государственное бюджетное общеобразовательное учреждение Самарской области основная общеобразовательная школа с.Сидоровка муниципального района Сергиевский Самарской области
(ГБОУ ООШ с.Сидоровка)

Рассмотрена и рекомендована	Проверено:	Утверждаю
к утверждению методическим объединением учителей Протокол № 1 от 31.0.2021 года _____ /Баканова Н.В./	ответственный за учебную работу /ВласовА.О./ от 31.08.2021 года	Директор ГБОУ ООШ с.Сидоровка _____ /Воропаева О.Г./ Приказ № 241 - од от 31.08.2021 года

Рабочая программа по внеурочной деятельности
«Информационная безопасность»

На уровень основного общего образования

Количество часов – 34
(7кл – 34 ч.)

Срок реализации- 1 год

Составитель: учитель информатики

Воропаева О.Г.

Приложение к ООП ООО

C=RU, O=ГБОУ ООШ с. Сидоровка, CN=О.Г. Воропаева, E=sidor-school@mail.ru
00b386c3f17a762903
2022.01.12 16:15:07+04'00'

с.Сидоровка

ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОГО ПРЕДМЕТА

Выпускник научится:

- анализироватьдоменныеименакомпьютеровиадресадокументоввинтернете;
- безопасно использовать средства коммуникации,
- безопасно вести и применять способы самозащиты при попытке мошенничества,
- безопасно использовать ресурсы интернета.

Выпускник овладеет:

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

Выпускник получит возможность овладеть:

- 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.

СОДЕРЖАНИЕ УЧЕБНОГО ПРЕДМЕТА

Модуль 1.

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 паро- лей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чу- жом 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 проектов3 часа.

Повторение1 час.

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 про- граммы 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 проектов3 часа.

Повторение1 час.

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. Под- дельные 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.

Требования к содержанию итоговых проектно-исследовательских работ содержатся в приложении 1 к дан- ной рабочей программе

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 проектов3 часа.

Повторение1 час.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ УЧЕБНОГО ПРЕДМЕТА

	Тема раздела	**Количество часов**	**Деятельность учителя с учетом программы воспитания (модуля «Школьный урок»)**
	Модуль 1.Раздел 1. «Безопасность общения»	10	Побуждение обучающихся соблюдать на уроке нормы поведения, правила общения со сверстниками и учителем, соответствующие укладу школы, установление и поддержка доброжелательной атмосферы. Установление доверительных отношений между учителем и учениками, способствующих позитивному восприятию требований, привлечению внимания к изучаемой проблеме
	Раздел 2. «Безопасность устройств»	5	Применение видов деятельности обучающихся со словесной (знаковой) основой: самостоятельная работа с учебником, работа с научно-популярной литературой, разбор и сравнение материала по нескольким источникам, что позволит обучающимся приобретать опыт самостоятельного поиска, анализа и отбора информации для решения поставленных задач.
	Раздел 3 «Безопасность информации»	7	Включение в урок игровых процедур, которые помогают поддержать мотивацию детей к получению знаний (лекция с запланированными ошибками, наличие двигательной активности на уроках), налаживанию позитивных межличностных отношений в классе, помогают установлению доброжелательной атмосферы во время урока (сотрудничество, поощрение, доверие, получение важного дела, создание ситуации успеха).
	Выполнение и защита индивидуальных и групповых проектов	9	Инициирование и поддержка исследовательской деятельности в форме индивидуальных и групповых проектов, что дает возможность

			приобрести навыки самостоятельного решения теоретической проблемы, генерирования и оформления собственных идей, уважительного отношения к чужим идеям, публичного выступления, аргументирования и отстаивания своей точки зрения
	Повторение	3	Применение на уроке интерактивных форм работы учащихся: дискуссий, которые дают учащимся возможность приобрести опыт ведения конструктивного диалога в атмосфере нравственных и эстетических переживаний, столкновений различных взглядов и мнений, поиска истины и возможных путей решения задачи или проблемы, творчества учителя и учащихся.
	Всего	**34**	