Государственное бюджетное общеобразовательное учреждение средняя общеобразовательная школа имени Героя Советского Союза В.Г. Колесникова с.Новодевичье муниципального района Шигонский Самарской области

Программа рассмотрена на заседании МО классных руководителей Протокол №1 от 27.08.2025г. Руководитель МО_____ /Седлина Л.М./	Проверена. Заместитель директора по УВР _____ /Седлина Л.М./ 28.08.2025г.	Утверждена. Директор ГБОУ СОШ с.Новодевичье _____ /Птицына Е.А./ Приказ №_____от 28.08.2025г.

Программа внеурочной деятельности по общеинтеллектуальному направлению «Цифровая гигиена»

Срок реализации: 1 год

ЭП

C=RU, O=ГБОУ СОШ с.Новодевичье,
CN=Птицына Елена Александровна,
E=zu_n_devich_sch@63edu.ru
00d9a0f8100a620971
2025.08.28 16:04:06+04'00'

с. Новодевичье

Аннотация
курса внеурочной деятельности
«ЦИФРОВАЯ ГИГИЕНА»
(полное наименование программы)

Нормативная база программы:	- Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 02.03.2016) "Об образовании в Российской Федерации" -Письмо министерства образования и науки Самарской области "О внеурочной деятельности" от 17.02.2016 №МО-16-09-01/173-ту.
Общее количество часов:	34 ч
Уровень реализации:	Основное общее образование
Срок реализации:	1 год
Возраст учащихся:	13-15лет
Автор(ы) рабочей программы:	Учитель Птицына Е. А.

1.Планируемые результаты освоения курса внеурочной деятельности.

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.

Метапредметными результатами освоения учащимися программы являются:

Регулятивные универсальные учебные действия:

-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:

– 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:

– 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.

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.

2.Содержание курса внеурочной деятельности с указанием форм организации и видов учебной деятельности

№	Тема	Основное содержание темы	Характеристика основных видов деятельности
	Тема 1. «Безопасность общения»		
1	Общение в социальных сетях и мессенджерах	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	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	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	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	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные нас тройки приватности в личном профиле.

6	Публикацияинформации в социальных сетях	Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
7	Кибербуллинг	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	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.
9	Фишинг	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.
10	Выполнение и защита индивидуальных и групповых проектов		Самостоятельная работа.
Тема 2. «Безопасность устройств»			
1	Что такое вредоносный код	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
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	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.

		устройствах.	
3	Методы защиты от вредоносных программ	Способы защиты устройств от вредоносного Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Изучает виды антивирусных программ установки.
4	Распространение вредоносного кода для мобильных устройств	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		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»		
1	Социальная инженерия: распознать и избежать	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	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.
3	Безопасность при использовании платежных карт в Интернете	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.
4	Беспроводная технология связи	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.
5	Резервное копирование данных	Безопасность личной информации. Создание резервных копий на различных устройствах.	Создает резервные копии.
6	Основы государственной политики в области формирования культуры информационной безопасности	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации изнаниям. Основные направления государственной Политики в области формирования культуры информационной безопасности.	Умеет привести выдержки из законодательства РФ: -обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства.
7	Выполнение и защита индивидуальных		
8	Повторение, волонтерская практика, резерв		

3.Тематическое планирование.

№ п/п	Раздел. Темы раздела	Всего часов	Теоретич. занятия	Практич. занятия	Форма организации
I	**«Безопасность общения»**	10			
1	Общение в социальных сетях и мессенджерах	2	1	1	Лекция, деловая игра
2	С кем безопасно общаться в интернете	2	1	1	лекция деловая игра
3	Пароли для аккаунтов социальных сетей	12	1	1	Лекция, деловая игра
4	Безопасный вход в аккаунты	2	1	1	Лекция, деловая игра
5	Настройки конфиденциальности в социальных сетях	2	1	1	Лекция, деловая игра
6	Публикация информации в социальных сетях	2	1	1	Лекция, деловая игра
8	Кибербуллинг	2	2	2	лекция
9	Публичные аккаунты	2	1	1	Лекция, деловая игра
10	Фишинг	4	2	2	Лекция, деловая игра
11	Выполнение и защита индивидуальных и групповых проектов	6	3	3	деловая игра

II	**«Безопасность устройств»**				
	Что такое вредоносный код	2	1	1	лекция
	Распространение вредоносного кода	2	1	1	Лекция, деловая игра
	Методы защиты от вредоносных программ	4	2	2	лекция деловая игра
	Распространение вредоносного кода для мобильных устройств	2	1	1	Лекция, деловая игра
	Выполнение и защита индивидуальных и групповых проектов	6	3	3	деловая игра
III	**«Безопасность информации»**				
	Социальная инженерия: распознать и избежать	2	1	1	лекция
	Ложная информация в Интернете	2	1	1	лекция деловая игра
	Безопасность при использовании платежных карт в Интернете	2	1	1	лекция деловая игра
	Беспроводная технология связи	2	1	**1**	Лекция
	Резервное копирование данных	2	1	1	лекция деловая игра
	Основы государственной политики в области формирования культуры информационной безопасности	4	2	2	лекция деловая игра
	Выполнение и защита индивидуальных и групповых проектов	6	3	3	деловая игра
	Повторение, волонтерская практика	6	3	3	практика