государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа №7
имени Героя Советского Союза Ф.И. Ткачева
города Жигулевска городского округа Жигулевск Самарской области

Утверждено
Директор школы
_____Крюкова Л.В.
Приказ от «1» сентября 2021 г.
№ 170-ОД

Проверено
Зам. директора школы по УВР
_____Абрамова В.Н.
«31» августа 2021 г.

Рассмотрено на
заседании ШМО
_____Матузова О.В.
«30» августа 2021 г.
Протокол № 1

ЭП

C=RU, O=ГБОУ СОШ №7, CN=Крюкова Л.В., E=school7_zhg@samara.edu.ru
00bc5abd78f393aa6e
2021.09.24 07:52:54+04'00'

РАБОЧАЯ ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
ПО ОБЩЕИНТЕЛЛЕКТУАЛЬНОМУ НАПРАВЛЕНИЮ КУРС «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
7 класс

Составлена учителем:
Наумовой Ольгой Владимировной
Квалификационная категория: первая
Стаж педагогической работы: 17 лет

Пояснительная записка

Рабочая программа внеурочной деятельности «Информационная безопасность» разработана на основе:

- Федерального закона Российской Федерации от 29.12.2012 № 273-фз «Об образовании в Российской Федерации».
- Приказа Министерства образования и науки РФ от 17.05.2012 №413 «Об утверждении федерального государственного образовательного стандарта среднего общего образования» (в редакции от 29.06.2017).
- Письма Департамента общего образования Минобрнауки России от 12.05.2011 № 03-296 «Об организации внеурочной деятельности при введении федерального государственного образовательного стандарта общего образования».
- Письма Минобрнауки Самарской области от 17.02.2016 № МО-16-09-01/173-ту «Об организации занятий внеурочной деятельности в общеобразовательных организациях Самарской области, осуществляющих деятельность по основным общеобразовательным программам».
- Основной образовательной программы основного общего образования ГБОУ СОШ № 7.
- Примерных программ внеурочной деятельности. Авторской программы «Информационная безопасность, или на расстоянии одного вируса». Автор: Наместникова М.С.

Цели обучения курса

Основными целями изучения курса «Информационная безопасность» 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.

Место курса в учебном плане

Программа курса «Информационная безопасность» реализуется в 7-х классах, 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. Программа рассчитана на 34 учебных

часа. На изучение курса отводится по 1 часу в неделю в 7 классах в течение одного учебного года.

УМК:

1. Наместникова М.С. «Информационная безопасность, или на расстоянии одного вируса». 7-9 классы: Учебное пособие.

Личностные, метапредметные и предметные результаты освоения учебного курса

Метапредметные.

В результате освоения учебного курса обучающийся сможет:

Регулятивные универсальные учебные действия.

- 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.

Предметные универсальные учебные действия.

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.

Личностные универсальные учебные действия.
- 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 учебного курса

Раздел 1. «Безопасность общения»

Общение в социальных сетях и мессенджерах. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. 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. Пароли для аккаунтов социальных сетей. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию

паролей. Безопасный вход в аккаунты. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта. Настройки конфиденциальности в социальных сетях. Настройки приватности и конфиденциальности в разных

социальных сетях. Приватность и конфиденциальность в мессенджерах. Публикация информации в социальных сетях. Персональные данные. Публикация личной информации. Кибербуллинг. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. Публичные аккаунты. Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг. Фишинг. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Раздел 2. «Безопасность устройств»

Что такое вредоносный код. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов. 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. Методы защиты от вредоносных программ. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Распространение вредоносного кода для мобильных устройств. Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Раздел 3 «Безопасность информации»

Социальная инженерия: распознать и избежать. Приемы социальной инженерии. Правила безопасности при виртуальных контактах. Ложная информация в Интернете. Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы. Безопасность при использовании платежных карт в Интернете. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов. Беспроводная технология связи. Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях. Резервное копирование данных. Безопасность личной информации. Создание резервных копий на различных устройствах. 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.

Повторение. Волонтерская практика.

Тематическое планирование. 7 класс

п/п	Название разделов и тем уроков, количество часов	Элементы содержания урока	Предметные планируемые результаты обучения
«Безопасность общения»			
1	Общение в социальных сетях и мессенджерах	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Научиться выполнять базовые операции при использовании мессенджеров и социальныхсетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
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.	Научиться руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучит правила сетевого общения.
3	Пароли для аккаунтов социальных сетей	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Изучит основные понятия регистрационной информации и шифрования. Научиться их применить.
4	Безопасный вход в аккаунты	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Научиться объяснять причины использования безопасного входа при работе на чужом устройстве. Будет демонстрировать устойчивый навык безопасного входа.
5	Настройки конфиденциальности в социальных сетях	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Научиться раскрывать причины установки закрытого профиля; менять основные настройки приватности в личном профиле.
6	Публикация информации в социальных сетях	Персональные данные. Публикация личной информации.	Научиться осуществлять поиск и использовать информацию, необходимую для выполнения поставленных задач.
7	Кибербуллинг	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Научиться реагировать на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Научиться решать экспериментальные задачи; самостоятельно создавать источники информации разного типа и для разных аудиторий, соблюдая правила информационной

9-10	Фишинг	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Какзащититься от фишеров в социальных сетях и мессенджерах.	безопасности. Научиться анализировать проблемные ситуации; разрабатывать кейсы с примерами. Из личной жизни/жизни знакомых; разрабатывать и распространять чек-листа (памятки) по противодействию фишингу.
11-13	Выполнение и защита индивидуальных и групповых проектов		Самостоятельная работа.
«Безопасность устройств» (8 часов)			
14	Что такое вредоносный код	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Научиться соблюдать технику безопасности при эксплуатации компьютерных систем; использовать инструментальные программные средства и сервисы адекватно задаче.
15	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.	Научиться выявлять и анализировать (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
16-17	Методы защиты от вредоносных программ	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Изучит виды антивирусных программ и правила их установки.
18	Распространение вредоносного кода для мобильных устройств	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Научиться разрабатывать презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.
19-21	Выполнение и защита индивидуальных и групповых проектов		Научиться работать индивидуально и в группе; принимать позицию собеседника, понимая позицию другого; различать в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.

«Безопасность информации»			
22	Социальная инженерия: распознать и избежать	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Научиться находить нужную информацию в базах данных, составляя запросы на поиск; систематизировать получаемую информацию в процессе поиска; определять возможные
23	Ложная информация в Интернете	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	источники необходимых сведений, осуществляет поиск информации; отбирать и сравнивать материалы по нескольким источникам; анализировать и оценивать достоверность информации.
24	Безопасность при использовании платежныхкарт в Интернете	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Научиться приводить примеры рисков, связанных с совершением онлайн покупок (определить источник риска); разрабатывать возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.
25	Беспроводная технология связи	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичныхсетях.	Научиться использовать различную информацию, определять понятия. Изучит особенности и стиль ведения личных и публичных аккаунтов.
26-27	Резервное копирование данных	Безопасность личной информации. Создание резервных копий на различных устройствах.	Научиться создавать резервные копии.
28	Основы государственной политики вобласти 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.	Научиться привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства.
29-31	Выполнение и защита индивидуальных и групповых проектов		
32-34	Повторение, волонтерская практика		