Муниципальное бюджетное общеобразовательное учреждение
«Школа № 13 имени Героя Советского Союза Ф.В. Санчирова»
городского округа Самара

ОБСУЖДЕНО: на заседании МО 26.08.2024	ПРОВЕРЕНО: Заместитель директора по УВР Н.Б. Бирюкова «27» августа 2024 г.	УТВЕРЖДЕНО: Директором МБОУ Школы № 13 г.о. Самара Д.В. Окуленко (приказ по школе № 263-од от «28» августа 2024 г.)

Окуленко Д.В.

Окуленко Д.В.
O=МБОУ Школа №13 г.о. Самара, CN=Окуленко Д.В., E=shkola13-sanchirov@yandex.ru
2024.11.02 21:08:37+04'00'

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности для учащихся 8 классов
основного общего образования

Информационная безопасность

Направление: социально-гуманитарнон
Срок реализации: 1 год

Составитель: учитель информатики
Матназарова А.В.

Самара, 2024

Пояснительная записка

Программа курса «Информационная безопасность» (цифровая гигиена) адресована учащимся 8 классов, а также родителям обучающихся всех возрастов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам.

При составлении данной программы автором использованы следующие нормативно-правовые документы:

- Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Постановление Главного государственного врача РФ от 29.12.2010г. №189 «Об утверждении СанПиН 2.4.2.2821-10 ...» р.

«Санитарноэпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях»;

- Приказ МОиН РФ от 06.10.2009г №373 «Об утверждении и введении в действие федерального государственного образовательного стандарта начального общего образования» (с изменениями и дополнениями);
- Приказ МОиН РФ от 17 декабря 2010 года №1897 «Об утверждении и введении в действие федерального государственного стандарта основного общего образования»(с изменениями и дополнениями);
- Информационное письмо МОиН РФ №03-296 от 12 мая 2011г. «Об организации внеурочной деятельности при введении федерального государственного образовательного стандарта общего образования»;
- Приказ МОиН РФ от 31 декабря 2015 года №1576 «О внесении изменений в ФГОС НОО»;
- Приказ МОиН РФ от 31 декабря 2015 года №1577«О внесении изменений в ФГОС ООО»;
- Письмо МОиН РФ от 14 декабря 2015 года №09-3564 «О внеурочной деятельности и реализации дополнительных образовательных программ»;
- Письмо МОиН Самарской области от 17.02.2016 №МО-16-09-01/173- ТУ «О внеурочной деятельности»;
- Григорьев Д.В., Степанов П.В. Внеурочная деятельность школьников. Методический конструктор - М., 2010.

Основными целями изучения курса являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- формирование навыков своевременного распознавания онлайн- рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Пояснительная записка

Задачи программы:

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

Направление курса внеурочной деятельности: общекультурное.

Общая характеристика учебного курса. Курс «Информационная безопасность» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Данный курс предполагает организацию работы в соответствии с содержанием 2-х модулей, предназначенных для обучающихся 9 класса.

Модуль 1. «Информационная безопасность»

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей, обучающихся 9 классов. Рекомендуется для реализации в рамках внеурочной деятельности обучающихся.

В преподавании модуля «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме

или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

Место учебного курса в учебном плане

Программа учебного курса рассчитана на 34 учебных часа, из них 22 часа - учебных занятий, 9 часов - подготовка и защита учебных проектов, 3 часа - повторение. На изучение модуля 1 «Информационная безопасность» отводится по 1 часу в неделю 8 классе.

Планируемые результаты изучения учебного предмета

Личностные результаты:

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

Метапредметные.

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;

- выбирать из предложенных вариантов и самостоятельно искать

средства ресурсы для решения задачи достижения цели;

- составлять план решения проблемы (выполнения проекта, проведения исследования);
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

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

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- строить позитивные отношения в процессе учебной и познавательной деятельности;
- критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;

- делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.

- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;

- выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;

- использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;

- использовать информацию с учетом этических и правовых норм;

- создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Предметные:

Выпускник научится:

- анализировать доменные имена компьютеров и адреса документов в интернете;

- безопасно использовать средства коммуникации,

- безопасно вести и применять способы самозащиты при попытке мошенничества,

- безопасно использовать ресурсы интернета.

Выпускник получит возможность научиться:

- основам соблюдения норм информационной этики и права;

- основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;

- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет- ресурсы и другие базы данных.

Воспитательные результаты:

Первый уровень результатов — овладение первоначальными представлениями о нормах русского языка и правилах речевого этикета; приобретение школьником социальных знаний (об общественных нормах, устройстве общества, о социально одобряемых и неодобряемых формах поведения в обществе и т. п.), первичного понимания социальной реальности и повседневной жизни. Для достижения данного уровня результатов особое

значение имеет взаимодействие ученика со своими учителями как значимыми для него носителями положительного социального знания и повседневного опыта.

