

Муниципальное бюджетное общеобразовательное учреждение
«Школа № 43» г.о.Самара

ПРОВЕРЕНО

Заместитель директора по УВР
Романова Л.А.
«07» сентября 2022г.

УТВЕРЖДАЮ

Директор МБОУ Школа № 43
г.о.Самара
Мистосвет Пистолетова В.К.
Приказ № 338 от «08
» сентября 2022г.

РАБОЧАЯ ПРОГРАММА

внеурочной деятельности

«Цифровая гигиена»

9 класс

Учитель: Кирьяков Г.Е.

Классы: 9

Предмет: информатика

Уровень: базовый

Количество часов по учебному плану:

34 часа за год, в неделю – 1 час.

Рассмотрена на заседании МО учителей предметов политехнического цикла
Протокол № 1 от «08» августа 2022 г.

Председатель МО Кузнецова Н.А.
(Кузнецова Н.А.)
г. Самара, 2022

Муниципальное бюджетное общеобразовательное учреждение
«Школа № 43» г.о.Самара

ПРОВЕРЕНО

Заместитель директора по УВР
_____ Романова Л.А.
« » _____ 2022г.

УТВЕРЖДАЮ

Директор МБОУ Школа № 43
г.о.Самара
_____ Пистолетова В.К.
Приказ № ____ от «
» _____ 2022г.

РАБОЧАЯ ПРОГРАММА

внеурочной деятельности

«Цифровая гигиена»

9 класс

Учитель: Кирьяков Г.Е.

Классы: 9

Предмет: информатика

Уровень: базовый

Количество часов по учебному плану:

34 часа за год, в неделю – 1 час.

Рассмотрена на заседании МО учителей предметов политехнического цикла

Протокол № 1 от « » августа 2022 г.

Председатель МО _____ (Кузнецова Н.А.)

г. Самара, 2022

Рабочая программа внеурочной деятельности «Цифровая гигиена» для 9 классов составлена в соответствии с нормативно-правовыми документами:

- Федеральный закон Российской Федерации от 29.12.2012 г. № 273-ФЗ "Об образовании в Российской Федерации" (с изменениями и дополнениями);
- Приказ Министерства образования и науки Российской Федерации от 17 декабря 2010 г № 1897 «Об утверждении Федерального государственного образовательного стандарта основного общего образования» (с изменениями и дополнениями);
- Основная образовательная программа основного общего образования МБУ «Школа № 71», составленная на основе примерной основной образовательной программы основного общего образования, одобренной Федеральным учебно-методическим объединением по общему образованию (Протокол заседания от 8 апреля 2015 года № 1/15 (в редакции протокола от 04.02.2020 № 1/20);

I. Результаты освоения курса внеурочной деятельности

Программа курса способствует овладению детьми универсальными учебными действиями (познавательными, коммуникативными, регулятивными, личностными) и предметными умениями.

Личностные результаты освоения программы курса

- 1) 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;
- 2) 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;
- 3) освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- 4) формирование понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные результаты освоения программы курса

Регулятивные умения:

- 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 учебные умения:

- 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 учебные умения:

- 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.

В результате освоения программы курса «Цифровая гигиена» формируются следующие **предметные умения**, соответствующие требованиям федерального государственного образовательного стандарта начального общего образования:

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.

II. Содержание курса внеурочной деятельности

Программа курса «Цифровая гигиена» адресована учащимся 7 классов. Она 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 организации занятий могут быть различными: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), 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.).

Главные цели и задачи:

- 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);
- формирование общекультурных навыков 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.

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 курса 9 класс (34 часа)

Раздел 1. «Безопасность общения»

Общение в социальных сетях и мессенджерах (1ч)

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

С кем безопасно общаться в интернете (1ч)

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Пароли для аккаунтов социальных сетей (1ч)

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Безопасный вход в аккаунты (1ч)

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

Настройки конфиденциальности в социальных сетях (1ч)

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

Публикация информации в социальных сетях (1ч)

Персональные данные. Публикация личной информации.

