

Государственное бюджетное общеобразовательное
учреждение Самарской области
средняя общеобразовательная школа с.Алькино
муниципального района Похвистневский
Самарской области
(ГБОУ СОШ с.Алькино)

«Рассмотрено» Руководитель МО _____/Сайфулин Р.Р./ Протокол № ____ от « 29 » __08__ 2022_ г.	«Проверено» Зам. директора по УВР _____/Шигапова А.Х./ «30 » __08__ 2022_ г.	«Утверждаю» Директор ГБОУ СОШ с. Алькино _____/Ф. М. Маннанов/ « 31 » __08__ 2022 г.
---	--	---

РАБОЧАЯ ПРОГРАММА
ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«Информационная безопасность»
7-9 класс
Срок реализации – 3 года

Учитель Сайфулин Р.Р.
Класс 7-9
Всего часов в год 34
Всего часов в неделю 1

с. Алькино – 2020

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа курса внеурочной деятельности «Цифровая гигиена» адресована учащимся 7-8 классов и направлена на достижение следующих планируемых результатов Федерального государственного образовательного стандарта основного общего образования: - предметных (образовательные области «Математика и информатика», «Физическая культура, экология и ОБЖ»);

- метапредметных (регулятивных, познавательных, коммуникативных);
- личностных.

Рабочая программа ориентирована на учебник:

Порядковый номер учебника в Федеральном перечне	Автор/Авторский коллектив	Название учебника	Класс	Издатель учебника	Нормативный документ
	М.С.Наместникова	«Информационная безопасность или на расстоянии одного вируса»	7-9	Москва «Просвещение» 2019 г.	

Из авторской программы взят технологический компонент и модифицирован по часам.

2.ОБЩИЕ ПОЛОЖЕНИЯ

Курс является важной составляющей частью работы с учащимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.), задумывающимися о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории и технологических основ информационной безопасности. Направление программы курса внеурочной деятельности – общекультурное. Программа курса ориентирована на выполнение требований к организации и содержанию внеурочной деятельности школьников. Ее реализация даёт возможность раскрытия индивидуальных способностей школьников,

развития интереса к различным видам индивидуальной и групповой деятельности, закрепления умения самостоятельно организовать свою учебную, в том числе проектную деятельность. Кроме того, программа курса дает возможность закрепить ряд результатов обучения, предусмотренных программами учебных курсов по предметам «Информатика» и «Основы безопасности жизнедеятельности».

Программа рассчитана на 1 ч. в неделю.

В 1 полугодии - 17 часов, во 2 полугодии - 17 часов.

Всего за год – 34 часов.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОГО ПРЕДМЕТА

Цель программы:

- формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

Задачи программы:

- дать представление о современном информационном обществе, информационной безопасности личности и государства; - сформировать навыки ответственного и безопасного поведения в современной информационно-телекоммуникационной среде;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом;
- сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовать информационный процесс);
- дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
- познакомить со способами защиты от противоправных посягательств в сети Интернет, защиты личных данных.

Назначение программы – помочь детям узнать новые возможности компьютера и научиться ими пользоваться в повседневной жизни.

Результаты освоения программы

Личностные результаты

К личностным результатам освоения информационных и коммуникационных технологий как инструмента в учёбе и повседневной жизни можно отнести:

- критическое отношение к информации и избирательность её восприятия;
- уважение к информации о частной жизни и информационным результатам других людей;
- осмысление мотивов своих действий при выполнении заданий с жизненными ситуациями;
- начало профессионального самоопределения, ознакомление с миром профессий, связанных с информационными и коммуникационными технологиями.

Метапредметные результаты

Регулятивные универсальные учебные действия:

- освоение способов решения проблем творческого характера в жизненных ситуациях;
- формирование умений ставить цель – создание творческой работы, планировать достижение этой цели, создавать вспомогательные эскизы в процессе работы;
- оценивание получающегося творческого продукта и соотнесение его с изначальным замыслом, выполнение по необходимости коррекции либо продукта, либо замысла.

Познавательные универсальные учебные действия:

- поиск информации в индивидуальных информационных архивах учащегося, информационной среде образовательного учреждения, в федеральных хранилищах информационных образовательных ресурсов;
- использование средств информационных и коммуникационных технологий для решения коммуникативных, познавательных и творческих задач.

