

государственное бюджетное общеобразовательное учреждение Самарской области средняя
общеобразовательная школа №3 городского округа Чапаевск Самарской области

Проверено
Куратор по ВР
Карасева Н.Н. _____
(подпись)

Педагогический совет №16
«29» августа 2022 г.

Утверждаю
Директор ГБОУ СОШ №3 г.о. Чапаевск
Кочеткова Е.А. _____
(подпись)

Приказ №58-од
от «29» августа 2022г.

РАБОЧАЯ ПРОГРАММА

Курса внеурочной деятельности «Цифровая гигиена» Класс 7-9

Количество часов по учебному плану 34 в год 1 в неделю.

Рассмотрена на заседании МО точных наук

Протокол № 1 от « 29 » 08 2022г.

Председатель МО _____ Быкова Л.В.

(подпись)

Пояснительная записка

Рабочая программа учебного курса внеурочной деятельности «Цифровая гигиена» для 7—9 классов разработана в соответствии с требованиями:

- Федерального закона от 29.12.2012 № 273 «Об образовании в Российской Федерации»;
- ООП основного общего образования ГБОУ СОШ №3,
- Программы воспитания ГБОУ СОШ №3;
- СанПиН 1.2.3685-21;
- Плана внеурочной деятельности ОО на 2022-2023 учебный год;
- Стратегии развития воспитания в Российской Федерации на период до 2025 года, утвержденной распоряжением Правительства от 29.05.2015 № 996-р; СП 2.4.3648-20;
- Примерной рабочей программы учебного курса «Цифровая гигиена» для основной школы и линии учебников М.С. Наместникова Информационная безопасность, или На расстоянии одного вируса. 7-9 классы.

Основными **целями** из учения 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).

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, изображений, 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.

Сроки освоения программы: 3 года по 1 ч в неделю в каждом классе.

Всего: 7 класс — 34 ч, 8 класс — 34 ч, 9 класс — 34 ч. Всего на курс 102 ч.

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, 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.

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 2 часа. История возникновения Интернета. Понятия Интернет-угроз. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. Практическая работа: Назначение социальных сетей и мессенджеров. 1 час.

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

Практическая работа: Пароли для аккаунтов и социальных сетей. 1 час.

Тема 4. Безопасный вход в аккаунты. 2 часа. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Практическая работа: Разработка алгоритма, если аккаунт взломан. 1 час.

Тема 5. Настройки конфиденциальности в социальных сетях. 2 часа. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Практическая работа: Вход в аккаунт социальных сетей. 1 час.

Тема 6. Публикация информации в социальных сетях. 2 часа. Персональные данные. Публикация личной информации.

Практическая работа: Публикация информации в социальных сетях. 1 час.

Тема 7. Кибербуллинг. 2 часа. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Практическая работа: Способы защиты от кибербуллинга. Правила пользования сайтами социальных сетей. 1 час.

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.

Практическая работа: Как защититься от фишеров в социальных сетях и мессенджерах. 1 час.

Повторение по разделу Безопасность общения. 2 часа.

Проверочная работа по разделу «Безопасность общения» 1 час.

Выполнение индивидуальных и групповых проектов. 4 часа.

Защита индивидуальных и групповых проектов. 3 часа.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 2 часа. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 2 часа. 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.

Практическая работа: Распространение вредоносного кода. 1 час.

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.

Практическая работа: Методы защиты от вредоносных программ. 1 час.

Тема 4. Распространение вредоносного кода для мобильных устройств. 2 часа. Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Практическая работа: Защита от вредоносного кода. 1 часа.

Повторение по разделу Безопасность устройств. 1 часа.

Проверочная работа по разделу «Безопасность устройств» 1 час.

Выполнение индивидуальных и групповых проектов. 2 часа.

Защита индивидуальных и групповых проектов. 2 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.

Практическая работа: Ложная информация в Интернете. 1 час

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.

Практическая работа: Работа в публичных сетях. 2 час

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.

Повторение по разделу Безопасность общения. 2 часа.

Проверочная работа по разделу «Безопасность общения» 1 час.

Выполнение индивидуальных и групповых проектов. 2 часа.

Защита индивидуальных и групповых проектов. 2 часа.

Волонтерская практика. 3 часа.

ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ: просматривание отрывков из познавательных, научно-популярных фильмов, видеоролики, урок-дискуссия, обсуждение, беседы, рассматривание ситуативных иллюстраций, творческая работа, работа в группах.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

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.

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.

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.

Форма промежуточной аттестации.

Освоение программы по курсу внеурочной деятельности «Цифровая гигиена» для 7-9 классов сопровождается промежуточной аттестацией в форме защиты проектов.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

7 класс

№	Раздел	Количество часов			ЭОР
		теория	практика	проект	
1	«Безопасность общения»	23	7	4	https://vk.com/gigyena https://lbz.ru/books/1105/11204/ https://lbz.ru/metodist/authors/ib/7-9.php
	Подготовка проекта			3	
	Защита проекта			1	
	Итого	34			

8 класс

№	Раздел	Количество часов			ЭОР
		теория	практика	проект	
1.	«Безопасность устройств»	12	3	2	http://school-collection.edu.ru - http://fcior.edu.ru

					https://lbz.ru/metodist/authors/ib/7-9.php
2	«Безопасность информации»	12	3	2	http://intuit.ru https://knife.media/digital-hygiene/ https://lbz.ru/metodist/authors/ib/7-9.php
	Подготовка проекта			1	
	Защита проекта			1	
	Итого	34			

9 класс

№	Раздел	Количество часов			ЭОР
		теория	практика	проект	
1	«Безопасность общения»	10	3		https://lbz.ru/metodist/authors/ib/7-9.php
2	«Безопасность устройств»	5	2		http://school-collection.edu.ru - http://fcior.edu.ru https://lbz.ru/metodist/authors/ib/7-9.php
3	«Безопасность информации»	8	3	3	http://intuit.ru https://knife.media/digital-hygiene/
	Подготовка проекта			2	
	Защита проекта			1	
	Итого	34			