МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования и науки Самарской области
Северное управление министерства образования Самарской области

ГБОУ СОШ с. Шламка

РАССМОТРЕНО	ПРОВЕРЕНО	УТВЕРЖДЕНО
Руководитель МО протокол №1 от 20.08.2025 г.	Ответственный по УР	Директор ГБОУ СОШ с. Шламка
_____	_____	_____
Стручкова Ю.В	Хамидуллина Н.Н.. 20.08.2025 г.	Мавлютов М.Ф Приказ №34-од от 21.08.2025 г

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
(ID 6990652)

«ЦИФРОВАЯ ГИГИЕНА»
для обучающихся 7-9 классов

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ОБЩАЯ ХАРАКТЕРИСТИКА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
Рабочая программа разработана в соответствии с нормативно-правовыми документами:
1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 N273-ФЗ (ред. от 25.05.2019)
2. Федеральный государственный образовательный стандарт основного общего образования, утверждённый приказом министерства образования и науки РФ 17декабря 2010 года №1897 (редакция 31.12.2015 г.)
3. СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» (утверждены постановлением Главного государственного санитарного врача РФ от 29 декабря 2010г.№189, зарегистрированным в Минюсте России 3 марта 2011г., регистрационный номер19993 с изменениями и дополнениями от 29 июня 2011г., 25 декабря 2013г., 24 ноября2015г.)
4. Основная образовательная программа основного общего образования ГБОУСОШ с. Шламка.

Образовательный процесс осуществляется с использованием учебников, учебных пособий, входящих в действующий федеральный перечень. Перечень учебников ежегодно утверждается приказом директора школы. Программа курса «Цифровая гигиена» адресована учащимся 7-9 классов, а также родителям обучающихся всех возрастов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика»,«Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам.

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
Цифровая гигиена

Основными целями изучения 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, изобразительных, 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

сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт. Данный курс предполагает организацию работы в соответствии с содержанием 2-х модулей, предназначенных для обучающихся 7-9 классов и родителей обучающихся любого возраста соответственно.

Модуль 1. «Информационная безопасность» Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7-9 классов. Рекомендуется для реализации в рамках внеурочной деятельности обучающихся. В преподавании модуля «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат. Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.). Место учебного курса (Модуль 1) в учебном плане Программа учебного курса (Модуль 1) рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. На изучение модуля 1 «Информационная безопасность» отводится по 1 часу в неделю в 7, 8 или 9 классах. Учебные занятия по программе могут быть реализованы в различных вариантах:1. в течение одного учебного года в 7, 8 или 9 классах.

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

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.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

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

- 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

- 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 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.

Требования к содержанию итоговых проектно-исследовательских

2. Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы.
Гипотеза сформулирована корректно и соответствуют теме работы.
3.Есть планирование проектно-исследовательской деятельности, корректировка ее в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта – распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен корректно.
4. Используется и осмысляется междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников.
5. Определѐн объѐм собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов сточки зрения значимости для собственной проектно-исследовательской работы, выявлена его новизна, библиография и интернет ресурсы грамотно оформлены.
6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
7. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях.

Критерии презентации проектно-исследовательской работы (устного выступления)
1. Демонстрация коммуникативных навыков при защите работы. Владение

5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видеоролик, мультфильм и т.д.).
6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление входе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение четко обозначить пути создания сетевого продукта.
7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Наименование разделов и тем программы	Количество часов	Основное содержание	Основные виды деятельности	Электронные (цифровые) образовательные ресурсы
Раздел 1. ** «Безопасность общения»**					
1.1	Общение в социальных сетях и мессенджерах	1	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент		
1.2	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.		

1.3	Пароли для аккаунтов социальных сетей.	1	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.		
1.4	Безопасный вход в аккаунты	1	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.		
1.5	Настройки конфиденциальности в социальных сетях	1	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах		
1.6	Публикация информации в социальных сетях.	1	Персональные данные. Публикация личной информации.		

1.7	Психологическое насилие, систематическое издевательства, преследование в сети интернет	1	Определение. Возможные причины психологического насилия в сети и как его избежать? Как не стать жертвой психологического насилия в интернете. Как помочь жертве психологического насилия в сети интернет.		
1.8	Публичные аккаунты.	1	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.		
1.9	Фишинг	2	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах		
1.10	Выполнение и защита индивидуальных и групповых проектов	3			
Итого		13			

Раздел 2. «Безопасность устройств»					
2.1	Что такое вредоносный код	1	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.		
2.2	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		
2.3	Методы защиты от вредоносных программ.	2	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.		

2.4	Распространение вредоносного кода для мобильных устройств	1	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.		
2.5	Выполнение и защита индивидуальных и групповых проектов	3			
Итого		8			
Раздел 3. 3 «Безопасность информации»					
3.1	Социальная инженерия: распознать и избежать.	1	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.		
3.2	Ложная информация в Интернете	1	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.		

3.3	Безопасность при использовании платежных карт в Интернете	1	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.		
3.4	Беспроводная технология связи.	1	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.		
3.5	Резервное копирование данных	1	Безопасность личной информации. Создание резервных копий на различных устройствах		
3.6	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 формирования культуры информационной безопасности.		

3.7	Выполнение и защита индивидуальных и групповых проектов	3			
3.8	Повторение. Волонтерская практика.	3			
Итого		13			
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34			

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ

№ п/п	Тема урока	Количество часов			Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
1	Общение в социальных сетях и мессенджерах	1			
2	С кем безопасно общаться в интернете	1			
3	Пароли для аккаунтов социальных сетей.	1			
4	Безопасный вход в аккаунты	1			
5	Настройки конфиденциальности в социальных сетях	1			
6	Публикация информации в социальных сетях.	1			
7	Психологическое насилие, систематическое издевательства, преследование в сети интернет.	1			

8	Публичные аккаунты.	1			
9	Фишинг	1			
10	Проверочная работа по разделу «Безопасность общения»	1			
11	Выполнение индивидуальных и групповых проектов	1			
12	Выполнение индивидуальных и групповых проектов	1			
13	Защита проекта	1			
14	Что такое вредоносный код	1			
15	Распространение вредоносного кода	1			
16	Методы защиты от вредоносных программ.	1			
17	Проверочная работа по разделу «Безопасность устройств»	1			

18	Распространение вредоносного кода для мобильных устройств	1			
19	Выполнение индивидуальных и групповых проектов	1			
20	Выполнение индивидуальных и групповых проектов	1			
21	Защита индивидуальных и групповых проектов	1			
22	Социальная инженерия: распознать и избежать.	1			
23	Ложная информация в Интернете	1			
24	Безопасность при использовании платежных карт в Интернете	1			
25	Беспроводная технология связи.	1			
26	Резервное копирование данных	1			
27	Основы государственной политики в области формирования культуры	1			

	информационной безопасности.				
28	Основы государственной политики в области формирования культуры информационной безопасности.	1			
29	Выполнение индивидуальных и групповых проектов	1			
30	Выполнение индивидуальных и групповых проектов	1			
31	Защита индивидуальных и групповых проектов	1			
32	Повторение.	1			
33	Волонтерская практика.	1			
34	Волонтерская практика.	1			
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34			

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ МАТЕРИАЛЫ ДЛЯ УЧЕНИКА

Информационная безопасность, или на расстоянии одного вируса 7-9 классы. Учебное пособие для общеобразовательных организаций. Москва "Просвещение" 2019 год.

ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ И РЕСУРСЫ СЕТИ

Библиотека ЦОК