ЗАПАДНОЕ УПРАВЛЕНИЕ МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ САМАРСКОЙ ОБЛАСТИ

государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа № 12 города Сызрани городского округа Сызрань Самарской области

Рассмотрена	**Проверена**	**Утверждена**
на заседании ШМО	зам. директора по УВР	Приказом № 197/2 –ОД от 30.08.2022 г.
Протокол № 1 от 26.08.2022г.	_____ Н.А. Прокофьева	Директор ГБОУ СОШ № 12 г. Сызрани
	«30» августа 2022 г.	_____ О.Н. Важнова
		МП

РАБОЧАЯ ПРОГРАММА

ПО ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«Цифровая гигиена» 7 класс

1 час в неделю

34 часа в год

Программа курса «Цифровая гигиена» адресована учащимся 7 классов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным, метапредметным и личностным результатам.

Сроки реализации программы: 1 год. Программа реализует общеинтеллектуальное направление во внеурочной деятельности. На реализацию программы отводится 1 час в неделю (одно занятие в неделю по 40 мин), всего 34 часа в год.

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7 классов.

Результаты освоения курса внеурочной деятельности

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 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.

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.

Личностные

- 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.

Содержание курса внеурочной деятельности
с указанием форм и организацией видов деятельности

Раздел 1. «Безопасность общения»

Обучающийся научится:

- общению в социальных сетях и мессенджерах.
- понимать и правильно применять на бытовом уровне понятий: социальная сеть; мессенджеры; пользовательский контент.
- понимать и правильно применять на бытовом уровне понятий: персональные данные как основной капитал личного пространства в цифровом мире; правила добавления друзей в социальных сетях; профиль пользователя; анонимные социальные сети.
- приводить примеры сложных паролей; использовать онлайн генераторы паролей; правила хранения паролей.
- приводить примеры видов аутентификации; настройки безопасности аккаунта.
- определять настройки приватности и конфиденциальности в разных социальных сетях.
- определять кибербуллинг, возможные причины кибербуллинга и как его избежать, знать как не стать жертвой кибербуллинга или как помочь жертве кибербуллинга.

Обучающийся получит возможность:

- сформировать представление о настройках приватности публичных страниц, овершеринге.
- сформировать представление о фишинге как мошенническом приеме.

Форма организации: беседа, просмотр презентации, видео; конкурсы рисунков, ребусов; ролевые игры.

Виды деятельности: игровая, познавательная, проблемно-ценностное общение, досугово-развлекательная деятельность (досуговое общение), художественное творчество.

Раздел 2. «Безопасность устройств»

Обучающийся научится:

- приводить примеры вредоносных кодов, способы доставки вредоносных кодов; исполняемые файлы и расширения вредоносных кодов; вредоносная рассылка.
- понимать и правильно применять на бытовом уровне методы защиты от вредоносных программ

Обучающийся получит возможность:

- сформировать представление о распространении вредоносного кода для мобильных устройств
- сформировать представление о вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Форма организации: беседа, просмотр презентации, видео; поисковые исследования; ролевые игры.

Виды деятельности: игровая, познавательная, проблемно-ценностное общение, досугово-развлекательная деятельность (досуговое общение), художественное творчество.

Раздел 3 «Безопасность информации»

Обучающийся научится:

- приводить примеры приемов социальной инженерии;
- понимать и правильно применять на бытовом уровне методы использования платежных карт в Интернете Обучающийся получит возможность;
- сформировать представление о распространении вредоносного кода для мобильных устройств;
- приводить примеры уязвимости Wi-Fi-соединений;
- сформировать представление о вредоносных кодах для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства;
- сформировать представление об основах государственной политики в области формирования культуры информационной безопасности.

Обучающийся получит возможность:

- сформировать представление о цифровом пространстве как площадка самопрезентации, экспериментирования и освоения различных социальных ролей
- сформировать представление о транзакциях и связанных с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов

Форма организации: беседа, просмотр презентации; поисковые исследования.
Виды деятельности: игровая, познавательная, проблемно-ценностное общение, досугово-развлекательная деятельность (досуговое общение), техническое творчество.

Тематическое планирование

№	Содержание	Количество часов
	Безопасность общения	
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	1
10.	Фишинг	1
11.	Выполнение индивидуальных и групповых проектов	1
12.	Выполнение индивидуальных и групповых проектов	1
13.	Защита индивидуальных и групповых проектов	1
	Безопасность устройств	
14.	Что такое вредоносный код	1
15.	Распространение вредоносного кода	1
16.	Методы защиты от вредоносных программ	1
17.	Методы защиты от вредоносных программ	1
18.	Распространение вредоносного кода для мобильных устройств	1
19.	Выполнение индивидуальных и групповых проектов	1
20.	Выполнение индивидуальных и групповых проектов	1
21.	Защита индивидуальных и групповых проектов	1
	Безопасность информации	
22.	Социальная инженерия: распознать и избежать	1
23.	Ложная информация в Интернете	1
24.	Безопасность при использовании платежных карт в Интернете	1
25.	Беспроводная технология связи	1
26.	Резервное копирование данных	1
27.	Основы государственной политики в области формирования культуры информационной безопасности	1
28.	Основы государственной политики в области формирования культуры информационной безопасности	1
29.	Выполнение индивидуальных и групповых проектов	1
30.	Выполнение индивидуальных и групповых проектов	1
31.	Защита индивидуальных и групповых проектов	1
32.	Повторение	1
33.	Волонтерская практика	1
34.	Резерв	1