МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Департамент образования администрации городского округа Самара

муниципальное бюджетное общеобразовательное учреждение

«Школа №62 имени Е.Н. Бородина» г.о. Самара

Рассмотрено на заседании МО учителей естественно-научного цикла	«СОГЛАСОВАНО»	«УТВЕРЖДЕНО»
Протокол №1 от 29.08.2023 г.	Зам. директора по УВР	Директор МБОУ Школы №62
Председатель МО	_____Гилязова И.С.	г.о. Самара
_____Васильева Н.Н.	от 29.08.2023 г.	_____Емелина Т.В.
		Приказ № 60-од от 30.08.2023 г.

Т.В. Емелина

Подписан цифровой подписью: Т.В. Емелина
DN: O=МБОЛУ Школа №. 62 г.о. Самара, CN=Т.В. Емелина, E=school_62@samara.edu.ru
Основание: Я подтверждаю этот документ
Расположение:
Дата: 2023.10.24 19:23:02+04'00'
Foxit PDF Reader Версия: 12.0.1

РАБОЧАЯ ПРОГРАММА

внеурочной деятельности
«ЦИФРОВАЯ ГИГИЕНА»
для 7 класса

Самара 2023

Пояснительная записка

Программа курса «Цифровая гигиена» адресована учащимся 7класса, а также родителям обучающихся всех возрастов и учитывает требования, выдвигаемые федеральным государственным образовательным стан дартом основного общего образования к предметным (образовательные обла- сти «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 Интерне- том.

Общая характеристика учебного курса
Курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условия для сокращения цифро- вого разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Модуль 1. «Информационная безопасность»[1]

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познава- тельных возможностей обучающихся 7-9 классов. Рекомендуется для реализа- ции в рамках внеурочной деятельности обучающихся.
В преподавании модуля «Информационная безопасность» могут исполь- зоваться разнообразные форматы обучения: традиционный урок (коллектив- ная 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 инфор- мационную угрозу, определять степень ее опасности, предвидеть последствияинформационной угрозы и противостоять им и профилактики негативных тен- денций в развитии информационной культуры учащихся, повышения защи- щенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электрон- ных 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.

Характеристика личностных, метапредметных и предметных результа- тов освоения учебного курса (Модуль 1) [2]

Предметные:
Выпускник научится:
анализировать доменные имена компьютеров и адреса документов в интер-нете;
безопасно использовать средства коммуникации,
безопасно вести и применять способы самозащиты при попытке мошенни-чества,
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 форми- ровании 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 про-блему;
выдвигать версии решения проблемы, формулировать гипотезы, предвос-хищать конечный результат;
ставить цель деятельности на основе определенной проблемы и существу- ющих возможностей;
выбирать из предложенных вариантов и самостоятельно искать сред- ства/ресурсы для решения задачи/достижения цели;
составлять план решения проблемы (выполнения проекта, проведения ис-следования);
описывать свой опыт, оформляя его для передачи другим людям в виде тех-нологии решения практических задач определенного класса;

находить достаточные средства для выполнения учебных действий в изме- няющейся

ситуации и/или при отсутствии планируемого результата;
работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных ха- рактеристик 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 связимежду явлениями, из этих обстоятельств выделять определяющие, способ- ные быть причиной данного явления, выявлять причины и следствия явле-ний;
строить рассуждение от общих закономерностей к частным явлениям и отчастных явлений к общим закономерностям;
излагать полученную информацию, интерпретируя ее в контексте решае-мой 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 дея-тельности;
критически относиться к собственному мнению, с достоинством призна- вать ошибочность своего мнения (если оно таково) и корректировать его;
договариваться о правилах и вопросах для обсуждения в соответствии с по-ставленной перед группой задачей;
делать оценочный вывод о достижении цели коммуникации непосред- ственно после завершения коммуникативного контакта и обосновывать его.
целенаправленно искать и использовать информационные ресурсы, необ- ходимые 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 язы- ков 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, со-здание 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 безопас-ности.

Личностные.
осознанное, уважительное и доброжелательное отношение к окружающимлюдям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор вирту- альных собеседников;
готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире про- фессий и профессиональных предпочтений, с учетом устойчивых познава-тельных интересов;
освоенность социальных норм, правил поведения, ролей и форм социаль- ной жизни в группах и сообществах;
сформированность понимания ценности безопасного образа жизни; инте- риоризация правил индивидуального и коллективного безопасного поведе- ния в информационно-телекоммуникационной среде.

Содержание программы учебного курса (Модуль 1).
Содержание программы учебного курса (Модуль 1) соответствует те- мам примерной основной образовательной программы основного общего об- разования (ПООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позво-ляет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопас- ность общения», «Безопасность устройств», «Безопасность информации».
Каждый раздел учебного курса (Модуля 1) завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.
За счет часов, предусмотренных для повторения материала (4 часа), возможно проведение занятий для учащихся 4-6 классов. Эти занятия в каче- стве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные в ходе выполнения учеб- ных заданий по основным темам курса.
Содержание учебного курса (Модуль 1).

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 се-тях. 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 какего 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 отфишеров в социальных сетях и мессенджерах.
Выполнение и защита индивидуальных и групповых проектов[3]. 3 часа.

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. 3 часа.[4] Раздел 3 «Безопасность информации»
Тема 1. Социальная инженерия: распознать и избежать. 1 час.
Приемы социальной инженерии. Правила безопасности при виртуаль- ных 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 Интернете. 1 час.
Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. 1 час.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила 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 формирования 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. 3 часа.[5]
Повторение. Волонтерская практика. 3 часа.

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. В2-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)