государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа № 4 п.г.т. Алексеевка городского округа Кинель Самарской области

СОГЛАСОВАНО
на заседании
методического объединения
Протокол №1 от 29.08.2023

ПРОВЕРЕНО
зам. директора по ВР
_____Хасанмурадова З.Д.
от 30.08.2023

УТВЕРЖДАЮ
директор ГБОУ СОШ №4
п.г.т. Алексеевка
_____/Т.Н. Соболева/
Приказ №171-о от 31.08.2023

О=ГБОУ СОШ №4 п.г.т. Алексеевка, CN=Соболева Т.Н., E=tanusha080875@mail.ru
00f3912be085840487
2023.08.31 10:08:40+04'00'

РАБОЧАЯ ПРОГРАММА
ПО ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«Информационная безопасность»
(цифровая гигиена)
7 и 9 классы

Пояснительная записка

Рабочая программа по «Цифровой гигиене» для основной школы составлена в соответствии с:

1. Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
2. Федеральным государственным образовательным стандартом основного общего образования (далее ФГОС ООО), утвержденный Приказом Министерства образования и науки Российской Федерации от «31» мая 2021 г. № 287;
3. Перечень учебников, рекомендованных к использованию при реализации имеющих государственную аккредитацию образовательных программ начального общего, основного общего, среднего общего образования, осуществляющими образовательную деятельность за 2018 г.;
4. Основной образовательной программой основного общего образования ГБОУ СОШ № 4 п.г.т. Алексеевка;
5. Учебным планом ГБОУ СОШ № 4 п.г.т. Алексеевка.

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.

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).

Основные 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.

Количество часов, отведенных на изучение дисциплины.

В соответствии с учебным планом ГБОУ СОШ № 4 п.г.т. Алексеевка на освоение программы отведено следующее количество часов:

Распределение учебного времени представлено в таблице.

Класс	Количество часов на ступени основного образования
7	34
9	34
Всего	68

Форма контроля на занятиях информационной безопасности: текущий, периодический, итоговый и самоконтроль.

Виды контроля: тест, самостоятельная работа.

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 8-9 классов и родителей обучающихся любого возраста соответственно.

Модуль 1. «Информационная безопасность»

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и

познавательных возможностей, обучающихся 7, 9 классов. Рекомендуется 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 кейсметоду), 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.)

Характеристика личностных, метапредметных и предметных результатов освоения учебного курса (Модуль 1)

Предметные:

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.

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.

За счет часов, предусмотренных для повторения материала (4 часа), возможно проведение занятий для учащихся 4-6 классов. Эти занятия в качестве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные в ходе выполнения учебных занятий по основным темам курса.

Содержание учебного курса 7 класс.

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.

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.

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.

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 часа.

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.

Тематическое планирование учебного курса 9 класс.

Тема 1. Информация и личность. 6 часов.

Информация. Источники информации. Виды информационных воздействий. Информационная безопасность. Угрозы информационной безопасности. Передача информации в условиях вынужденного автономного существования. Роль информации в обеспечении личной безопасности. Уровни и меры защиты информации. Защиты персональной информации. Информация и права потребителя.

Тема 2. Информация и здоровье. 6 часов.

Влияние информации на здоровье человека. Оценка информационных влияний (мотив, цель, средства, реальные результаты). Методы и средства защиты человека от негативного воздействия информации. Дезинформация. Реклама.

Тема 3. Информация и компьютер. 4 часа.

Виды угроз для цифровой информации. Программно-технические меры обеспечения информационной безопасности (параметры безопасности, управление доступом). Программно-технические меры обеспечения информационной безопасности (антивирусные программы). Виды программного обеспечения (лицензионное, условно бесплатное, свободно распространяемое). Условия использования.

Тема 4. Информация и общество. 5 часов.

Роль информации в социальных отношениях. Негативные проявления массовой культуры. Информационная безопасность и СМИ. Влияние образной информации на человека. Информационная война. Информационный терроризм.

Тема 5. Информационная безопасность в сети. 4 часа.

Виды и особенности сетевых информационных угроз. Необходимость различных форм контроля над информационными потоками. Программные средства родительского контроля. Обеспечение информационной безопасности обучающихся. Системы контентной фильтрации.

Тема 6. Правовые основы обеспечения информационной безопасности. 5 часов.

Свобода доступа к информации и свобода ее распространения. Защита интеллектуальной собственности. Авторское право и тиражирование Криптография и защита информации. ЭЦП и сертификаты. Правовое регулирование в информационной сфере. Информационная безопасность как составляющая национальной безопасности.