Кибербуллинг (1ч)

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

Публичные аккаунты (1ч)

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Фишинг (2ч)

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 (3ч)

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

Раздел 2. «Безопасность устройств»

Что такое вредоносный код (1ч)

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Распространение вредоносного кода (1ч)

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.

Методы защиты от вредоносных программ (2ч)

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

Распространение вредоносного кода для мобильных устройств (1ч)

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов (3ч)

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

Раздел 3 «Безопасность информации»

Социальная инженерия: распознать и избежать (1ч)

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Ложная информация в Интернете (1ч)

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Безопасность при использовании платежных карт в Интернете (1ч)

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Беспроводная технология связи (1ч)

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

Резервное копирование данных (1ч)

Безопасность личной информации. Создание резервных копий на различных устройствах.

Основы государственной политики в области формирования культуры информационной безопасности (2ч)

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 (3ч)

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

Повторение. Волонтерская практика (3ч)

III. Тематическое планирование

В основе выбора методов и приемов, форм работы лежит ориентация на целевые приоритеты, обозначенные в Рабочей программе воспитания Школы:

-установление доверительных отношений между педагогическим работником и его обучающимися, способствующих позитивному восприятию обучающимися требований и просьб педагогического работника, привлечению их внимания к обсуждаемой на уроке информации, активизации их познавательной деятельности;

-побуждение обучающихся соблюдать на уроке общепринятые нормы поведения, правила общения со старшими (педагогическими работниками) и сверстниками (обучающимися), принципы учебной дисциплины и самоорганизации;

-привлечение внимания обучающихся к ценностному аспекту изучаемых на уроках явлений, организация их работы с получаемой на уроке социально значимой информацией – инициирование ее обсуждения, высказывания обучающимися своего мнения по ее поводу, выработки своего к ней отношения;

- использование воспитательных возможностей содержания учебного предмета через демонстрацию обучающимся примеров ответственного, гражданского поведения, проявления человеколюбия и добросердечности, через подбор соответствующих текстов для чтения, задач для решения, проблемных ситуаций для обсуждения в классе.

9 класс

(из расчёта 1 час в неделю - 34 часа)

№ п/п	Наименование темы	Кол-во часов
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	1
5.	Настройки конфиденциальности в социальных сетях	1
6.	Публикация информации в социальных сетях	1
7.	Кибербуллинг	1
8.	Публичные аккаунты	1
9.	Фишинг	1
10.	Фишинг	1
11.	Выполнение и защита индивидуальных и групповых проектов	1
12.	Выполнение и защита индивидуальных и групповых проектов	1
13.	Выполнение и защита индивидуальных и групповых проектов	1
14.	Что такое вредоносный код	1
15.	Распространение вредоносного кода	1
16.	Методы защиты от вредоносных программ	1
17.	Методы защиты от вредоносных программ	1
18.	Распространение вредоносного кода для мобильных устройств	1
19.	Выполнение и защита индивидуальных и групповых проектов	1
20.	Выполнение и защита индивидуальных и групповых проектов	1
21.	Выполнение и защита индивидуальных и групповых проектов	1

22.	Социальная инженерия: распознать и избежать	1
23.	Ложная информация в Интернете	1
24.	Безопасность при использовании платежных карт в Интернете	1
25.	Беспроводная технология связи	1
26.	Резервное копирование данных	1
27.	Основы государственной политики в области формирования культуры информационной безопасности	1
28.	Основы государственной политики в области формирования культуры информационной безопасности	1
29.	Выполнение и защита индивидуальных и групповых проектов	1
30.	Выполнение и защита индивидуальных и групповых проектов	1
31.	Выполнение и защита индивидуальных и групповых проектов	1
32.	Повторение. Волонтерская практика	1
33.	Повторение. Волонтерская практика	1
34.	Повторение. Волонтерская практика	1