

**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**Министерство образования и науки Самарской области**  
**Северное управление**  
**ГБОУ ООШ с. Сидоровка**

РАССМОТРЕНО  
на заседании МО  
Протокол № 1  
от «31» августа 2023 г.

СОГЛАСОВАНО  
Заместитель директора по  
УВР  
«31» августа 2023 г.

УТВЕРЖДЕНО  
и.о. директора ГБОУ  
ООШ с.Сидоровка  
\_\_\_\_\_  
Власов А.О.  
Приказ № 115  
от «31» августа 2023 г.

**Рабочая программа**  
**курса внеурочной деятельности «Информационная безопасность»**

для обучающихся 7 класса  
Количество часов- 34ч.  
Срок реализации 1 год

Приложение к ООП ООО

## Пояснительная записка

Программа курса «Цифровая гигиена» адресована учащимся 7-9 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.

**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 ответственности 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.

Данный курс предполагает организацию работы в соответствии с содержанием 2-х модулей, предназначенных для обучающихся 7-9 классов и родителей обучающихся любого возраста соответственно.

## **Модуль 1. «Информационная безопасность»**

### **ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОГО ПРЕДМЕТА**

*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 УЧЕБНОГО ПРЕДМЕТА**

#### **Модуль 1.**

##### **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. 1 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 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** 3 часа.

**Повторение** 1 час.

**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 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. 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.

**Повторение** 1 час.

**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.

Требования к содержанию итоговых проектно-исследовательских работ содержатся в приложении 1 к данной рабочей программе

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

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных 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.

**Выполнение и защита индивидуальных и групповых проектов** 3 часа.

**Повторение** 1 час.

## ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ УЧЕБНОГО ПРЕДМЕТА

	Тема раздела	Количество часов	Деятельность учителя с учетом программы воспитания (модуля «Школьный урок»)
	Модуль 1.Раздел 1. «Безопасность общения»	10	Побуждение обучающихся соблюдать на уроке нормы поведения, правила общения со сверстниками и учителем, соответствующие укладу школы, установление и поддержка доброжелательной атмосферы. Установление доверительных отношений между учителем и учениками, способствующих позитивному восприятию требований, привлечению внимания к изучаемой проблеме
	Раздел 2. «Безопасность устройств»	5	Применение видов деятельности обучающихся со словесной (знаковой) основой: самостоятельная работа с учебником, работа с научно-популярной литературой, разбор и сравнение материала по нескольким источникам, что позволит обучающимся приобретать опыт самостоятельного поиска, анализа и отбора информации для решения поставленных задач.
	Раздел 3 «Безопасность информации»	7	Включение в урок игровых процедур, которые помогают поддержать мотивацию детей к получению знаний (лекция с запланированными ошибками, наличие двигательной активности на уроках), налаживанию позитивных межличностных отношений в классе, помогают установлению доброжелательной атмосферы во время урока (сотрудничество, поощрение, доверие, получение важного дела, создание ситуации успеха).
	Выполнение и защита индивидуальных и групповых проектов	9	Инициирование и поддержка исследовательской деятельности в форме индивидуальных и групповых проектов, что дает возможность

			приобрести навыки самостоятельного решения теоретической проблемы, генерирования и оформления собственных идей, уважительного отношения к чужим идеям, публичного выступления, аргументирования и отстаивания своей точки зрения
	Повторение	3	Применение на уроке интерактивных форм работы учащихся: дискуссий, которые дают учащимся возможность приобрести опыт ведения конструктивного диалога в атмосфере нравственных и эстетических переживаний, столкновений различных взглядов и мнений, поиска истины и возможных путей решения задачи или проблемы, творчества учителя и учащихся.
	<b>Всего</b>	<b>34</b>	

## Модуль 2.

При работе с родителями важнейшей задачей является преодоление «цифрового разрыва» и обучение родителей правильной оценке своих возможностей в помощи детям в Интернете – возможностей, которые достаточно велики.

Разработчики курса предполагают, что родители с большей готовностью включатся в программу развития цифровой гигиены, предлагающую им общение, совместный поиск и развивающие игры и т.п.

Вместе с тем, формами проведения мероприятий для родителей также могут являться: лектории, выступления на родительских собраниях, микро- обучение на основе технологий онлайн обучения, геймификация, создание чек-листов, совместное обучение, совместные родительско-детские проекты и пр.

Практические материалы для реализации данного модуля представлены в приложении 2 к данной рабочей программе. Разработчики курса «Цифровая гигиена» предлагают использовать вышеуказанное приложение в качестве конструктора при подготовке к мероприятиям.

### Тематическое планирование учебного курса (Модуль 2).

**Тема 1. История возникновения Интернета. Понятия Интернет- угроз. Изменения границ допустимого в контексте цифрового образа жизни**

Тема 2. Изменения нормативных моделей развития и здоровья детей и подростков.

**Тема 3. Цифровая гигиена: зачем это нужно? Понятие периметра безопасности. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка. Баланс ценностей развития и ценностей безопасности.**

Тема 4. Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

**Тема 5. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребёнка для профилактики насилия в Сети?**

Тема 6. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?

**Тема 7. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.**

Тема 8. Пособия и обучающие программы по формированию навыков цифровой гигиены.