

Муниципальное общеобразовательное учреждение  
«Средняя общеобразовательная школа № 4 имени Героя труда Ставрополя  
П.В. Лобанова», пос. Верхнестепной, Степновского муниципального округа  
Ставропольского края

Принята на заседании  
педагогического совета  
протокол № 5

от « 28 » 10 2024 г

Утверждаю  
Директор МОУ СОШ № 4  
П. В. Лобанова, пос. Верхнестепной  
С.В. Кульчитская  
« 28 » 10 2024 г



# Рабочая программа курса внеурочной деятельности «Цифровая гигиена»

Возраст: 13-16 лет  
Срок реализации: 1 год

Составитель:  
Беклемышева Мария Александровна,  
педагог дополнительного образования

пос. Верхнестепной, 2024 г

## Пояснительная записка

Примерная рабочая программа курса внеурочной деятельности «Цифровая гигиена» составлена на основе:

- Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;
- Федерального государственного образовательного стандарта основного общего образования (далее ФГОС ООО), утвержденного Приказом Министерства просвещения Российской Федерации от 31 мая 2021 г. № 287;
- Федеральной образовательной программы основного общего образования (далее – ФОП ООО), утвержденной приказом Министерства просвещения Российской Федерации от 18 мая 2023 г. № 370.

Программа курса «Цифровая гигиена» адресована обучающимся 7-11-х классов, а также родителям обучающихся всех возрастов 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.

Курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры) 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 8-х классов. Рекомендуются для реализации в рамках внеурочной деятельности обучающихся.

В преподавании модуля «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), 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.).

**Срок реализации программы:** 1 учебный год.

**Объём освоения программы:**

количество недель – 36,

количество часов – 108.

**Режим занятий:** 3 занятия в неделю, в т. ч. 1 час – подготовка к конкурсам.

**Форма обучения:** очная

**Форма проведения занятий:** групповая, индивидуальная.

**Адресат программы:** Программа предназначена для детей 13-16 лет и рассчитана на 1 год обучения. Группы формируются по возрастному признаку, без предварительного тестирования с учетом наполняемости групп.

**Основной целью** изучения курса «Цифровая гигиена» является:

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.

## Планируемые результаты

### *Предметные и 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 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.

Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн-занятия, подготовленные в ходе выполнения учебных заданий по основным темам курса.

### **Содержание учебного курса**

#### **Введение. Инструктаж по технике безопасности (2 часа)**

#### **Раздел 1. «Безопасность общения»**

##### **Тема 1. Общение в социальных сетях и мессенджерах (2 часа)**

Теория. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров.

Практика. Пользовательский контент.

##### **Тема 2. С кем безопасно общаться в интернете (2 часа)**

Теория. Персональные данные как основной капитал личного пространства в цифровом мире.

Практика. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

##### **Тема 3. Пароли для аккаунтов социальных сетей (3 часа)**

Теория. Сложные пароли. Онлайн-генераторы паролей. Правила хранения паролей.

Практика. Использование функции браузера по запоминанию паролей.

##### **Тема 4. Безопасный вход в аккаунты (3 часа)**

Теория. Виды аутентификации.

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

##### **Тема 5. Настройки конфиденциальности в социальных сетях (3 часа)**

Теория. Настройки приватности и конфиденциальности в разных социальных сетях.

Практика. Приватность и конфиденциальность в мессенджерах.

##### **Тема 6. Публикация информации в социальных сетях (3 часа)**

Теория. Персональные данные.

Практика. Публикация личной информации.

##### **Тема 7. Кибербуллинг (3 часа)**

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

## **Тема 8. Публичные аккаунты (8 часа)**

Теория. Настройки приватности публичных страниц.

Практика. Правила ведения публичных страниц. Овершеринг.

## **Тема 9. Фишинг (3 часа)**

Теория. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов.

Практика. Как защититься от фишеров в социальных сетях и мессенджерах.

## **Выполнение и защита индивидуальных и групповых проектов (8 часов)**

### **Раздел 2. «Безопасность устройств»**

#### **Тема 1. Что такое вредоносный код (3 часа)**

Теория. Виды вредоносных кодов.

Практика. Возможности и деструктивные функции вредоносных кодов.

#### **Тема 2. Распространение вредоносного кода (3 часа)**

Теория. Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты.

Практика. Способы выявления наличия вредоносных кодов на устройствах.

Действия при обнаружении вредоносных кодов на устройствах.

#### **Тема 3. Методы защиты от вредоносных программ (3 часа)**

Теория. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики.

Практика. Правила защиты от вредоносных кодов.

#### **Тема 4. Распространение вредоносного кода для мобильных устройств (3 часа)**

Теория. Расширение вредоносных кодов для мобильных устройств.

Практика. Правила безопасности при установке приложений на мобильные устройства.

## **Выполнение и защита индивидуальных и групповых проектов (8 часа)**

### **Раздел 3 «Безопасность информации»**

#### **Тема 1. Социальная инженерия: распознать и избежать (4 часа)**

Теория. Приемы социальной инженерии.

