Государственное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа
имени полного кавалера ордена Славы А.И. Дырина п.г.т. Балашейка
муниципального района Сызранский Самарской области

Рассмотрена на заседании методического объединения учителей физико-математического цикла Руководитель_____ Емельянова Л.В. Протокол № 1 от 30.08.2024 г.	Проверена Заместитель директора по УВР _____ Короткова О.В. 30.08.2024 г.	Утверждена приказом № 480 - ОД от 30.08.2024 Директор: _____Сибутина И.А.

Сибутина Ирина Александровна
C=RU, O=ГБОУ СОШ п.г.т. Балашейка, CN=Сибутина Ирина Александровна, E=balash_sch@samara.edu.ru
00f31ddeb037d06795
2024-08-31 18:46:03

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности
«Цифровая гигиена»
на уровне основного общего образования
(7 класс)

2024 год

Рабочая программа курса внеурочной деятельности общеинтеллектуального направления «Цифровая гигиена» на уровне основного общего образования составлена на

основе Федерального государственного образовательного стандарта основного общего образования (утвержден приказом министерства образования и науки Российской Федерации № 1897 от 17.12.2010 в редакции приказов Минобрнауки № 1644 от 29.12.2014 и № 1577 от 31.12.2015), в соответствии с основной образовательной программой основного общего образования и плана внеурочной деятельности ГБОУ СОШ п.г.т. Балашейка.

Рабочая программа внеурочной деятельности «Цифровая гигиена» составлена на основе Примерной рабочей программы учебного курса «Цифровая гигиена» основного общего образования, рекомендованной Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019). Самара.

В учебном плане ГБОУ СОШ п.г.т. Балашейка на изучение курса внеурочной деятельности «Цифровая гигиена» отводится в 7 классе – 34 часа в год (1 час в неделю). Итого на уровне основного общего образования – 34 часа.

Результаты освоения курса внеурочной деятельности «Цифровая гигиена»

Предметные результаты

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.

Метапредметные результаты

Регулятивные универсальные учебные действия:

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 технологиирешения 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:

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 частныхявлений к общим закономерностям;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагатьи применять способ проверки достоверности информации;
- критически оценивать содержание и форму текста;
- определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия:

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 послезавершения 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.

Личностные результаты

- 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.

Содержание курса внеурочной деятельности «Цифровая гигиена» с указанием форм организации и видов деятельности

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах.

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

Вид деятельности: аудиторная.

Форма деятельности: беседа, работа в группах, рефлексия.

Тема 2. С кем безопасно общаться в интернете.

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

Вид деятельности: аудиторная.

Форма деятельности: беседа, работа в группах, рефлексия.

Тема 3. Пароли для аккаунтов социальных сетей.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использованиефункции браузера по запоминанию паролей.

Вид деятельности: аудиторная.

Форма деятельности: беседа, практическая работа, рефлексия.

Тема 4. Безопасный вход в аккаунты.

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

Вид деятельности: аудиторная.

Форма деятельности: круглый стол, работа в группах, рефлексия.

Тема 5. Настройки конфиденциальности в социальных сетях.

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

Вид деятельности: аудиторная и внеаудиторная.

Форма деятельности: беседа, практическая работа, рефлексия.

Тема 6. Публикация информации в социальных сетях.

Персональные данные. Публикация личной информации.

Вид деятельности: аудиторная.

Форма деятельности: беседа, рефлексия.

Тема 7. Кибербуллинг.

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

Вид деятельности: аудиторная.

Форма деятельности: беседа, работа в группах, творческая работа, рефлексия.

Тема 8. Публичные аккаунты.

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

Вид деятельности: аудиторная.

Форма деятельности: беседа, работа в группах, исследовательская работа, рефлексия.

Тема 9. Фишинг.

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.

Вид деятельности: аудиторная.

Форма деятельности: беседа, работа в парах, рефлексия.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Вид деятельности: аудиторная.

Форма деятельности: дискуссия, рефлексия.

Тема 2. Распространение вредоносного кода.

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.

Вид деятельности: аудиторная.

Форма деятельности: беседа, индивидуальная работа, рефлексия.

Тема 3. Методы защиты от вредоносных программ.

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

Вид деятельности: аудиторная.

Форма деятельности: беседа, работа в группах, рефлексия.

Тема 4. Распространение вредоносного кода для мобильных устройств.

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства. Выполнение и защита индивидуальных и групповых проектов.

Вид деятельности: аудиторная и внеаудиторная.

Форма деятельности: беседа, защита проекта, рефлексия.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Вид деятельности: аудиторная.

Форма деятельности: лекция, рефлексия.

Тема 2. Ложная информация в Интернете.

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

Вид деятельности: аудиторная.

Форма деятельности: беседа, поиск информации, рефлексия.

Тема 3. Безопасность при использовании платежных карт в Интернете.

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

Вид деятельности: аудиторная.

Форма деятельности: диспут, рефлексия.

Тема 4. Беспроводная технология связи.

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

Вид деятельности: аудиторная.

Форма деятельности: беседа, работа в микро-группах, рефлексия.

Тема 5. Резервное копирование данных.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Вид деятельности: аудиторная.

Форма деятельности: беседа, работа в микро-группах, рефлексия.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.

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. Повторение. Волонтерская практика.

Вид деятельности: аудиторная и внеаудиторная.

Форма деятельности: беседа, защита проектов, работа в микро-группах, рефлексия.

Тематическое планирование

№ п\п	Наименование темы (раздела)	Количество часов на изучение
Раздел 1. «Безопасность общения» (13 часов)		
1	Тема 1. Общение в социальных сетях и мессенджерах.	1
2	Тема 2. С кем безопасно общаться в интернете.	1
3	Тема 3. Пароли для аккаунтов социальных сетей.	1
4	Тема 4. Безопасный вход в аккаунты.	1
5	Тема 5. Настройки конфиденциальности в социальных сетях.	1
6	Тема 6. Публикация информации в социальных сетях.	2
7	Тема 7. Кибербуллинг.	2
8	Тема 8. Публичные аккаунты.	1
9	Тема 9. Фишинг.	3
Раздел 2. «Безопасность устройств» (8 часов)		
10	Тема 1. Что такое вредоносный код.	1
11	Тема 2. Распространение вредоносного кода.	2
12	Тема 3. Методы защиты от вредоносных программ.	3
13	Тема 4. Распространение вредоносного кода для мобильных устройств.	2
Раздел 3 «Безопасность информации» (13 часов)		
14	Тема 1. Социальная инженерия: распознать и избежать.	2
15	Тема 2. Ложная информация в Интернете.	2

16	Тема 3. Безопасность при использовании платежных карт в Интернете.	2
17	Тема 4. Беспроводная технология связи.	2
18	Тема 5. Резервное копирование данных.	2
19	Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.	3
Итого: 34 часа		