Второй уровень результатов — овладение навыками адаптации в различных жизненных ситуациях, развитие самостоятельности и личной ответственности за свои поступки; получение школьником опыта переживания и позитивного отношения к базовым ценностям общества (человек, семья, Отечество, природа, мир, знания, труд, культура), ценностного отношения к социальной реальности в целом. Для достижения данного уровня результатов особое значение имеет взаимодействие школьников между собой на уровне класса, школы, то есть в защищенной, дружественной про социальной среде. Именно в такой близкой социальной среде ребёнок получает (или не получает) первое практическое подтверждение приобретённых социальных знаний, начинает их ценить (или отвергает).

Третий уровень результатов — овладение умением ориентироваться в целях, задачах, средствах и условиях общения, выбирать языковые средства для решения коммуникативных задач; получение школьником опыта самостоятельного общественного действия. Только в самостоятельном общественном действии, действии в открытом социуме, за пределами дружественной среды школы, для других, зачастую незнакомых людей, которые вовсе не обязательно положительно к нему настроены, юный человек действительно становится (а не просто узнаёт о том, как стать) социальным деятелем, гражданином, свободным человеком.

Содержание программы учебного курса.

Содержание программы учебного курса соответствует те-мам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста. За счет часов, предусмотренных для повторения материала (4 часа), возможно проведение занятий для учащихся 4-6 классов. Эти занятия в качестве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные в ходе выполнения учебных заданий по основным темам

курса.

Содержание учебного курса.

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час.

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

Тема 2. С кем безопасно общаться в интернете. 1 час.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей. 1 час.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей.

Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.

Настройки приватности и конфиденциальности в разных социальных сетях.

Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 1 час.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. 1 час.

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. 2 часа.

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах.

Действия при обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 час.

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

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.

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

Выполнение и защита индивидуальных и групповых проектов. 3 часа.4

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

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

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

Транзакции и связанные с ними риски. Правила совершения онлайн покупок.

Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. 1 час.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила

работы в публичных сетях.

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.5 Повторение. Волонтерская практика. 3 часа.

Тематическое планирование 8 класс (34ч.)

№	Тема	Кол-во часов	Теория	Практика
Тема 1. «Безопасность общения»				
1.	Общение в социальных сетях и мессенджерах	1	1	
2.	С кем безопасно общаться в интернете	1	1	
3.	Пароли для аккаунтов социальных сетей	1	1	
4.	Безопасный вход в аккаунты	1	1	
5.	Настройки конфиденциальности в социальных сетях	1		1
6.	Публикация информации в социальных сетях	1		1
7.	Кибербуллинг	1	1	
8.	Публичные аккаунты	1	1	
9.	Фишинг	1	1	
10.	Выполнение и защита индивидуальных и групповых	1		1
11.	Выполнение и защита индивидуальных и групповых	1		1
12.	Выполнение и защита индивидуальных и групповых	1		1
Тема 2. «Безопасность устройств»				
13.	Что такое вредоносный код	1	1	
14.	Распространение вредоносного кода	1	1	
15.	Методы защиты от вредоносных программ	1	1	
16.	Методы защиты от вредоносных программ	1		1
17.	Распространение вредоносного кода для мобильных	1	1	
18.	Выполнение и защита индивидуальных и групповых	1		1
19.	Выполнение и защита индивидуальных и групповых	1		1
20.	Выполнение и защита индивидуальных и групповых	1		1
Тема 3 «Безопасность информации»				
21.	Социальная инженерия: распознать и избежать	1	1	
22.	Ложная информация в Интернете	1	1	
23.	Безопасность при использовании платежных карт в	1	1	
24.	Беспроводная технология связи	1	1	
25.	Резервное копирование данных	1	1	
26.	Основы государственной политики в области	1	1	
27.	Основы государственной политики в области	1	1	
28.	Выполнение и защита индивидуальных и групповых	1		1
29.	Выполнение и защита индивидуальных и групповых	1		1
30.	Выполнение и защита индивидуальных и групповых	1		1
31.	Повторение, волонтерская практика	1		1
32.	Волонтерская практика	1		1
33.	Волонтерская практика	1		1
34.	Волонтерская практика	1		1
	Итого	34	18	16

Список источников:

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

2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. - М.: Право и закон, 2014. - 182 с.

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

4. Дети в информационном обществе // http://detionline.com/journal/about

5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2016. - 239 с.

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

7. Защита детей by Kaspersky // https://kids.kaspersky.ru/

8. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. - М.: Ру-сайнс, 2017. - 64 с.

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

10. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa

11. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005. - 304 с.

12. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. № 22(66)

13. 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.