муниципальное бюджетное общеобразовательное учреждение городского округа Тольятти «Школа №79 имени П.М. Калинина»

РАССМОТРЕНО ПРИНЯТО УТВЕРЖДАЮ
на заседании методического на заседании Директор МБУ «Школа №79» объединения учителей физико- Педагогического совета
математического цикла Тарасова М.А. Протокол №1 от 29.08.2025 Протокол №1 от 29.08.2025 Приказ №230-1 ОД от 29.08.2025
Африна Л.П.

РАБОЧАЯ ПРОГРАММА
курса внеурочной деятельности
«Цифровая гигиена»

Класс: 7 класс

Рабочая программа курса внеурочной деятельности «Цифровая гигиена» 9 класс составлена на основе примерной рабочей программы учебного курса
«Цифровая гигиена» рекомендованного координационным советом учебно- методических объединений в системе общего образования Самарской области.

1. Планируемые результаты освоения курса внеурочной деятельности

«Цифровая гигиена»

Предметные:

Выпускник научится:

1. Анализировать доменные имена компьютеров и адреса документов в интернете;
2. Безопасно использовать средства коммуникации;
3. Безопасно вести и применять способы самозащиты при попытке мошенничества;
4. Безопасно использовать ресурсы интернета.

Выпускник овладеет:

1. Приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет сервисов и т.п.

Выпускник получит возможность овладеть:

1. Основами соблюдения норм информационной этики и права;
2. Основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
3. 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:

1. Идентифицировать собственные проблемы и определять главную проблему;
2. Выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
3. Ставить цель деятельности на основе определенной проблемы и существующих возможностей;
4. Выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
5. Составлять план решения проблемы (выполнения проекта, проведения исследования);
6. Описывать свой опыт, оформляя его для передачи другим людям в

виде технологии решения практических задач определенного класса;

7. Оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
8. Находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
9. Работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
10. принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

1. Выделять явление из общего ряда других явлений;
2. Определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
3. Строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
4. Излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
5. Самостоятельно указывать на информацию, нуждающуюся в

проверке, предлагать и применять способ проверки достоверности информации;

6. Критически оценивать содержание и форму текста;
7. Определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

1. Строить позитивные отношения в процессе учебной и познавательной деятельности;
2. Критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
3. Договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
4. Делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его;
5. Целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
6. Выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных язы- ков в соответствии с условиями коммуникации;
7. Использовать компьютерные технологии (включая выбор адекватных

задаче инструментальных программно-аппаратных средств и решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;

8. Использовать информацию с учетом этических и правовых норм;
9. Создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Личностные.

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. Освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
4. Сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

2. Содержание учебного курса «Цифровая гигиена» 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 приватностии 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 часа.
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 экспериментирования и самопрезентации, ролей. освоения различных социальных новости. Поддельные страницы. Фейковые

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 раз- личных 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 информацион- ной безопасности.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.5 Повторение. Волонтерская практика. 3 часа.
Форма организации деятельности: проект.

Основные виды деятельности: проектная и исследовательская деятельность; стенгазета; проблемно-ценностное общение; макет; отчёт по результатам исследования, волонтёрская практика.
Форма промежуточной аттестации: выставка работ по различным проектным задачам.

3. Тематическое планирование курса внеурочной деятельности «Цифровая гигиена»

№ п/п	Тема	Количество	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
			Тема 1. «Безопасность общения»	
1	Общение в социальных сетях и мессенджерах	1	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2	С кем безопасно общаться в интернете	1	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
3	Пароли для аккаунтов социальных сетей	1	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Изучает основные понятия регистрационной информации и шифрования. Умеетих применить.
4	Безопасный вход в аккаунты	1	Виды аутентификации. Настройки безопасности	Объясняет причины использования безопасного

		аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.		входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.
5	Настройки конфиденциальности в социальных сетях	1	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.
6	Публикация информации в социальных сетях	1	Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
7	Кибербуллинг	1	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	1	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности. Анализ проблемных ситуаций. Разработка кейсов с примерами
9	Фишинг	2	Фишинг как мошеннический прием. Популярные варианты	

			распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу. Самостоятельная работа.
10	Выполнение и защита индивидуальных и групповых проектов	3		
			Тема 2. «Безопасность устройств»	
1	Что такое вредоносный код	1	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче. Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
2	Распространение вредоносного кода	1	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.	
3	Методы защитыот вредоносных программ	2	Способы защиты устройств от вредоносного кода. Антивирусные программы и их	Изучает виды антивирусных программ и правила их установки.

		характеристики. Правила защиты от вредоносных кодов.	
4	Распространение вредоносного кода для мобильных устройств	1 Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.
5. Выполнение и защита индивидуальных и групповых проектов		3	Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.
1	Социальная инженерия: распознать и избежать	Тема 3 «Безопасность информации» 1 Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
2	Ложная информация в Интернете	1 Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.

3	Безопасность при использовании платежных карт в Интернете	1	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете. Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
4	Беспроводная технология связи	1	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	
5	Резервное копирование данных	1	Безопасность личной информации. Создание резервных копий на устройствах.	Создает резервные копии. Создание различных
6	Основы государственной политики в области формирования культуры информационной безопасности	2	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области	Умеет привести выдержки из законодательства РФ: обеспечивающего конституционное право на поиск, получение и распространение информации;

	формирования культуры информационной безопасности.		
7	Выполнение и защита индивидуальных и групповых проектов	3	отражающего аспекты киберпространства. правовые защиты
8	Повторение, волонтерская практика, резерв	3	
Итого		34	