Коммуникативные универсальные учебные действия:

- создание гипермедиасообщений, включающих текст, набираемый на клавиатуре, цифровые данные, неподвижные и движущиеся, записанные и созданные изображения и звуки, ссылки между элементами сообщения;
- подготовка выступления с аудиовизуальной поддержкой.

Предметные результаты

1. Модуль «Безопасность общения».

В результате изучения данного модуля учащиеся узнают:

- ✓ что такое социальные сети;
- ✓ предназначение мессенджеров, как их безопасно использовать;
- ✓ что такое пароли и аккаунты, аутентификация, репутация,

кибербуллинг, фишинг и др.

научатся:

- ✓ входить в аккаунт социальных сетей;
- ✓ настраивать конфиденциальность в социальных сетях и работать

с различными браузерами;

2. Модуль «Безопасность устройств»

В результате изучения данного модуля учащиеся узнают:

- ✓ что такое вредоносный код;
- ✓ как распространяется вредоносный код;
- ✓ методы защиты от вредоносных программ

научатся:

- ✓ различать файлы по расширению;
- ✓ устанавливать и применять антивирусные программы;
- ✓ применять другие методы защиты от вредоносных программ;

3. Модуль «Безопасность информации».

В результате изучения данного модуля учащиеся узнают:

- ✓ что такое социальная инженерия и целевая атака;
- ✓ ложная (фейковая) информация в Интернете;
- ✓ что такое беспроводная технология связи;
- ✓ что такое резервное копирование данных

В результате изучения данного модуля учащиеся научатся:

- ✓ как безопасно отправлять данные;
- ✓ как безопасно переходить по ссылкам;
- ✓ создавать резервные копии данных;

4. СОДЕРЖАНИЕ УЧЕБНОГО ПРЕДМЕТА

№ п/п	Название раздела (блока)	Кол-во часов на изучение раздела (блока)	Из них кол-во часов, отведенных на практическую часть и контроль
			практика
1.	Введение	1	0
2.	Модуль «Безопасность общения»	16	4
3.	Модуль «Безопасность устройств»	9	5
4.	Модуль «Безопасность информации»	8	5
	Всего часов	34	14

Формы текущего контроля знаний, умений, навыков; промежуточной и итоговой аттестации учащихся

Все формы контроля по продолжительности рассчитаны на 10-15 минут. Текущий контроль осуществляется с помощью компьютерного практикума в форме практических работ и практических заданий.

Тематический контроль осуществляется по завершении крупного блока в форме тестирования или викторины.

Перечень средств ИКТ, необходимых для реализации программы **Аппаратные средства**

- Компьютер;
- Проектор;
- Принтер;
- Модем
- Устройства вывода звуковой информации — наушники для индивидуальной работы со звуковой информацией
 - Устройства для ручного ввода текстовой информации и манипулирования экранными объектами — клавиатура и мышь.
 - Устройства для записи (ввода) визуальной и звуковой информации: сканер; фотоаппарат; видеокамера; диктофон, микрофон.

Программные средства:

- Операционная система – Windows;
- Файловый менеджер (в составе операционной системы или др.);
- Антивирусная программа;
- Программа-архиватор;
- Интегрированное офисное приложение, включающее текстовый редактор, растровый и векторный графические редакторы, программу разработки презентаций и электронные таблицы;
 - Простая система управления базами данных;
 - Виртуальные компьютерные лаборатории;
 - Система оптического распознавания текста;
 - Мультимедиа проигрыватель
 - Система программирования;
 - Браузер;
 - Программа интерактивного общения;

