Муниципальное бюджетное общеобразовательное учреждение
городского округа Тольятти «Школа №20»

СОГЛАСОВАНА	**ПРИНЯТА**	**УТВЕРЖДЕНА**
на заседании методического объединения классных руководителей Протокол № 1 от 29.08 2019 г. Руководитель МО _____ / Чалкова С.И.	на заседании Педагогического Совета Протокол № 1 от 30.08 2019 г.	Директор МБУ «Школа № 20» _____ О.Н. Солодовникова № 305-од от 30.08 2019 г.

РАБОЧАЯ ПРОГРАММА

По курсу внеурочной деятельности «Цифровая гигиена»

8 класс

Составитель: Афанасьева Е.Н.

Направление: социальное

Тольятти,
2019

Рабочая программа составлена на основе следующих нормативных документах:

1. Федеральный Закон «Об образовании в Российской Федерации» № 273-ФЗ от 29 декабря 2012 г. (редакция от 07.05.2013),
2. Федеральный Государственный образовательный стандарт основного общего образования (приказа Минобрнауки России от 17.12.2010 No1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (в действующей редакции);
3. Основной образовательной программы начального общего образования МБУ «Школа № 20»;
4. Программа учебного курса «Цифровая гигиена»/ Министерство образования и науки Самарской области, 2019.

В программе курса «Цифровая гигиена» значительные ресурсы направлены на то, чтобы просто дать элементарные знания безопасной жизни в цифровом мире. Проблема кибер безопасности не в технологиях. Применение действительно серьёзных технологий крайне дорого, кибер атаки случаются ежесекундно, но это решаемый вопрос. Главная угроза — это безграмотность людей.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

Метапредметные.

• 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.

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 информационнотелекоммуникационной среде.

Предметные:

• 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 Интернетресурсы и другие базы данных.

СОДЕРЖАНИЕ КУРСА

Содержание программы учебного курса (Модуль 1) 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 (Модуля 1) 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 заданий по основным темам курса.

Содержание учебного курса (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.

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 5 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 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.5

Повторение. Волонтерская практика. 3 часа.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№	Раздел	Количество часов	Виды деятельности
1.	Тема 1. «Безопасность общения»	13	Беседы, проект
2.	Тема 2. «Безопасность устройств»	8	Дискуссии, проект
3.	Тема 3 «Безопасность информации»	13	Творческие задания
	Итого	34	