

**Государственное бюджетное общеобразовательное учреждение Самарской области основная общеобразовательная школа № 32 города Сызрани городского округа Сызрань Самарской области**

РАССМОТРЕНА  
на заседании педагогического совета  
протокол № 2 от «28» августа 2024 г.

УТВЕРЖДАЮ:  
И.о.директора ГБОУ ООШ № 32 г.  
Сызрани

\_\_\_\_\_  
Е.А.Прокопенкова  
Приказ № 53 од от «28» августа 2024 г.

**РАБОЧАЯ ПРОГРАММА  
КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ  
«ЦИФРОВАЯ ГИГИЕНА»**

на 2024-2025 учебный год  
(8 класс)

Сызрань 2024 г.

## **ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

Данная программа разработана в соответствии с Федеральным государственным образовательным стандартом основного общего образования (Приказ Минобрнауки России № 287 от 31.05.2021г. «Об утверждении федерального государственного образовательного стандарта основного общего образования») и является модифицированной общеобразовательной программой, составленной на основе примерной рабочей программы учебного курса «Цифровая гигиена». Программа Рекомендована координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол №27 от 21.08.2019), Самара.

Сроки реализации образовательной программы: программа рассчитана на 1 год обучения.

Занятия по программе внеурочной деятельности «Цифровая гигиена» для учащихся 8 класса проводятся 1 раз в неделю по 1 часу, 34 часа в год. Общее количество часов – 34 часа.

### **1. Результаты освоения курса внеурочной деятельности**

#### ***Личностные результаты:***

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; и териоризация правил индивидуального и коллективного безопасного поведения в информационно- телекоммуникационной среде.

#### ***Метапредметные результаты:***

*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.

### ***Предметные результаты:***

#### *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.

## **Содержание курса внеурочной деятельности с указанием форм организации и видов деятельности 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 паро-лей. 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 кибербуллинга.

### **Тема 8. Публичные аккаунты.**

Настройки приватности публичных страниц. Правила ведения публичных 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 различных 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.

Формы организации: беседы, практикум, круглые столы, проект.

Виды деятельности: индивидуальные, групповые, индивидуально-групповые, фронтальные, практикумы, проектная деятельность.

| № п/п | Наименование разделов  | Всего часов | Из них     |               | Характеристика основных видов деятельности   | Формы организации занятий                           |
|-------|------------------------|-------------|------------|---------------|--|---|
|       |                        |             | аудиторные | внеаудиторные |  |   |
| 1     | Безопасность общения   | 13          | 13         | 0             | Выполняют базовые операции при использовании мессенджеров и социальных сетей. Создают свой образ в сети Интернет. Изучают историю и социальную значимость личных аккаунтов в сети Интернет. Руководствуются в общении социальными ценностями и установками коллектива и общества в целом. Изучают правила сетевого общения. Изучают основные понятия регистрационной информации и шифрования. Умеют их применить. Раскрывают причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле. Осуществляют поиск и используют информацию, необходимую для выполнения поставленных задач. | Лекция, практическая работа, проектная деятельность |
| 2     | Безопасность устройств | 8           | 8          | 0             | Соблюдают технику безопасности при эксплуатации компьютерных систем. Используют инструментальные программные средства. Изучают виды антивирусных программ и правила их установки. Разрабатывают презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для  | Лекция, практическая работа, проектная деятельность |

|   |                         |    |    |   |  |   |
|---|-------------------------|----|----|---|--|---|
|   |                         |    |    |   | учащихся более младшего возраста.  |   |
| 3 | Безопасность информации | 13 | 13 | 0 | Находят нужную информацию в базах данных, составляя запросы на поиск. Систематизируют получаемую информацию в процессе поиска. Определяют возможные источники необходимых сведений, осуществляет поиск информации. Отбирают и сравнивают материал по нескольким источникам. Анализируют и оценивают достоверность информации. Приводят примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывают возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете. Умеют привести | Лекция, практическая работа, проектная деятельность |

Тематическое планирование

| № Раздела | Тема (раздел)   | Количество часов на изучение |
|-----------|---|------------------------------|
| <b>1</b>  | <b>Безопасность общения</b>                             | <b>13</b>                    |
|           | Общение в социальных сетях и мессенджерах               | 1                            |
|           | С кем опасно общаться в интернете                       | 1                            |
|           | Пароли для аккаунтов социальных сетей                   | 1                            |
|           | Безопасный вход в аккаунты                              | 1                            |
|           | Настройки конфиденциальности в социальных сетях         | 1                            |
|           | Публикация информации в социальных сетях                | 1                            |
|           | Кибербулинг   | 1                            |
|           | Публичные аккаунты                                      | 1                            |
|           | Фишинг  | 2                            |
|           | Выполнение и защита индивидуальных и групповых проектов | 3                            |

|          |   |           |
|----------|---|-----------|
| <b>2</b> | <b><i>Безопасность устройств</i></b>  | <b>8</b>  |
|          | Что такое вредоносный код   | 1         |
|          | Распространение вредоносного кода   | 1         |
|          | Методы защиты от вредоносных программ   | 2         |
|          | Распространение вредоносного кода для мобильных устройств                                   | 1         |
|          | Выполнение и защита индивидуальных и групповых проектов                                     | 3         |
| <b>3</b> | <b><i>Безопасность информации</i></b>   | <b>13</b> |
|          | Социальная инженерия: распознать и избежать   | 1         |
|          | Ложная информация в Интернете   | 1         |
|          | Безопасность при использовании платежных карт в Интернете                                   | 1         |
|          | Беспроводная технология связи   | 1         |
|          | Резервное копирование данных  | 1         |
|          | Основы государственной политики в области формирования культуры информационной безопасности | 2         |
|          | Выполнение и защита индивидуальных и групповых проектов                                     | 3         |
| <b>4</b> | <b><i>Повторение, волонтерская практика, резерв</i></b>                                     | <b>3</b>  |
|          | Всего   | 34        |