Частное общеобразовательное учреждение средняя общеобразовательная школа «Общеобразовательный центр «Школа»

РАССМОТРЕНА	ПРОВЕРЕНА	УТВЕРЖДЕНА
на заседании МО	Зам. директора по УВР	Приказом директора
протокол № 1	Чигирева Е.В.	ЧОУ СОШ
от 29.08. 2022 г.	«30» августа 2022 г.	«Общеобразовательный центр «Школа»
		№130 – од от 31.08.2022

ЧОУ СОШ «ОБЩЕОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР «ШКОЛА»

Сидорова Светлана Ивановна
я подтверждаю этот документ своей удостоверяющей подписью
2022-09-11 22:10:19

Программа курса внеурочной деятельности «Информационная безопасность»

Направление: социальное

Возраст: 13 - 14 лет

Количество часов в неделю: 1 час

Срок реализации: 1 год

Составитель: Первая Н.А.

г. Тольятти

2022 - 2023

Пояснительная записка

Программа курса «Информационная безопасность» адресована учащимся 7-9 классов 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 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, изобразительных, 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.

Программа курса «Информационная безопасность» разработана на основе программы курса «Информационная безопасность, или на расстоянии одного вируса» Наместниковой М.С., Примерной рабочей программы «Цифровая гигиена» (СИПКРО, 2019).

Результаты изучения курса

Освоение курса обеспечивает достижение на уровне основного общего образования следующих образовательных результатов:

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

Патриотическое воспитание:

проявлением интереса к прошлому и настоящему российской науки, к использованию этих достижений в других науках и прикладных сферах.

Трудовое воспитание:

установкой на активное участие в решении практических задач, осознанием важности образования на протяжении всей жизни для успешной профессиональной деятельности и развитием необходимых умений.

Ценности научного познания:

ориентацией в деятельности на современную систему научных представлений об основных закономерностях развития человека, природы и общества, пониманием науки как сферы человеческой деятельности, этапов её развития и значимости для развития цивилизации; овладением языком информатики как средством познания мира; овладением простейшими навыками исследовательской деятельности.

Физическое воспитание, формирование культуры здоровья и эмоционального благополучия:

готовностью применять знания в интересах своего здоровья, ведения здорового образа жизни (чередование времени работы за компьютером со временем отдыха, безопасностью в сети Интернет); сформированностью навыка рефлексии, признанием своего права на ошибку и такого же права другого человека.

Личностные результаты, обеспечивающие адаптацию обучающегося к изменяющимся условиям социальной и природной среды:

готовностью к действиям в условиях неопределённости, повышению уровня своей компетентности через практическую деятельность, в том числе умение учиться у других людей, приобретать в совместной деятельности новые знания, навыки и компетенции из опыта других;

необходимостью в формировании новых знаний, в том числе формулировать идеи, понятия, гипотезы об объектах и явлениях, в том числе ранее не известных, осознавать дефициты собственных знаний и компетентностей, планировать своё развитие;

способностью осознавать стрессовую ситуацию, воспринимать стрессовую ситуацию как вызов, требующий контрмер, корректировать принимаемые решения и действия, формулировать и оценивать риски и последствия, формировать опыт;

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.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Метапредметные результаты освоения программы курса характеризуются овладением универсальными познавательными действиями, универсальными коммуникативными действиями и универсальными регулятивными действиями.

1) Универсальные познавательные действия обеспечивают формирование базовых когнитивных процессов обучающихся (освоение методов познания окружающего мира; применение логических, исследовательских операций, умений работать с информацией).

Базовые логические действия:

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.

Базовые исследовательские действия:

использовать вопросы как исследовательский инструмент познания; формулировать вопросы, фиксирующие противоречие, проблему, самостоятельно устанавливать искомое и данное, формировать гипотезу, аргументировать свою позицию, мнение;

проводить по самостоятельно составленному плану несложный эксперимент;

прогнозировать возможное развитие процесса, а также выдвигать предположения о его развитии в новых условиях.

Работа с информацией:

выявлять недостаточность и избыточность информации, данных, необходимых для решения задачи;

выбирать, анализировать, систематизировать и интерпретировать информацию различных видов и форм представления.

2) Универсальные коммуникативные действия обеспечивают сформированность социальных навыков обучающихся.

Общение:

воспринимать и формулировать суждения в соответствии с условиями и целями общения; ясно, точно, грамотно выражать свою точку зрения, давать пояснения по ходу решения задачи, комментировать полученный результат;

в ходе обсуждения задавать вопросы по существу обсуждаемой темы, проблемы, решаемой задачи, высказывать идеи, нацеленные на поиск решения; сопоставлять свои суждения с суждениями других участников диалога, обнаруживать различие и сходство позиций; в корректной форме формулировать разногласия, свои возражения;

представлять результаты решения задачи, эксперимента, исследования, проекта; самостоятельно выбирать формат выступления с учётом задач презентации и особенностей аудитории.

Сотрудничество:

понимать и использовать преимущества командной и индивидуальной работы при решении учебных задач; принимать цель совместной деятельности, планировать организацию совместной работы, распределять виды работ, договариваться, обсуждать процесс и результат работы;

обобщать мнения нескольких людей;

участвовать в групповых формах работы (обсуждения, обмен мнениями, мозговые штурмы и др.); выполнять свою часть работы и координировать свои действия с другими членами

команды; оценивать качество своего вклада в общий продукт по критериям, сформулированным участниками взаимодействия.

3) Универсальные регулятивные действия обеспечивают формирование смысловых установок и жизненных навыков личности.

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.

Предметные результаты освоения курса

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.

Содержание учебного курса

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 паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом 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 кибербуллинга.

Тема 8. Публичные аккаунты. 1 час.

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. 2 часа.

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. 3 часа.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

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. 2 час.

Способы защиты устройств от вредоносного кода. Антивирусные программы 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 безопасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

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, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные 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 различных 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.

Повторение. Волонтерская практика. 3 часа.

В процессе преподавания курса используются разнообразные формы и форматы обучения:

- традиционный урок (коллективная и групповая формы работы),
- тренинги (в классической форме или по кейсметоду),
- дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение),
- смешанное обучение;
- лекции приглашенных специалистов.

Тематическое планирование

Тема	содержание	Кол-во часов
Тема 1. «Безопасность общения»		
Общение в социальных сетях и мессенджерах	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	1
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.	1
Пароли для аккаунтов социальных сетей	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	1
Безопасный вход в аккаунты	Виды аутентификации. Настройки безопасности. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	1
Настройки конфиденциальности в социальных сетях	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	1
Публикация информации в социальных сетях	Персональные данные. Публикация личной информации.	1
Кибербуллинг	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	1
Публичные аккаунты	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	1
Фишинг	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	2
Выполнение и защита индивидуальных и групповых проектов		3
Тема 2. «Безопасность устройств»		
Что такое вредоносный код	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	1
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.	1

Методы защиты от вредоносных программ	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	2
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		3
Тема 3 «Безопасность информации»		
Социальная инженерия: распознать и избежать	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	1
Ложная информация в Интернете	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	1
Безопасность при использовании платежных карт в Интернете	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	1
Беспроводная технология связи	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	1
Резервное копирование данных	Безопасность личной информации. Создание резервных копий на различных устройствах.	1
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.	1
Выполнение и защита индивидуальных и групповых проектов		3
Повторение, волонтерская практика, резерв		3
ИТОГО		34