5. Календарно-тематическое планирование

№ урока	Дата проведения		Тема урока	Тип урока	Характеристика основных видов учебной деятельности обучающихся	Виды/ формы контроля
	по плану	по факту				
Введение (1 час)						
1	01-08.09		Введение. Цели изучения курса информатики и ИКТ. Техника безопасности и организация рабочего места. Гигиенические, эргономические и технические условия безопасной эксплуатации компьютера.	Урок-лекция.	Следует требованиям техники безопасности, гигиены, эргономики и ресурсосбережения при работе со средствами информационных и коммуникационных технологий	Беседа
Модуль «Безопасность общения» (16 часов)						
2	08-15.09		Общение в социальных сетях и мессенджерах	Урок-лекция Презентация	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет. Изучает правила сетевого общения. Изучает основные понятия регистрационной	
3	15-22.09		Общение в социальной сети «В Контакте»			Практика
4	22-29.09		С кем безопасно общаться в Интернете	Урок-лекция Презентация		
5	29.09-06.10		Пароли для аккаунтов социальных сетей	Урок-лекция Презентация		Тест Викторин
6	06.10-13.10		Пароли для аккаунтов социальных сетей	Придумать пароли		Практика
7	13.10-20.10		Вход в аккаунт социальных сетей	Урок-лекция		

				Презентация	<p>информации и шифрования. Умеет их применить.</p> <p>Объясняет причины использования безопасного входа устойчивый навык безопасного входа.</p> <p>Раскрывает причины установки закрытого профиля.</p> <p>Меняет основные настройки приватности в личном профиле.</p> <p>Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников</p>		
8	20.10-27.10		Вход в аккаунт с режимом инкогнито			Практика	
9	10.11-17.11		Настройки конфиденциальности в социальных сетях	Урок-лекция Презентация			
10	17.11-24.11		Публикация информации в социальных сетях	Урок-лекция Презентация			
11	24.11-01.12		Публикация информации в социальных сетях на примере сети «В Контакте»				
12	01.12-08.12		Кибербуллинг	Урок-лекция Презентация			
13	08.12-15.12		Публичные аккаунты	Урок-лекция Презентация			
14	22.12-29.12		Создать публичный аккаунт			Практика	
15	12.01-19.01		Фишинг	Урок-лекция Презентация			
16	19.01-26.01		Тест по модулю «Безопасность общения»			Тест Викторина	
Модуль «Безопасность устройств» (9 часов)							
17	26.01-02.02		Что такое вредоносный код	Урок-лекция Презентация		<p>Соблюдает технику безопасности при эксплуатации компьютерных систем.</p> <p>Использует инструментальные программные средства и сервисы адекватно задаче.</p>	
18	02.02-09.02		Распространение вредоносного кода	Урок-лекция Презентация			Викторина
19	09.02-16.02		Методы защиты от вредоносных программ	Урок-лекция Презентация			
20	16.02-02.03		Распространение вредоносного кода для мобильных устройств	Урок-лекция Презентация			

21	02.03-09.03		Программы-архиваторы		Изучает виды антивирусных программ и правила	
22	09.03-16.03		Поиск и установка программ мессенджеров на мобильные устройства			Практика
23	16.03-23.03		Приемы и методы оптимизации и очистки мобильных устройств от вредоносного кода.			Практика
24	30.03-06.04		Возможности мессенджеров на мобильных устройствах			Практика
25	06.04-13.04		Тест по модулю «Безопасность устройств»			Викторина
Модуль «Безопасность информации» (8 часа)						
26	20.04-27.04		Социальная инженерия: распознать избежать		приобретает трудовые умения и навыки при работе на компьютере, опыт практической деятельности по созданию информационных объектов, полезных для человека и общества, умения использовать компьютерную технику для работы с информацией	Практика
27	27.04-04.05		Ложная информация в Интернете			Практика
28	04.05-11.05		Безопасность при использовании платежных карт в Интернете			Практика
29	11.05-18.05		Беспроводная технология			
30	18.05-25.05		Беспроводная технология			Практика
31	25.05-31.05		Резервное копирование данных			Практика
32			Резервное копирование данных			Практика
33	31.05		Тест по модулю «Безопасность		Викторина	

			информации»			
34			Тест по курсу «Цифровая гигиена» («Безопасность общения», «Безопасность устройств» и «Безопасность информации»)			
ИТОГО			34 часа			

Лист корректировки календарно-тематического планирования

Предмет «Цифровая гигиена»

Класс 7-9

Учитель Сайфулин Р.Р,

- учебный год

№ урока	Тема	Количество часов		Причина корректировки	Способ корректировки
		по плану	дано		
	Введение	1			
	Модуль «Безопасность общения»	16			
	Модуль «Безопасность устройств»	9			
	Модуль «Безопасность информации»	8			
	Итого	34			