читают переписку, затем каждая группа зачитывает свою часть переписки и и отвечает на вопросы.	Карточки с заданиями	20 мин
4. Подведение итогов Выявляется самое успешное частное детективное агентство.	Ученики все вместе выбирают		2 мин

	победителя		