

**государственное бюджетное общеобразовательное учреждение  
Самарской области средняя общеобразовательная школа № 9  
имени кавалера ордена Мужества Д.И.Герасименко  
«Центр образования» городского округа Октябрьск Самарской области**

**Рассмотрена**

на заседании  
методического  
объединения учителей  
Протокол № 1  
от «25» августа 2025г.

**Проверена**

Зам. директора по УВР  
\_\_\_\_\_ Е.А. Кузьмина  
«26» августа 2025 г.

**Утверждена**

Приказом № 419  
от «29» августа 2025г.  
И.о. директора школы  
\_\_\_\_\_ А.А. Мельдер

**РАБОЧАЯ ПРОГРАММА**  
**по внеурочной деятельности**  
**«Цифровая гигиена»**  
для обучающихся 7 класса

## **I. Пояснительная записка**

Программа по внеурочному курсу «Цифровая гигиена» составлена в соответствии с нормативно-правовыми документами:

- ✓ Федеральным законом «Об образовании в РФ» №273-ФЗ от 29.12.12г.;
- ✓ Приказом Минобрнауки России от 17.12.2010 г. №1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (в редакции от 29.12.2014 №1644, от 31 декабря 2015 г. N 1577);
- ✓ СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» (утвержден постановлением Главного государственного санитарного врача РФ 29.12.2010г. №189 (в редакции от 25.12.2013, 24 ноября 2015 г.);
- ✓ Примерной основной образовательной программой основного общего образования (одобрена решением федерального учебно- методического объединения по общему образованию (протокол от 8 апреля 2015 г. № 1/15, входит в специальный государственный реестр примерных основных образовательных программ, размещена на официальном сайте <http://edu.crowdexpert.ru/results-noo>).

**Основными целями** изучения курса «Цифровая гигиена» являются:

- ✓ Обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- ✓ Формирование навыков своевременного распознавания онлайн рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

**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, 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.

### **Общая характеристика учебного курса**

Курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

### **Описание места курса «Цифровая гигиена» в плане внеурочной деятельности**

В соответствии с планом внеурочной деятельности ГБОУ СОШ №9 «Центр образования» г.о.Октябрьск курс «Цифровая гигиена» реализуется в 7А классе в объеме 34 часа, из расчета 1 час в неделю. Продолжительность занятий 40 минут.

### **Формы текущего контроля и промежуточной аттестации**

Форма текущего контроля: устный опрос; наблюдение за самостоятельной работой обучающегося, за его умением работать в группе сверстников; практическая работа; рефлексия в форме вербального проговаривания или письменного выражения своего отношения к теме, собственному участию в совместной работе.

## **II. Планируемые результаты освоения курса внеурочной деятельности**

### **Предметные:**

- ✓ 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;
- ✓ 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;
- ✓ 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;
- ✓ договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- ✓ целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- ✓ 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;
- ✓ критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- ✓ делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его;
- ✓ выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации.

**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.

### **III. Содержание внеурочного курса внеурочной деятельности «Цифровая гигиена»**

#### **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 паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом 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. 2 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 час.

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. 3 часа.**

#### **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 расширение 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 программы 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 проектов. 3 часа.**

### 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. Поддельные 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.

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

Тема 5. Резервное копирование данных. 2 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 3 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 и защита индивидуальных и групповых проектов. 3 часа.**

**Тематическое планирование курса внеурочной деятельности «Цифровая гигиена» с указанием количества часов, отводимых на освоение каждой темы.**

| №                                         | Тема                                                                                        | Кол-во часов |
|-------------------------------------------|---------------------------------------------------------------------------------------------|--------------|
| <b>Раздел 1. «Безопасность общения»</b>   |                                                                                             |              |
| 1.                                        | Общение в социальных сетях и мессенджерах                                                   | 1            |
| 2.                                        | С кем безопаснообщаться 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            |
| <b>Раздел 2. «Безопасность устройств»</b> |                                                                                             |              |
| 1.                                        | Что такое вредоносный код                                                                   | 1            |
| 2.                                        | Распространение вредоносного кода                                                           | 1            |
| 3.                                        | Методы защиты от вредоносных программ                                                       | 2            |
| 4.                                        | Распространение вредоносного кода для мобильных устройств                                   | 1            |
| 5.                                        | Выполнение и защита индивидуальных и групповых проектов                                     | 3            |
| <b>Раздел 3 «Безопасность информации»</b> |                                                                                             |              |
| 1.                                        | Социальная инженерия: распознать и избежать                                                 | 1            |
| 2.                                        | Ложная информация в Интернете                                                               | 1            |
| 3.                                        | Безопасность при использовании платежных карт в Интернете                                   | 1            |
| 4.                                        | Беспроводная технология связи                                                               | 1            |
| 5.                                        | Резервное копирование данных                                                                | 2            |
| 6.                                        | Основы государственной политики в области формирования культуры информационной безопасности | 3            |
| 7.                                        | Выполнение и защита индивидуальных и групповых проектов                                     | 3            |