муниципальное бюджетное общеобразовательное учреждение
«Школа №69 имени Героя Советского Союза А.С.Бойцова»
городского округа Самара

Утверждаю	Проверено	Рассмотрено на заседании ШМО
Директор _____/И.В.Хапина/	«31»08 2024г	учителей естественно-математического цикла
«01»09 2024г	Зам.директора по УВР	Протокол №1 от «31» 08 2024г
Приказ №315-од	_____/Е.А.Касаткина/	Руководитель МО
		_____/Л.О.Нефедова/

м.п.

Рабочая программа

учебного предмета

«Информационная безопасность»

7-8 класс

(ID 5588484**)**

уровень реализации программы: базовый

Программу разработал:

Зозуленко П.С.

ЭП
ждаю
Хапина этот
Ирина докумен
Владим т
ировна 2024.08.3
0

Самара,2024

Пояснительная записка

Рабочая программа курса «Информационная безопасность» составлена в соответствии с требованиями Федерального государственного стандарта основного общего образования, Примерной рабочей программы учебного курса «Цифровая гигиена» (модуль «Информационная безопасность») на основании письма Министерства образования и науки Самарской области от 28.08.2019 № МО-16-09-01/847-ту «О преподавании курса «Цифровая гигиена».

Для реализации программы используется:

- Информационная безопасность, или на расстоянии одного вируса 7-9 классы: учебное пособие для общеобразовательных организаций / М.С. Наместникова. Просвещение, 2019.

Цель программы:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;

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.

Место предмета в учебном плане

Программа курса «Информационная безопасность» рассчитана на 34 учебных часа.

Планируемые результаты освоения предмета «Информационная безопасность»

Личностные результаты

Обучающийся сформирует	**Обучающийся получит возможность сформировать**
⊓ 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; ⊓ освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;	⊓ 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; ⊓ понимание ценности безопасного образа жизни; интериоризации правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные результаты

Регулятивные УУД

Обучающийся сформирует	**Обучающийся получит возможность сформировать**
⊓ умение ставить цель деятельности на основе определенной проблемы и существующих возможностей; ⊓ умение составлять план решения проблемы (выполнения проекта, проведения исследования); ⊓ Возможность описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса; ⊓ умение работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата; ⊓ навык принимать решение в учебной ситуации и нести за него ответственность.	⊓ умение идентифицировать собственные проблемы и определять главную проблему; ⊓ умение выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат; ⊓ умение выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели; ⊓ умение оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата; ⊓ навык находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;

Познавательные УУД

Обучающийся сформирует	**Обучающийся получит возможность сформировать**
⊓ способность определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть	⊓ умение выделять явление из общего ряда других явлений; ⊓ навык строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;

причиной данного явления, выявлять причины и следствия явлений; П способность излагать полученную информацию, интерпретируя ее в контексте решаемой задачи; П умение определять необходимые ключевые поисковые слова и запросы.	П способность самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации; П умение критически оценивать содержание и форму текста;

Коммуникативные УУД

Обучающийся сформирует	*Обучающийся получит возможность сформировать*
П умение договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей; П способность целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ; П умение выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации; П навык 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.;	П позитивные отношения в процессе учебной и познавательной деятельности; П умение делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его. П использовать информацию с учетом этических и правовых норм; П создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Предметные результаты

Обучающийся научится	*Обучающийся получит возможность*
П анализировать доменные имена компьютеров и адреса документов в интернете; П безопасно использовать средства коммуникации, П безопасно вести и применять способы самозащиты при попытке мошенничества, П безопасно использовать ресурсы интернета. П приемами безопасной организации своего личного пространства данных	П овладеть основами соблюдения норм информационной этики и права; П овладеть основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности; П использовать для решения коммуникативных задач в области безопасности жизнедеятельности

с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.	различные источники информации, включая Интернет- ресурсы и другие базы данных.

Содержание учебного курса

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах.
Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. 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.

Тема 3. Пароли для аккаунтов социальных сетей.
Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты.
Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях.
Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях.
Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг.
Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибер-буллинга.

Тема 8. Публичные аккаунты.
Настройки приватности публичных страниц. Правила ведения публич-ных страниц. Овершеринг.

Тема 9. 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

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. 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.

Тема 3. Методы защиты от вредоносных программ.

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

Тема 4. 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.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете.

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

Тема 3. Безопасность при использовании платежных карт в Интернете.

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

Тема 4. Беспроводная технология связи.

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

Тема 5. Резервное копирование данных.

Безопасность личной информации. Создание резервных копий на раз-

личных устройствах.

Тема 6. 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

Повторение. Волонтерская практика.

Тематическое планирование
7 класс

№ п/п	Наименование разделов, тем	Кол –во часов
Безопасное общение – 13 часов		
1.	Общение в социальных сетях и мессенджерах	1
2.	С кем безопасно общаться в интернете	1
3.	Пароли для аккаунтов социальных сетей	1
4.	Безопасный вход в аккаунты	1
5.	Настройки конфиденциальности в социальных сетях	1
6.	Публикация информации в социальных сетях	1
7.	Кибербуллинг	1
8.	Публичные аккаунты	1
9.	Фишинг	2
10.	Выполнение и защита индивидуальных и групповых проектов	3
Безопасность устройств - 8 часов		
11.	Что такое вредоносный код	1
12.	Распространение вредоносного кода	1
13.	Методы защиты от вредоносных программ	2
14.	Распространение вредоносного кода для мобильных устройств	1
15.	Выполнение и защита индивидуальных и групповых проектов	3
Безопасность информации - 13 часов		
16.	Социальная инженерия: распознать и избежать	1
17.	Ложная информация в Интернете	1
18.	Безопасность при использовании платежных карт в Интернете	1
19.	Беспроводная технология связи	1
20.	Резервное копирование данных	1
21.	Основы государственной политики в области формирования культуры информационной безопасности	2
22.	Выполнение и защита индивидуальных и групповых проектов	3
23.	Повторение. Волонтерская практика	3