Разработка и защита проектов.4 часа.

Тематическое планирование

Раздел	количество часов
7 класс	
Безопасность общения	**13**
Общение в социальных сетях и мессенджерах	1
С кем безопасно общаться в интернете	1
Пароли для аккаунтов социальных сетей	1
Безопасный вход в аккаунты	1
Настройки конфиденциальности в социальных сетях	1
Публикация информации в социальных сетях	1
Кибербуллинг	1
Публичные аккаунты	1
Фишинг	2
Выполнение и защита индивидуальных и групповых проектов	3
Безопасность устройств	**8**
Что такое вредоносный код	1
Распространение вредоносного кода	1
Методы защиты от вредоносных программ	2
Распространение вредоносного кода для мобильных устройств	1
Выполнение и защита индивидуальных и групповых проектов	3
Безопасность информации	**13**
Социальная инженерия: распознать и избежать	1
Ложная информация в Интернете	1
Безопасность при использовании платежных карт в Интернете	1
Беспроводная технология связи	1
Резервное копирование данных	1
Основы государственной политики в области формирования культуры информационной безопасности	2
Выполнение и защита индивидуальных и групповых проектов	3
Повторение	2
Итоговое тестирование на знание информационной безопасности	1
Итого	**34**
9 класс	
Информация и личность	**6**
Информация. Источники информации. Виды	1

информационных воздействий	
Информационная безопасность. Угрозы информационной безопасности.	1
Передача информации в условиях вынужденного автономного существования.	1
Роль информации в обеспечении личной безопасности.	1
Уровни и меры защиты информации. Защиты персональной информации.	1
Информация и права потребителя.	1
Информация и здоровье	**6**
Влияние информации на здоровье человека.	1
Оценка информационных влияний (мотив, цель, средства, реальные результаты). Дезинформация. Реклама.	3
Методы и средства защиты человека от негативного воздействия информации.	2
Информация и компьютер	**4**
Виды угроз для цифровой информации.	1
Программно-технические меры обеспечения информационной безопасности (параметры безопасности, управление доступом).	1
Программно-технические меры обеспечения информационной безопасности (антивирусные программы).	1
Виды программного обеспечения (лицензионное, условно бесплатное, свободно распространяемое). Условия использования.	1
Информация и общество.	**5**
Роль информации в социальных отношениях.	1
Негативные проявления массовой культуры.	1
Информационная безопасность и СМИ. Влияние образной информации на человека.	1
Информационная война.	1
Информационный терроризм.	1
Информационная безопасность в сети	**4**
Виды и особенности сетевых информационных угроз.	1
Необходимость различных форм контроля над информационными потоками.	1
Программные средства родительского контроля.	1
Обеспечение информационной безопасности обучающихся. Системы контентной фильтрации.	1
Правовые основы обеспечения информационной безопасности.	**5**
Свобода доступа к информации и свобода ее	1

распространения.	
Защита интеллектуальной собственности. Авторское право и тиражирование.	1
Криптография и защита информации. ЭЦП и сертификаты.	1
Правовое регулирование в информационной сфере.	1
Информационная безопасность как составляющая национальной безопасности.	1
Разработка и защита проекта	**4**
Итого	**34**

Планируемые результаты изучения учебного предмета

Выпускник научится:

– работать 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);

– необходимым умениям, для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственное отношение к взаимодействию в современной информационно - телекоммуникационной среде;

– применять 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.;

– применять 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;

– профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Требования к содержанию итоговых

проектно-исследовательских работ.

Критерии содержания текста проектно-исследовательской работы.

1. Во введении сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована, но при этом четко определена, в необходимости исследования есть аргументы.
2. Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соответствуют теме работы.
3. Есть планирование проектно-исследовательской деятельности, корректировка ее в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта – распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен корректно.
4. Используется и осмысляется междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников.
5. Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов с точки зрения значимости для собственной проектно-исследовательской работы, выявлена его новизна, библиография и интернет ресурсы грамотно оформлены.
6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
7. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях.

Критерии презентации проектно-исследовательской работы (устного выступления)

1. Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержание работы, достаточная осведомленность в терминологической системе

проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.

2. Умение чётко отвечать на вопросы после презентации работы.

3. Умение создать качественную презентацию. Демонстрация умения использовать IT-технологии и создавать слайд презентацию на соответствующем его возрасту уровне.

4. Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне.

5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видео-ролик, мультфильм и т.д.).

6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение четко обозначить пути создания сетевого продукта.

7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.