государственное бюджетное общеобразовательное учреждение Самарской области
основная общеобразовательная школа с. Максимовка
муниципального района Богатовский Самарской области

РАССМОТРЕНА
на заседании МО учителей предметников
рекомендована к утверждению
Протокол № 1 от 25.08.2022 г.
Руководитель МО_____Карунец Н.В.

C=RU, O=ГБОУ ООШ с. Максимовка, CN=Зайнутдинов Р_С_, E=maksim_sch@samara.edu.ru
00dc35513095f145ab
2022-09-07 15:27:31

УТВЕРЖДЕНА
Директор ГБОУ ООШ с. Максимовка
_____Зайнутдинов Р.С.
Приказ № 65/д от 29.08.2022 г.

РАБОЧАЯ ПРОГРАММА
КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

7 класс
Классы

МОДУЛЬ ДЛЯ РОДИТЕЛЕЙ «ЦИФРОВАЯ ГИГИЕНА»

1 год
срок реализации

СОГЛАСОВАНА
рекомендована к утверждению
25.08.2022 г.
Ио зам директора по УВР
_____Зайнутдинова О.А.

СОСТАВИТЕЛЬ:
Должность: учитель информатики
ФИО: Абросимова Л.В.

Планируемые результаты освоения курса внеурочной деятельности «Информационная безопасность» 7 класс

№	Название раздела (темы)	Планируемые результаты		
		личностные	**предметные**	**метапредметные**
1.	Безопасность общения	• 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	Ученик 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. Ученик получит возможность научиться: • соблюдать нормы информационной этики и права; • самоконтролю, самооценке, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности; • решению использовать коммуникативные задачи в области безопасности жизнедеятельности различных источников информации, включая Интернет- ресурсы и другие базы данных.	Регулятивные: • 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: • выделять явление из общего ряда других явлений; • определять обстоятельства, которые предшествовали
2.	Безопасность устройств			
3.	Безопасность информации			

		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.		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. <u>Коммуникативные:</u> • 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.
	Итого: 34 ч.			

Содержание курса внеурочной деятельности «Информационная безопасность»

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.

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.

Тема 3. Пароли для аккаунтов социальных сетей. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

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.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

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.

Тема 3. Методы защиты от вредоносных программ. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

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.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи.

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

Тема 5. Резервное копирование данных. Безопасность личной информации. Создание резервных копий на различных устройствах.

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.

Тематическое планирование по курсу внеурочной деятельности
«Информационная безопасность»
7 класс

№	Название раздела (темы)	Количество часов	Количество контрольных работ
1	Безопасность общения	13	1
2	Безопасность устройств	8	1
3	Безопасность информации	13	1
	Итого:	**34**	**3**

МОДУЛЬ «ЦИФРОВАЯ ГИГИЕНА» (для родителей)

Пояснительная записка

Программа курса «Цифровая гигиена» адресована родителям обучающихся 1–9 классов с использованием материалов Федерального государственного образовательного стандарта основного общего образования, примерной рабочей программы учебного курса «Цифровая гигиена» для основной школы и линии учебников М.С. Наместникова Информационная безопасность, или На расстоянии одного вируса. 7-9 классы/ М.: Просвещение, 2019.

Основная цель изучения курса «Цифровая гигиена» – формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости). Данный курс предполагает организацию работы с родителями обучающихся 1-9 классов в рамках культурно-просветительской и профилактической деятельности педагогического коллектива школы. 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. Методы реализации курса: репродуктивный – (беседа, вопросы); проблемный; частично-поисковый – (творческие задания); объяснительно-иллюстративный. Составители курса предполагают, что родители с бóльшей готовностью включатся в программу развития цифровой гигиены, предлагающую им общение, совместный поиск, развивающие игры, просмотр отрывков из познавательных, научно-популярных фильмов, видеороликов, обсуждение ситуативных иллюстраций, творческая работа, работа в группах и т.п. Вместе с тем формами проведения мероприятий для родителей также могут являться: лектории, выступления на родительских собраниях, микрообучение на основе технологий он-лайн обучения, геймификация, создание чек-листов, совместное обучение, совместные родительско-детские проекты и пр. Занятия с родителями проводятся один раз в месяц на родительских собраниях.

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.

Список источников:

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

2. 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.

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

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

5. 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.

6. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества /

А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017 – 64 с.

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

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