Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа №2 «Образовательный центр» имени Героя Советского Союза И. Т. Краснова с. Большая Глушица муниципального района Большеглушицкий Самарской области

| РАССМОТРЕНО | ПРОВЕРЕНО | УТВЕРЖДАЮ |
|---|---|---|
| на заседании педагогического совета протокол № 1 от 29.08. 2025 г. | заместитель директора по ВР /Ямщикова Е.А. от 29.08. 2025 г. | Директор ГБОУ СОШ №2 «ОЦ» с. Большая Глушица _____/Фёдоров Е. Ю. Приказ №634 от 29.08.2025г. |

**Рабочая программа**
**по внеурочной деятельности**
**Информационная безопасность «Цифровая гигиена»**
**7-9 класс**

Срок реализации – 3 года

C=RU, O="ГБОУ СОШ №2 ""ОЦ"" с. Большая Глушица", CN=Е.Ю. Фёдоров, E=school2_bgl@samara.edu.ru
008558f92923db0913
2025.09.22 10:42:29+04'00'

**с. Большая Глушица**
**2025 год**

Программа курса «Цифровая гигиена» адресована учащимся 7/8/9 классов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам.

**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, 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.

## 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.

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7/8/9 классов. Рекомендуется для реализации в рамках внеурочной деятельности обучающихся.

В преподавании курса «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

**Место учебного курса в учебном плане**

Программа учебного курса рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. На изучение курса «Информационная безопасность» отводится по 1 часу в неделю в 7/8/9 классах.

## Планируемые результаты освоения учебного курса

| № | Название раздела (темы) | Планируемые результаты | | |
|---|---|---|---|---|
| | | личностные | предметные | метапредметные |
| 1 | **Безопасность общения** | осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять в поведения в информационно-телекоммуникационной среде. | **Выпускник научится:**<br>- анализировать доменные имена компьютеров и адреса документов в интернете.<br>**Выпускник овладеет:**<br>- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.<br>**Выпускник получит возможность овладеть:**<br>- основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности; | **Регулятивные универсальные учебные действия.**<br>В результате освоения учебного курса обучающийся сможет:<br>- идентифицировать собственные проблемы и определять главную проблему;<br>- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;<br>**Познавательные универсальные учебные действия.**<br>В результате освоения учебного курса обучающийся сможет:<br>- выделять явление из общего ряда других явлений;<br>– определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;<br>– строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;<br>**Коммуникативные универсальные учебные действия.**<br>В результате освоения учебного курса обучающийся сможет: |

| | | | | |
|---|---|---|---|---|
| | | | | - строить позитивные отношения в процессе учебной и познавательной деятельности;<br>- критически относиться к собственному мнению, с достоинством признавать ошибочность своего |
| | | | | мнения (если оно таково) и корректировать его;<br>- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей; |

| | | | | |
|---|---|---|---|---|
| **2** | **Безопасность устройств** | 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; | **Выпускник научится:**<br>- безопасно использовать средства коммуникации;<br>**Выпускник овладеет:**<br>- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.<br>**Выпускник получит возможность овладеть:**<br>- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных. | **Регулятивные универсальные учебные действия.**<br>В результате освоения учебного курса обучающийся сможет:<br>- ставить цель деятельности на основе определенной проблемы и существующих возможностей;<br>- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;<br>**Познавательные универсальные учебные действия.**<br>В результате освоения учебного курса обучающийся сможет:<br>- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;<br>- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации; **Коммуникативные универсальные учебные действия.**<br>В результате освоения учебного курса<br>- делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.<br>- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ; |

