

Государственное бюджетное общеобразовательное учреждение Самарской области основная общеобразовательная школа с. Верхнее Санчелеево муниципального района Ставропольский Самарской области

Согласовано

Протокол № 8 Методического Совета
от «27» июня 2024 г.

Утверждено

Директор ГБОУ ООШ с. Верхнее Санчелеево
Приказ № 194-од от «27» июня 2024 г.
Н.П. Безроднова



C=RU, O=ГБОУ
ООШ с.
Верхнее
Санчелеево,
CN=Безродн
ова Наталья
Петровна,
E=bezrodnova
1979@mail.ru
2023.10.05
10:11:
25+04'00'

**Рабочая программа
внеурочной деятельности
«Цифровая гигиена»
7 класс
(обеспечение безопасности жизни и здоровья
обучающихся)**

Составитель: учитель информатики
Ж.Ю. Дергунова

СОДЕРЖАНИЕ

| | |
|---|----|
| Пояснительная записка | 3 |
| Содержание обучения | 5 |
| Планируемые результаты освоения программы | 7 |
| Тематическое планирование | 11 |
| Учебно-методическое обеспечение образовательного процесса | 11 |

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Основополагающими при проектировании и составлении программы внеурочной деятельности «Цифровая гигиена» являются следующие документы:

1. Федеральный закон об образовании в Российской Федерации от 29.12.2012 №273-ФЗ (с изменениями и дополнениями).

2. Федеральный закон от 31 июля 2020 г. № 304-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся».

3. Концепция развития дополнительного образования детей до 2030 года, утвержденная Распоряжением Правительства РФ от 31 марта 2022 г. №678-р;

4. Федеральный проект «Успех каждого ребенка» в рамках Национального проекта «Образование», утвержденного Протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 3.09.2018 №10.

5. Приказ Министерства просвещения Российской Федерации от 3.09.2019 №467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей».

6. Федеральный закон от 13 июля 2020 г. №189-ФЗ «О государственном (муниципальном) социальном заказе на оказание государственных (муниципальных) услуг в социальной сфере» (с изменениями и дополнениями, вступившими в силу с 28.12.2022 г.).

7. Приказ Министерства просвещения Российской Федерации от 27 июля 2022 г. №629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам».

Актуальность программы. Предлагаемая программа внеурочной деятельности предназначена для обучающихся 7 классов и носит пропедевтический характер поведения обучающихся в виртуальном мире.

Концепция обучения ориентирована на расширение основных тем по

учебным предметам «Информатика» и «Основы безопасности жизнедеятельности» 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.

Цели программы:

- формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

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.

Основные виды и формы учебных занятий:

Демонстрационная - работу на компьютере выполняет учитель, а учащиеся наблюдают.

Фронтальная - недлительная, но синхронная работа учащихся по освоению или закреплению материала под руководством учителя.

Самостоятельная- выполнение самостоятельной работы с компьютером в пределах одного, двух или части урока. Учитель обеспечивает индивидуальный контроль за работой учащихся.

Творческий проект – выполнение работы в микро группах на протяжении нескольких занятий

Работа консультантов – ученик контролирует работу всей группы.

Форма контроля

В качестве домашнего задания предлагаются задания для учащихся по сбору и изучению информации по выбранной теме.

Контроль осуществляется в форме творческих проектов, самостоятельной разработки работ.

СОДЕРЖАНИЕ ОБУЧЕНИЯ

Раздел 1 «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 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. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Тема 10. Выполнение и защита индивидуальных и групповых проектов.

Раздел 2 «Безопасность устройств»

Тема 1 Что такое вредоносный код. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2 Распространение вредоносного кода. 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. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4 Распространение вредоносного кода для мобильных устройств. Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Тема 5 Выполнение и защита индивидуальных и групповых проектов.

Раздел 3 «Безопасность информации»

Тема 1 Социальная инженерия: распознать и избежать. Приемы социальной инженерии.

Правила безопасности при виртуальных контактах.

Тема 2 Ложная информация в Интернете. Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3 Безопасность при использовании платежных карт в Интернете. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4 Беспроводная технология связи. Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5 Резервное копирование данных. Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6 Основы государственной политики в области формирования культуры информационной безопасности. Доктрина национальной информационной безопасности.

Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ

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.

Метапредметные результаты:

Регулятивные:

- 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:

- 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

- 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 информацию с учетом этических и правовых норм;
- создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Предметные:

Обучающиеся научатся:

- 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.

Обучающиеся получат возможность научиться:

- приемам безопасной организации своего личного пространства данных, использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

- основам соблюдения норм информационной этики и права;
- основам 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.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

| № | Содержание | Количество часов |
|-------|-------------------------|------------------|
| 1. | Безопасность общения | 13 |
| 2. | Безопасность устройств | 8 |
| 3. | Безопасность информации | 13 |
| ИТОГО | | 34 |

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Учебно-методический комплекс программы «Логические и арифметические основы информатики» включает учебное пособие, программу, практические и контрольные работы, тесты.

Аппаратное обеспечение:

1. Моноблок и 12 ноутбуков.
2. Мультимедийный проектор, экран
3. Принтер, сканер
4. Видео – и DVD- проигрыватели
5. Интернет

Программное обеспечение:

ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ МАТЕРИАЛЫ ДЛЯ УЧЕНИКА

1. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019 – 80 с.

2. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УЧИТЕЛЯ

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. Дети в информационном обществе <http://detionline.com/journal/about>

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.: Русайнс, 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. 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.