

Государственное бюджетное общеобразовательное учреждение
Самарской области средняя общеобразовательная школа
с. Шилан муниципального района Красноярский
Самарской области

«РАССМОТРЕНО»

На заседании

Методического объединения

Протокол № 1 от «29»08.2022 г.

«ПРОВЕРЕНО»

Заместитель директора по УВР

_____ (Мартынова В.Е.)

«29» 08.2022г.

«УТВЕРЖДАЮ»

Директор ГБОУ СОШ

с. Шилан

_____ (Тынянов Н.П.)

приказ № 69/1-од

от «29» 08.2022г.

Рабочая программа
по внеурочной деятельности
«Цифровая гигиена»
7 класс
(социальное направление)

с.Шилан

2022 г.

Пояснительная записка.

Рабочая программа разработана в соответствии с нормативной базой организации внеурочной деятельности:

- Федерального закона от 29.12.2012 № 273 «Об образовании в Российской Федерации»;
- Приказа Минпросвещения от 31.05.2021 № 286 «Об утверждении федерального государственного образовательного стандарта начального общего образования»;
- Приказа Минпросвещения от 31.05.2021 № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования»;
- СанПиН 1.2.3685-21;
- Основной образовательной программой основного общего образования Государственного бюджетного общеобразовательного учреждения средняя общеобразовательная школа с.Шилан;
- Рабочей программой воспитания Государственного бюджетного общеобразовательного учреждения средняя общеобразовательная школа с.Шилан.

Основными целями изучения курса «Цифровая гигиена» являются:

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

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.

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

Годовая промежуточная аттестация проводится в форме тестирования.

II. Планируемые результаты освоения курса внеурочной деятельности

Предметные:

1. анализировать доменные имена компьютеров и адреса документов в Интернете;
2. безопасно использовать средства коммуникации;
3. безопасно вести и применять способы самозащиты при попытке мошенничества;
4. 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;
- 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.

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 внеурочного курса.

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.

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.

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 3. Беспроводная технология связи. 1 час.

Уязвимость Wi-Fi-

соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 4. 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.

Календарно – тематическое планирование.

№ п/п	Название темы	Кол – во часов
Безопасность общения		
1	Общение в социальных сетях и мессенджерах	1
2	С кем безопасно общаться в интернете	1
3	Пароли для аккаунтов социальных сетей	1
4	Безопасный вход в аккаунты	
5	Настройки конфиденциальности в социальных сетях	1
6	Публикация информации в социальных сетях	1
7	Кибербуллинг	1
8	Публичные аккаунты	1
9-10	Фишинг	2
«Безопасность устройств»		
1	Что такое вредоносный код	1
2	Распространение вредоносного кода	1
3-4	Методы защиты от вредоносных программ	2
5	Распространение вредоносного кода для мобильных устройств	1
6-8	Выполнение и защита индивидуальных и групповых проектов	3
«Безопасность информации»		
1-2	Социальная инженерия: распознать и избежать	2
3-4	Ложная информация в Интернете	
5	Безопасность при использовании платежных карт в Интернете	
6	Беспроводная технология связи	
7-8	Резервное копирование данных	2
9-10	Основы государственной политики в области формирования культуры информационной безопасности	2
11-13	Выполнение и защита индивидуальных и групповых проектов	3

14	Годовая промежуточная аттестация	1
15	Разбор типичных ошибок аттестационной работы	1
16	Итоговое занятие	1