

муниципальное бюджетное общеобразовательное учреждение
«Школа №73» городского округа Самара
Адрес: г. Самара, ул. Майская, 47, тел. 933-21-58

«РАССМОТРЕНО»

на заседании МО
учителей математики
Руководитель МО
_____/Чижова И.Ю.
протокол № 4
«12» «08» 2020г

«ПРОВЕРЕНО»

Зам. директора по УВР
МБОУ Школы № 73
Митина А.П.
«13» «09» 2020г.

«УТВЕРЖДАЮ»

Директор
МБОУ Школы № 73 г.о.Самара
Дрожда Н. Б.
Приказ № 110-од
«17» августа 2020г.

РАБОЧАЯ ПРОГРАММА
курса внеурочной деятельности
«Информационная безопасность»

(Программа разработана на основе авторской программы Наместниковой М. С. Информационная безопасность, или на расстоянии одного вируса: Учебное пособие для общеобразовательных организаций, 7-9 классы. – М.: Просвещение, 2019

Направление: Общекультурное
Форма организации: Кружок
Класс: 8

Срок реализации: 1 год

Составитель(и): Рыщенкова Ю.В.
Обсуждено и принято
на педагогическом совете школы
протокол № 5
от «14» «08» 2020г.

1. Планируемые результаты освоения учебного предмета, курса

ЛИЧНОСТНЫЕ

это сформировавшаяся в образовательном процессе система ценностных отношений учащихся к себе, другим участникам образовательного процесса, самому образовательному процессу, объектам познания, результатам образовательной деятельности. Основными личностными результатами, формируемыми при изучении информатики в основной школе, являются:

- наличие представлений об информации как важнейшем стратегическом ресурсе развития личности, государства, общества;
- понимание роли информационных процессов в современном мире;
- владение первичными навыками анализа и критичной оценки получаемой информации;
- ответственное отношение к информации с учетом правовых и этических аспектов ее распространения;
- развитие чувства личной ответственности за качество окружающей информационной среды;
- способность увязать учебное содержание с собственным жизненным опытом, понять значимость подготовки в области информатики и ИКТ в условиях развития информационного общества;
- готовность к повышению своего образовательного уровня и продолжению обучения с использованием средств и методов информатики и ИКТ;
- способность и готовность к общению и сотрудничеству со сверстниками и взрослыми в процессе образовательной, общественно-полезной, учебно-исследовательской, творческой деятельности;
- способность и готовность к принятию ценностей здорового образа жизни за счет знания основных гигиенических, эргономических и технических условий безопасной эксплуатации средств ИКТ.

МЕТАПРЕДМЕТНЫЕ

Регулятивные УУД

- 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 УУД

- 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 УУД

- 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

- 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.
- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
- основами 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.

2. Содержание учебного курса, предмета

1. «Безопасность общения»

Общение в социальных сетях и мессенджерах

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

С кем безопасно общаться в интернете

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

Пароли для аккаунтов социальных сетей

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Безопасный вход в аккаунты

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

Настройки конфиденциальности в социальных сетях

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Публикация информации в социальных сетях

Персональные данные. Публикация личной информации.

Кибербуллинг

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

Публичные аккаунты

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

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

2. «Безопасность устройств»

Что такое вредоносный код

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Распространение вредоносного кода

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.

Методы защиты от вредоносных программ

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

Распространение вредоносного кода для мобильных устройств

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

Выполнение и защита индивидуальных и групповых проектов

3 «Безопасность информации»

Социальная инженерия: распознать и избежать

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Ложная информация в Интернете

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

Безопасность при использовании платежных карт в Интернете

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Беспроводная технология связи

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Резервное копирование данных

Безопасность личной информации. Создание резервных копий на различных устройствах.

Основы государственной политики в области формирования культуры информационной безопасности

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.

Выполнение и защита индивидуальных и групповых проектов.

Форма промежуточной аттестации презентация

3. Тематическое планирование

№ урока	Наименование раздела, темы	Всего часов	В том числе	
			Теория	Практика
	Безопасность общения			
1	Общение в социальных сетях и мессенджерах	1	1	0
2	С кем безопасно общаться в интернете	1	0	1
3	Пароли для аккаунтов социальных сетей	1	1	0
4	Безопасный вход в аккаунты	1	1	0
5	Настройки конфиденциальности в социальных сетях	1	0	1
6	Публикация информации в социальных сетях	1	1	0
7	Кибербуллинг	1	1	0
8	Публичные аккаунты	1	0	1
9-10	Фишинг	2	1	1
11-13	Выполнение и защита индивидуальных и групповых проектов	3	1	2
	Безопасность устройств			
14	Что такое вредоносный код	1	0	1
15	Распространение вредоносного кода	1	1	0
16-17	Методы защиты от вредоносных программ	2	1	1
18	Распространение вредоносного кода для мобильных устройств	1	0	1
19-21	Выполнение и защита индивидуальных и групповых проектов	3	1	2
	Безопасность информации			
22	Социальная инженерия: распознать и избежать	1	1	0
23	Ложная информация в Интернете	1	0	1
24	Безопасность при использовании платежных карт в Интернете	1	1	0
25	Беспроводная технология связи	1	1	0
26	Резервное копирование данных	1	0	1

27-28	Основы государственной политики в области формирования культуры информационной безопасности.	2	1	1
29-31	Выполнение и защита индивидуальных и групповых проектов	3	1	2
32-34	Выполнение и защита индивидуальных и групповых проектов (Презентация)	3	2	1
	Всего: 34 часа		Кол-во часов 17 (%) 50	Кол-во часов 17 (%) 50