| | | | | |
|---|---|---|---|---|
| **3** | **Безопасность информации** | 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. | **Выпускник научится:**<br>- безопасно вести и применять способы самозащиты при попытке мошенничества,<br>- безопасно использовать ресурсы интернета.<br>**Выпускник овладеет:**<br>- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.<br>**Выпускник получит возможность овладеть:** основами соблюдения норм информационной этики и права; | **Регулятивные универсальные учебные действия.**<br>В результате освоения учебного курса обучающийся сможет:<br>- составлять план решения проблемы (выполнения проекта, проведения исследования);<br>- 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;<br>**Познавательные универсальные учебные действия.**<br>В результате освоения учебного курса обучающийся сможет:<br>– критически оценивать содержание и форму текста;<br>– определять необходимые ключевые поисковые слова и запросы.<br>**Коммуникативные универсальные учебные действия.**<br>В результате освоения учебного курса<br>-выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;<br>- использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов). |

**Содержание программы учебного курса.**

Содержание программы учебного курса соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

| Тема раздела | Основное содержание по темам | Форма организации учебных занятий |
|---|---|---|
| **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. | Урок-лекция<br>Презентация к уроку |
| **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. | Урок-лекция<br>Презентация к уроку |
| **Тема 3. Пароли для аккаунтов социальных сетей. 1 час.** | Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. | Урок-лекция<br>Презентация к уроку |
| **Тема 4. Безопасный вход в аккаунты. 1 час.** | Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта. | Урок-лекция<br>Презентация к уроку |
| **Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.** | Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в | Урок-лекция<br>Практическая работа |
| | мессенджерах. | |

| | | |
|---|---|---|
| **Тема 6. Публикация информации в социальных сетях. 1 час.** | Персональные данные. Публикация личной информации. | Урок-лекция<br>Презентация к уроку |
| **Тема 7. Кибербуллинг. 1 час.** | Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. | Урок-лекция<br>Презентация к уроку |
| **Тема 8. Публичные аккаунты. 1 час.** | Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг. | Урок-лекция<br>Практическая работа |
| **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. | Урок-лекция<br>Презентация к уроку |
| **Выполнение и защита индивидуальных и групповых проектов. 3 часа.** | **Создание буклета и (или) презентации на тему «Безопасное общение в сети Интернет»** | Самостоятельная работа на ПК<br>Самостоятельная работа в сети Интернет |
| **Раздел №2. Безопасность устройств.** | | |
| **Тема 1. Что такое вредоносный код. 1 час.** | Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов. | Урок-лекция<br>Презентация к уроку |
| **Тема 2. Распространение вредоносного кода. 1 час.** | Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка.<br>Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах. | Урок-лекция<br>Презентация к уроку |
| **Тема 3. Методы защиты от вредоносных программ. 2 часа** | Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. | Урок-лекция<br>Презентация к уроку |
| **Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.** | Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства. | Урок-лекция<br>Презентация к уроку |

| | | |
|---|---|---|
| **Выполнение и защита индивидуальных и групповых проектов. 3 часа.** | **Создание буклета и (или) презентации на тему «Защита персональных данных при использовании мобильных устройств»** | Самостоятельная работа на ПК<br>Самостоятельная работа в сети Интернет |
| **Раздел №3 Безопасность информации.** | | |
| **Тема 1. Социальная инженерия: распознать и избежать. 1 час.** | Приемы социальной инженерии. Правила безопасности при виртуальных контактах. | Урок-лекция<br>Презентация к уроку |
| **Тема 2. Ложная информация в Интернете. 1 час.** | Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы. | Урок-лекция<br>Групповая работа в сети Интернет |
| **Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.** | Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов. | Урок-лекция<br>Презентация к уроку |
| **Тема 4. Беспроводная технология связи. 1 час.** | Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях. | Урок-лекция<br>Презентация к уроку |
| **Тема 5. Резервное копирование данных. 1 час.** | Безопасность личной информации. Создание резервных копий на различных устройствах. | Урок-лекция<br>Создание резервных копий на мобильных устройствах |
| **Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.** | Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности. | Урок-лекция<br>Презентация к уроку |
| **Выполнение и защита индивидуальных и групповых проектов. 3 часа.** | Создание буклета и (или) презентации на тему «Правила безопасности при виртуальных контактах» | Самостоятельная работа на ПК<br>Самостоятельная работа в сети Интернет |
| **Повторение. Волонтерская практика. 3 часа.** | | |

