

государственное бюджетное общеобразовательное учреждение
Самарской области
основная общеобразовательная школа №39
города Сызрани городского округа Сызрань Самарской области

Рассмотрена: на заседании МО учителей естественно- математического цикла Протокол № 1 от “ <u>30</u> ” августа 2023 г.	Проверена: Зам. директора по УВР _____ О.В. Лаврушкина «30» августа 2023 г.	Утверждена: Приказом № 636 от «31» августа 2023 г. Директор ГБОУ ООШ № 39 _____ И.Н. Лисина
--	---	--

РАБОЧАЯ ПРОГРАММА

по внеурочной деятельности

«Цифровая гигиена» 7 класс



S=RU, O=ГБОУ ООШ №39 г.о.
Сызрань, SN=Лисина И.Н.,
E=school39_szr@samara.edu.ru
00d340fc40a1294d3f
2023.12.07 08:20:54+04'00'

Год разработки программы – 2023 г.

Пояснительная записка

Рабочая программа внеурочной деятельности «Цифровая гигиена» модуль «Информационная безопасность» составлена на основе Информационная безопасность. На основе примерной рабочей программы учебного курса «Цифровая гигиена». Основное общее образование.- Самара, 2019. Рекомендована Координационным советом учебно – методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019. Данный курс внеурочной деятельности рассчитан на 1 год обучения общим объемом 34 часа (1 час в неделю).

1. 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.

2. Содержание курса

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 часа.

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

Тема 2. С кем безопасно общаться в интернете. 1 часа.

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 часа.

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

Тема 4. Безопасный вход в аккаунты. 1 часа.

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

Тема 5. Настройки конфиденциальности в социальных сетях. 1 часа.

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

Тема 6. Публикация информации в социальных сетях. 1 часа.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 часа.

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

Тема 8. Публичные аккаунты. 1 часа.

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 проектов. **2 часов.**

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 часа.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 часа.

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. 1 часа.

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

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 часа.

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

Выполнение и защита индивидуальных и групповых проектов. **1 часа.**

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 2 часа.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 2 часа.

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. 3 часа.

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

Тема 4. Беспроводная технология связи. 2 часа.

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

Тема 5. Резервное копирование данных. 2 часа.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 1 часа.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение индивидуальных и групповых проектов. 3 часов.

Повторение, волонтерская практика, резерв. 4 часа.

3. Тематическое планирование

№ п/п	Тема занятия	Количество	ЭОР
	Тема 1. «Безопасность общения»	12	
1	Общение в социальных сетях и мессенджерах	1	https://apkpro.ru/informatsionnaya-bezopasnost/
2	С кем безопасно общаться в интернете	1	https://apkpro.ru/informatsionnaya-bezopasnost/

3	Пароли для аккаунтов социальных сетей	1	https://apkpro.ru/informatsionnaya-bezopasnost/
4	Безопасный вход в аккаунты	1	https://apkpro.ru/informatsionnaya-bezopasnost/
5	Настройки конфиденциальности в социальных сетях	1	
6	Публикация информации в социальных сетях	1	https://apkpro.ru/informatsionnaya-bezopasnost/
7	Кибербуллинг	2	https://apkpro.ru/informatsionnaya-bezopasnost/
8	Публичные аккаунты	1	
9	Фишинг	1	https://apkpro.ru/informatsionnaya-bezopasnost/
10	Выполнение и защита индивидуальных и групповых проектов	2	
	Тема 2. «Безопасность устройств»	6	
11	Что такое вредоносный код	1	https://apkpro.ru/informatsionnaya-bezopasnost/
12	Распространение вредоносного кода	1	https://apkpro.ru/informatsionnaya-bezopasnost/
13	Методы защиты от вредоносных программ	1	https://apkpro.ru/informatsionnaya-bezopasnost/
14	Распространение вредоносного кода для мобильных устройств	1	https://apkpro.ru/informatsionnaya-bezopasnost/

15	Выполнение и защита индивидуальных и групповых проектов	2	
	Тема 3 «Безопасность информации»	16	
16	Социальная инженерия: распознать и избежать	1	https://apkpro.ru/inf ormatsionnaya-bezopasnost/
17	Ложная информация в Интернете	2	https://apkpro.ru/inf ormatsionnaya-bezopasnost/
18	Безопасность при использовании платежных карт в Интернете	2	https://apkpro.ru/inf ormatsionnaya-bezopasnost/
19	Беспроводная технология связи	2	https://apkpro.ru/inf ormatsionnaya-bezopasnost/
20	Резервное копирование данных	2	https://apkpro.ru/inf ormatsionnaya-bezopasnost/
21	Основы государственной политики в области формирования культуры информационной безопасности	1	https://apkpro.ru/inf ormatsionnaya-bezopasnost/
22	Выполнение и защита индивидуальных и групповых проектов	2	https://apkpro.ru/inf ormatsionnaya-bezopasnost/
23	Повторение, волонтерская практика, резерв	4	