Практика. Правила безопасности при виртуальных контактах.

#### **Тема 2. Ложная информация в Интернете (4 часа)**

Теория. Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей.

Практика. Фейковые новости. Поддельные страницы.

#### **Тема 3. Безопасность при использовании платежных карт в Интернете (4 часа)**

Теория. Транзакции и связанные с ними риски. Правила совершения онлайн-покупок.

Практика. Безопасность банковских сервисов.

#### **Тема 4. Беспроводная технология связи (4 часа)**

Теория. Уязвимость Wi-Fi-соединений. Публичные и непубличные сети.

Практика. Правила работы в публичных сетях.

#### **Тема 5. Резервное копирование данных (4 часа)**

Теория. Безопасность личной информации.

Практика. Создание резервных копий на различных устройствах.

**Тема 6. Основы государственной политики в области формирования культуры информационной безопасности (3 часа)**

Теория. Доктрина национальной информационной безопасности.

Обеспечение свободы и равенства доступа к информации и знаниям.

Практика. Основные направления государственной политики в области формирования культуры информационной безопасности.

**Выполнение и защита индивидуальных и групповых проектов (9 часов) Повторение. Волонтерская практика (5 часов)**

**Учебный план**

№ п/п	Разделы	Количество часов		
		всего	теория	практика
1	Введение. Инструктаж по технике безопасности	2	2	0
2	«Безопасность общения»	43	33	10
3	«Безопасность устройств»	24	16	8
4	«Безопасность информации»	39	26	13
<b>Итого</b>		<b>108</b>	<b>77</b>	<b>41</b>



## Календарно - тематическое планирование учебного курса

№ п/п	Тема	Кол-во часов	Дата	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
1	Введение. Инструктаж по технике безопасности	2			
<b>Тема 1. «Безопасность общения»</b>					
2	Общение в социальных сетях и мессенджерах	2		Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров.	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
3	Пользовательский контент	2			
4	С кем безопасно общаться в интернете	3		Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя.	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения
5	Профили	2			
6	Анонимные социальные сети	2			
7	Пароли для аккаунтов социальных сетей	3		Сложные пароли. Онлайн-генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить

8					
9	Безопасный вход в аккаунты	2		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
10	Виды аутентификации.	2			
11	Настройки конфиденциальности в социальных сетях	3		Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле
12	Публикация информации в социальных сетях	3		Персональные данные. Публикация личной информации	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач
13	Кибербуллинг	3		Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников
14	Публичные аккаунты	3		Настройки приватности публичных страниц. Правила	Решает экспериментальные задачи. Самостоятельно создает источники

				ведения публичных страниц. Овершеринг	информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности
15	Фишинг	3		Фишинг как мошеннический прием. Популярные варианты. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу
16	Распространения фишинга	2			
17	Выполнение и защита индивидуальных и групповых проектов	8			Самостоятельная работа
<b>Тема 2. «Безопасность устройств»</b>					
18	Что такое вредоносный код	3		Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче
19	Распространение вредоносного кода	3		Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов

				Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах	
20	Методы защиты от вредоносных программ	3		Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила Защиты от вредоносных кодов	Изучает виды антивирусных программ и правила их установки
21	Распространение вредоносного кода для мобильных устройств	3		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
22	Выполнение и защита индивидуальных и групповых проектов	8			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

### Тема 3 «Безопасность информации»

23	Социальная инженерия: распознать и избежать	2		Приемы социальной инженерии. Правила безопасности при виртуальных контактах	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска
24	Ложная информация в Интернете	2		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. Анализирует и оценивает достоверность информации
25	Безопасность при использовании платежных карт в Интернете	2		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
26	Онлайн-покупки	2			
27	Беспроводная технология связи	2		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
28	Wi-Fi-соединения	2			
29	Резервное копирование данных	2		Безопасность личной информации. Создание	Создает резервные копии

30	Копии	2		резервных копий на различных устройствах	
31	Основы государственной политики в области формирования культуры информационной безопасности	3		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.
32	Выполнение и защита индивидуальных и групповых проектов	9			Выполняет проектную работу по одной из тем, предложенных на выбор учащихся и/или проверочного теста
33	Повторение, волонтерская практика, резерв	5			Проводит занятия для обучающихся 4-6 классов в качестве волонтерской практики
<b>Итого</b>		<b>102</b>			

## **Материально-техническое обеспечение:**

**Оборудование «Точки роста»:** мультимедийный комплекс, ноутбуки, МФУ.

### **Используемая литература:**

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с
2. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.
4. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2016. – 239 с.
5. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.
6. Защита детей by Kaspersky // <https://kids.kaspersky.ru/>
7. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Ру сайнс, 2017. – 64 с.
8. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.
9. Основы кибербезопасности. // <https://www.xn--d1abkefqip0a2f.xn-p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa>
10. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
11. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. № 22(66)
12. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.