**Календарно - тематическое планирование учебного курса**

| № | Тема | Количество часов | Основное содержание | Характеристика основных видов учебной деятельности обучающихся | Дата |
|---|---|---|---|---|---|
| **Раздел 1. «Безопасность общения»** | | | | | |
| 1 | Общение в социальных сетях и мессенджерах. | 1 | Социальная сеть. История социальных сетей. Мессенджеры.. Назначение социальных сетей и мессенджеров. . Пользовательский контент. | Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет. | |
| 2 | С кем безопасно общаться в интернете | 1 | Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети. | Руководствуется в общении социальными ценностями установками коллектива, общества в целом. Изучает правила сетевого общения. | |
| 3 | Пароли для аккаунтов в социальных сетях | 1 | Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. | Изучает основные понятия регистрационной информации и шифрования. Умеет их применять. | |
| 4 | Безопасный вход в аккаунты | 1 | Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта. | Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа. | |
| 5 | Настройка конфиденциальности в социальных сетях. | 1 | Настрой ка приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах. | Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле. | |
| 6 | Публикация информации в социальных сетях | 1 | Персональные данные. Публикация личной информации. | Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач. | |
| 7 | Кибербуллинг | 1 | Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать. Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. | Реагирует на опасные ситуации, распознаѐт провокации и попытки манипуляции со стороны виртуальных собеседников. | |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Публичные аккаунты | 1 | Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг. | Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности. | |
| 9 | Фишинг | 2 | Фишинг как мошеннический приём. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах. | Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни или жизни знакомых. Разработка и распространение памятки по противодействию фишингу. | |
| 10 | Выполнение и защита индивидуальных и групповых проектов | 3 | Создание буклета и (или) презентации на тему «Безопасное общение в сети Интернет» | Самостоятельная работа. Работа в группах. | |
| **Раздел 2. «Безопасность устройств»** | | | | | |
| 11 | Что такое вредоносный код | 1 | Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов. | Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче. | |
| 12 | Распространение вредоносного кода | 1 | 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. | Выявляет и анализирует (при помощи чек- листа) возможные угрозы информационной безопасности объектов. | |
| 13 | Методы защиты от вредоносных программ | 2 | Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. | Изучает виды антивирусных программ и правила их установки. | |
| 14 | Распространение вредоносного кода для мобильных устройств | 1 | Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства. | Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста. | |
| 15 | Выполнение и защита индивидуальных и групповых проектов | 3 | Создание буклета и (или) презентации на тему «Защита персональных данных при использовании мобильных устройств» | Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | (аргументы), факты; гипотезы, аксиомы, теории. | |
| **Раздел 3 «Безопасность информации»** | | | | | |
| 16 | Социальная инженерия: распознать и избежать | 1 | Приемы социальной инженерии. Правила безопасности при виртуальных контактах | Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска. | |
| 17 | Ложная информация в Интернете | 1 | Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы. | Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. | |
| 18 | Безопасность при использовании платежных карт в Интернете | 1 | Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов. | Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете. | |
| 19 | Беспроводная технология связи | 1 | Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях. | Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов. | |
| 20 | Резервное копирование данных | 1 | Безопасность личной информации. Создание резервных копий на различных устройствах. | Создает резервные копии. | |
| 21 | Основы государственной политики в области формирования культуры информационной безопасности | 2 | Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности. | Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства. | |
| 22 | Выполнение и защита индивидуальных и групповых проектов | 3 | | Создание буклета и (или) презентации на тему «Правила безопасности при виртуальных контактах» | |
| 23 | Повторение, волонтерская | 3 | | Проведение мероприятий по сетевой | |
| | практика, резерв | | | безопасности с учащимися ОУ. | |
| **ИТОГО** | | 34 | | | |