государственное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа №14 «Центр образования»
имени кавалера ордена Ленина Н.Ф.Шутова
городского округа Сызрань Самарской области

РАССМОТРЕНО на заседании МО протокол № 1 от «_30_»_08_2020 г.	ПРОВЕРЕНО Заместитель директора по УВР от «_30_»_08__2020 г.	**УТВЕРЖДАЮ** Директор ГБОУ СОШ №14 «Центр образования» г.о.Сызрань
_____ Круглова С.В.	_____ Фомина Т.А.	_____ Марусина Е.Б. Приказ №527-од от 01.09.2020г.

Рабочая программа

внеурочной деятельности

«Цифровая гигиена»

9 класс

Направление: социальное

Рабочая программа ГБОУ СОШ № 14 «Центр образования» г. о. Сызрань внеурочной деятельности «Цифровая гигиена» (социальное направление) на уровне основного общего образования (9 классы) составлена с учётом требований Федерального государственного образовательного стандарта основного общего образования (утвержден приказом Министерства образования и науки Российской Федерации от 17.12.2010 года №1897) к результатам освоения основной образовательной программы основного общего образования, на основе примерной рабочей программы учебного курса «Цифровая гигиена», рекомендовано Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019).

Данная рабочая программа рассчитана на 1 год обучения 34 часа (9 класс – 1час в неделю, 34ч.).

Программа курса «Цифровая гигиена» адресована 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 инфор-мационной культуре учащихся, повышения защищенности детей от информа-ционных 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.

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.

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 за-даче 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.

Содержание курса внеурочной деятельности с указанием форм организации и видов деятельности

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 1 час.

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. 1 час.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паро-лей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чу-жом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.

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

Тема 6. Публикация информации в социальных сетях. 1 час.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибер-буллинга.

Тема 8. Публичные аккаунты. 1 час.

Настройки приватности публичных страниц. Правила ведения публич-ных страниц. Овершеринг.

Тема 9. Фишинг. 2 часа.

Фишинг как мошеннический прием. Популярные варианты распростра-нения 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. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вре-доносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

Способы доставки вредоносных кодов. Исполняемые файлы и расшире-ния вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Спо-собы выявления наличия вредоносных кодов на устройствах. Действия при об-наружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 час.

Способы защиты устройств от вредоносного кода. Антивирусные про-граммы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.

Расширение вредоносных кодов для мобильных устройств. Правила без-опасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

Цифровое пространство как площадка самопрезентации, эксперименти-рования и освоения различных социальных ролей. Фейковые новости. Под-дельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интер-нете. 1 час.

Транзакции и связанные с ними риски. Правила совершения онлайн по-купок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. 1 час.

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

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на раз-личных устройствах.

Тема 6. Основы государственной политики в области формирова-ния культуры информационной безопасности. 2 час.

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. 3 часа.

Тематическое планирование

№ п/п	Наименование темы, раздела.	Всего часов
Тема 1. Безопасность общения		
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	Кибербулинг	1
8	Публичные аккаунты	1
9	Фишинг	2
10	Выполнение и защита индивидуальных групповых проектов	3
Тема 2. Безопасность устройств		
1	Что такое вредоносный код	1
2	Распространение вредоносного кода	1
3	Методы защиты от вредоносных программ	2
4	Распространение вредоносного кода для мобильных устройств	1
5	Выполнение и защита индивидуальных и групповых проектов	3
Тема 3. Безопасность информации		
1	Социальная инженерия: распознать и избежать	1
2	Ложная информация в Интернете	1
3	Безопасность при использовании платежных карт в Интернете	1
4	Беспроводная технология связи	1
5	Резервное копирование данных	1
6	Основы государственной политики в области формирования культуры информационной	2

	безопасности	
7	Выполнение и защита индивидуальных и групповых проектов	3
8	Повторение, волонтерская практика, резерв	3
Итого:		34

Модуль 2.

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

Разработчики курса предполагают, что родители с бóльшей готовностью включатся в программу развития цифровой гигиены, предлагающую им обще-ние, совместный поиск и развивающие игры и т.п.

Вместе с тем, формами проведения мероприятий для родителей также 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.

Практические материалы для реализации данного модуля представлены приложении 2 к данной рабочей программе. Разработчики курса «Цифровая гигиена» предлагают использовать вышеуказанное приложение в качестве конструктора при подготовке к мероприятиям.

Тематическое планирование учебного курса (Модуль 2).

Тема 1. История возникновения Интернета. Понятия Интернет-угроз. Изменения гра~~ниц допустимого в контекс~~те 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 Интер-нет. 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 навы-ков цифровой гигиены.

C=RU, O="ГБОУ СОШ №14 "" Центр образования"" г.о. Сызрань", CN=Марусина Елена Борисовна, E=school14_szr@samara.edu.ru
00 a4 a9 2e ea 81 de ab ad
2021.09.01 12:34:43+03'00'