МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«Школа № 94 имени полного кавалера ордена Славы Щеканова Н.Ф.»
городского округа Самара

РАССМОТРЕНО
на методическом объединении
учителей математики

Председатель ШМО_____

Протокол № 1

От « 30» августа 2021 г.

СОГЛАСОВАНО
Зам. директора по ВР

_____ Инькова Н.В.

от «30» августа 2021 г.

УТВЕРЖДАЮ
Директор МБОУ школы № 94

_____ Ковалева Т.А.

«30» августа 2021г.

Приказ № 129 от 03.08.2021

Программа

внеурочной деятельности обучающихся

«Информационная безопасность»

Направление: общеинтеллектуальное

Вид деятельности: факультатив

Возрастной состав: 8 классы

Срок реализации: 1 год

Разработчик: Инькова Н.В.

Самара, 2021

Пояснительная записка

Рабочая программа внеурочной деятельности «Цифровая гигиена» составлена в соответствии:

- Федеральным государственным образовательным стандартом основного общего образования;
- Авторской программой «Информационная безопасность, или на расстоянии одного вируса», М.С.Наместникова, 2019
- ООП ООО МБОУ школы № 94 г.о. Самара.

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.

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, изобрази-тельных, 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 поведения школьников, связанного с компьютерными технологиями и Интернетом.

Общая характеристика учебного курса

Курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

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, почто-вые 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.).

Программа рассчитана на 1 год (34 учебных часа) для обучающихся 8 классов. Занятия проходят 1 раз в неделю по 45 мин.

Организация работы в соответствии с содержанием второго модуля, предназначена для родителей обучающихся любого возраста соответственно.

Планируемые результаты освоения курса внеурочной деятельности

Личностные результаты

У ученика буду сформированы	Ученик получит возможность для формирования
• 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; • сформированности понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные результаты

Регулятивные универсальные учебные действия

Ученик научится	Ученик получит возможность научиться
• 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	• 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

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;	получения запланированных характеристик продукта/результата; • принимать решение в учебной ситуации и нести за него ответственность

Познавательные универсальные учебные действия

Ученик научится	Ученик получит возможность научиться
• 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

Ученик научится	Ученик получит возможность научиться
• 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	• использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) 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.

передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;	

Предметные результаты

Ученик научится	Ученик получит возможность научиться
8 класс	
• 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.	• 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.

Формами диагностики и подведения итогов
После каждой темы, в течение учебного года, выполнение и защита проектно-исследовательских работ.
Требования к содержанию итоговых проектно-исследовательских работ содержатся в приложении 1 к данной рабочей программе

Тематическое планирование программы

№	Название раздела	Общее количество часов	Теоретические занятия	Практические занятия
1	Раздел 1. «Безопасность общения»	13	3	10
2	Раздел 2. «Безопасность устройств»	8	4	4
3	Раздел 3 «Безопасность информации»	13	3	10
	Итого	34	10 (29%)	24 (71%)

Содержание курса (Модуль 1)

№ урока	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
Раздел 1. «Безопасность общения»				
1	Общение в социальных сетях и	1	Социальная сеть. История социальных	Выполняет базовые операции при использовании

	мессенджерах		сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	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	Объясняет причины использования безопасного
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.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий,

			Овершеринг.	соблюдая правила информационной безопасности
9, 10	Фишинг	2	Фишинг как мошеннический прием. Популярные варианты	Анализ проблемных ситуаций. Разработка кейсов с примерами
11-13	Выполнение и защита индивидуальных и групповых проектов	3	Самостоятельная работа.	
Раздел 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	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.
19-21	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.	
Раздел 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.
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 информационной безопасности	2	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации;

			государственной политики в области	
29-31	Выполнение и защита индивидуальных и групповых проектов	3		
32-34	Повторение, волонтерская практика, резерв	3		

Модуль 2. «Работа с родителями»

При работе с родителями важнейшей задачей является преодоление «цифрового разрыва» и обучение родителей правильной оценке своих возможностей в помощи детям в Интернете – возможностей, которые достаточно велики.

Родители с бóльшей готовностью включатся в программу развития цифровой гигиены, предлагающую им общение, совместный поиск и развивающие игры и т.п.

Формами проведения мероприятий для родителей могут являться: лектории, выступления на родительских собраниях, микро-обучение на основе технологий онлайн обучения, геймификация, создание чек-листов, совместное обучение, совместные родительско-детские проекты и пр.

Тематическое планирование учебного курса (Модуль 2).

Тема 1. История возникновения Интернета. Понятия Интернет-угроз. Изменения границ допустимого в контексте цифрового образа жизни

Тема 2. Изменения нормативных моделей развития и здоровья детей и подростков.

Тема 3. Цифровая гигиена: зачем это нужно? Понятие периметра безопасности. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка. Баланс ценностей развития и ценностей безопасности.

Тема 4. Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 5. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребёнка для профилактики насилия в Сети?

Тема 6. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?

Тема 7. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.

Тема 8. Пособия и обучающие программы по формированию навыков цифровой гигиены.

Приложение 1

Требования к содержанию итоговых проектно-исследовательских работ

Критерии содержания текста проектно-исследовательской работы

1. Во введении сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована, но при этом четко определена, в необходимости исследования есть аргументы.
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. Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов с точки 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 риторическими умениями, раскрытие автором содержание работы, достаточная осведомленность в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.
2. Умение чётко отвечать на вопросы после презентации работы.
3. Умение создать качественную презентацию. Демонстрация умения использовать IT-технологии и создавать слайд презентацию на соответствующем его возрасту уровне.
4. Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне
5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видео-ролик, 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 в ходе 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.

Список источников:

1. Бабаш А.В. Информационная безопасность: Лабораторный практи-кум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с

2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и за-кон, 2014. – 182 с.

3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.

4. Дети в информационном обществе // http://detionline.com/journal/about

5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2016. – 239 с.

6. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.

7. Защита детей by Kaspersky // https://kids.kaspersky.ru/

8. Кузнецова А.В. Искусственный интеллект и информационная без-опасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Ру-сайнс, 2017. – 64 с.

9. Наместникова М.С. Информационная безопасность, или На расстоя-нии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.

10. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa

11. Стрельцов А.А. Правовое обеспечение информационной безопасно-сти России: теоретические и методологические основы. – Минск, 2005. – 304 с.

12. Сусоров И.А. Перспективные технологии обеспечения кибербез-опасности // Студенческий: электрон. научн. журн. 2019. № 22(66)

13. Цифровая компетентность подростков и родителей. Результаты все-российского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.