Министерство образования и науки Самарской области
Юго - Восточное управление министерства образования и науки Самарской области
Государственное бюджетное общеобразовательное учреждение Самарской области
средняя общеобразовательная школа имени Героя Советского Союза Агибалова Михаила Павловича
с. Зуевка муниципального района Нефтегорский Самарской области

РАССМОТРЕНО
На заседании МС
Протокол № 5
от «25» августа 2023г.

СОГЛОСОВАНО
Заместитель директора по УР
_____Гребенкина Е.В.
Приказ №54-од
от «25» августа 2023г.

УТВЕРЖДЕНО
к использованию в образовательной деятельности
Директор ГБОУ СОШ с.Зуевка
_____Воротынцева Л.А.
Приказ №54-од
«25» августа 2023г.

C=RU, OU=Директор, O=ГБОУ СОШ с. Зуевка, CN=Воротынцева Людмила Анатольевна, E="zuev_sch@samara.edu.ru"
446606, Самарская обл, Нефтегорский р-он, с. Зуевка, ул. Школьная, 3
2023-08-29 14:35:19

РАБОЧАЯ ПРОГРАММА
По внеурочной деятельности

Направления: общекультурное.
Предмет (курс) информационная безопасность
Класс 7-8
Количество часов по учебному плану 34 в год 1 в неделю
Составлена в соответствии с примерной рабочей программой курса внеурочной деятельности «информационная безопасность»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа составлена на основе следующих документов:

1. Федеральный Закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный государственный образовательный стандарт основного общего образования (ФГОС ООО).
3. Основная образовательная программа основного общего образования ГБОУ СОШ с. Зуевка.
4. Примерная рабочая программа учебного курса «Цифровая гигиена» (7-9 классы) (рекомендованная координационным советом УМО в системе общего образования СО, 2019 г.)

I. РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА

Личностные, метапредметные и предметные результаты освоения содержания курса

Программа курса обеспечивает достижение выпускниками основной школы комплекса личностных, метапредметных и предметных результатов.

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.

Метапредметные.

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 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.

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 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 жизни в группах и сообществах;
- сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

II.СОДЕРЖАНИЕ КУРСА

Разде 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.

Пособия и обучающие программы по формированию навыков цифровой гигиены.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№	Тема занятия	Всего часов	Теория	Практика	Формы деятельности
Тема 1. «Безопасность общения»					
1	Общение в социальных сетях и мессенджерах	1	1	0	Беседа
2	С кем безопасно общаться в интернете	1	0,5	0,5	Беседа, круглый стол.
3	Пароли для аккаунтов социальных сетей	1	0,5	0,5	Квест, дискуссия.
4	Безопасный вход в аккаунты	1	0	1	Практикум.
5	Настройки конфиденциальности в социальных сетях	1	0	1	Практикум.
6	Публикация информации в социальных сетях	1	1	0	Учебный диалог
7	Кибербуллинг	1	1	0	Беседа
8	Публичные аккаунты	1	0	1	Исследовательская работа, практикум.
9-10	Фишинг	2	1	1	Беседа, обсуждение, практикум.
11-13	Выполнение и защита индивидуальных и групповых проектов	3	1	2	Работа в парах
Тема 2. «Безопасность устройств»					
14	Что такое вредоносный код	1	0,5	0,5	Презентация, беседа.
15	Распространение вредоносного кода	1	1	0	Развивающая игра
16-17	Методы защиты от вредоносных программ	2	1	1	Обсуждение, урок-исследование.
18	Распространение вредоносного кода для мобильных устройств	1	0	1	Практикум
19-21	Выполнение и защита индивидуальных и групповых проектов	3	1	2	Работа в парах
Тема 3 «Безопасность информации»					
22	Социальная инженерия: распознать и избежать	1	0,5	0,5	Презентация.
23	Ложная информация в Интернете	1	0,5	0,5	Мини-проект
24	Безопасность при использовании платежных карт в Интернете	1	1	0	Изучение информации
25	Беспроводная технология связи	1	1	0	Задание исследовательского характера
26-27	Резервное копирование данных	2	1	1	Обсуждение. Исследование.

			1		Проектная работа.
28-29	Основы государственной политики в области формирования культуры информационной безопасности	2	1	1	Учебный диалог
30-31	Пособия и обучающие программы по формированию навыков цифровой гигиены.	2	0,5	1,5	Исследовательская работа, урок-практикум.
32-34	Выполнение и защита индивидуальных и групповых проектов	3	1	2	Работа в парах

Программа учебного курса
«ЦИФРОВАЯ ГИГИЕНА»

(для родителей обучающихся)

Пояснительная записка

Программа курса «Цифровая гигиена» адресована родителям обучающихся всех возрастов и составлена на основе примерной рабочей программы учебного курса «Цифровая гигиена» (основное общее образование), Самара, СИПКРО, 2019 (рекомендована Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019), утверждена на уровне министерства образования и науки Самарской области).

Основными целями изучения курса «Цифровая гигиена» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре родителей 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 информационныхобъектов 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.

Формами проведения мероприятий для родителей являются:

– выступления на классных родительских собраниях,

– мини-семинары на основе технологий онлайн-обучения,

– совместное обучение,

– совместные родительско-детские проекты.

Общая характеристика учебного курса

Курс «Цифровая гигиена» является важной составляющей работы с родителями обучающихся, 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 детей. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.
Данный курс предполагает организацию работы в соответствии с содержанием модуля, предназначенного для родителей обучающихся любого возраста соответственно.

Модуль 2 «Цифровая гигиена» (предназначен для родиетелей обучающихся).

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.
Разработчики курса предполагают, что родители с бóльшей готовностью включатся в программу развития цифровой гигиены, предлагающую им общение, совместный поиск и развивающие игры и т.п.
Вместе с тем, формами проведения мероприятий для родителей также могут являться: лектории, выступления на родительских собраниях, микрообучение на основе технологий онлайн обучения, геймификация, создание чек-листов, совместное обучение, совместные родительско-детские проекты и пр.
Практические материалы для реализации данного модуля представлены в приложении 2 к данной рабочей программе. Разработчики курса «Цифровая гигиена» предлагают использовать вышеуказанное приложение в качестве конструктора при подготовке

к мероприятиям.

№ п/п	Название темы	Сроки проведения
1.	Пособия и обучающие программыпоформированию навыков цифровой гигиены. История возникновения Интернета.Понятия Интернет-угроз. Изменения границ допустимого в контекстецифрового образа жизни.	Октябрь
2.	Изменения нормативных моделей развития и здоровья детей и подростков.	Ноябрь
3.	Цифровая гигиена: зачем этонужно? Понятие периметра безопасности. Обеспечение эмоционально-психологического периметра безопасностив соответствии с возрастными особенностями ребенка. Баланс ценностейразвития и ценностей безопасности.	Декабрь
4.	Угрозы информационной безопасности:атаки, связанные с компьютерной инженерией. Способы выявленияналичия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.	Январь
5.	Угрозы информационной безопасности:атаки, связанные с компьютерной инженерией. Способы выявления наличиявредоносных кодов на устройствах.	Февраль

	Действия при обнаружении вредоносных кодов на устройствах.	
6.	Угрозы информационной безопасности:атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребёнка дляпрофилактики насилия в Сети?	Март
7.	Угрозы информационной безопасности: атаки, связанные с социальной инженерией.Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?	Апрель
8.	Контентные риски. Настройка и Безопасное использование смартфона илипланшета. Семейный доступ.	Май

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://d
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.

14.