

**Календарно-тематическое планирование ВД «Цифровая гигиена»
9 г класс**

| № п/п | Тема | Количество часов | 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. Умеет их применить. |
| 4 | Безопасный вход в аккаунты | 1 | Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта. | Объясняет причины использования безопасного 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 | 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. | Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности. |
| 9 -10 | Фишинг | 2 | Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах. | Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу |
| 11,12,13 | Выполнение и защита индивидуальных и групповых проектов | 3 | | Самостоятельная работа. |
| Тема 2. «Безопасность устройств» | | | | |
| 14 | 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. |
| 15 | 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. | Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов. |
| 16-17 | Методы защиты от вредоносных программ | 2 | Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. | Изучает виды антивирусных программ и правила их установки. |
| 18 | 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. |
| 19,20,21 | 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. |
| Тема 3 «Безопасность информации» | | | | |

| | | | | |
|-------|---|---|---|---|
| 22 | Социальная инженерия: распознать и избежать | 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. |
| 23 | 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. |
| 24 | 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. |
| 25 | Беспроводная технология связи | 1 | Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях. | Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов. |
| 26 | Резервное копирование данных | 1 | Безопасность личной информации. Создание резервных копий на различных устройствах. | Создает резервные копии. |
| 27-28 | Основы государственной политики в области формирования культуры | 2 | Доктрина национальной информационной безопасности. Обеспечение свободы и равенства | Умеет привести выдержки из законодательства РФ: |

| | | | | |
|----------|---|---|--|---|
| | информационной безопасности | | доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности. | - обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего аспекты киберпространства. |
| 29,30,31 | Выполнение и защита индивидуальных и групповых проектов | 3 | | |
| 32,33,34 | Повторение, волонтерская практика, резерв | 3 | | |