Государственное бюджетное общеобразовательное учреждение Самарской области
основная общеобразовательная школа № 23 городского округа Чапаевск Самарской области

Рассмотрено на заседании педагогического совета Протокол № 1 от 24.08.2020 г.	Проверено Ответственная за учебную работу _____Иншакова С.В. 28.08.2020 г.	Утверждаю Директор ГБОУ ООШ № 23 г.о.Чапаевск _____Копылова Ж.В. Приказ № 71-од 28.08.2020г.

Рабочая программа

внеурочной деятельности

«Информационная безопасность»

2020 - 2021 учебный год

8 класс

Составитель программы:
Иншакова С.В., учитель информатики

2020 г.

Программа курса «Информационная безопасность» состоит из двух модулей и адресована учащимся 7, 8, 9 классов (Модуль1), а также родителям обучающихся всех возрастов с 1 по 9 класс (Модуль 2). Программа учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным, метапредметным и личностным результатам.

Разработана на основании примерной рабочей программы учебного курса «Цифровая гигиена», рекомендованной Координационном советом Учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019), на основе программы курса «Информационная безопасность, или на расстоянии одного вируса» Наместниковой М.С.

Место внеурочной деятельности в учебном плане

Программа курса рассчитана на один год (34 учебных часа, из них 22 часа - учебных занятий, 9 часов - подготовка и защита учебных проектов, 3 часа – повторение, т.е. по 1 часу в неделю в 7, 8 и 9 классах. в течение одного учебного года

Модуль для родителей предусматривает: выступления на родительских собраниях, мини семинары, совместные родительско-ученические проекты, презентаций личного опыта.

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.

Результаты освоения курса (Модуль 1)

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

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.

Виды деятельности обучающегося: Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.

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.

Виды деятельности обучающегося Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.

Тема 3. Пароли для аккаунтов социальных сетей. 1 час.

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

Виды деятельности обучающегося Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Виды деятельности обучающегося Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа

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

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

Виды деятельности обучающегося Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.

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

Персональные данные. Публикация личной информации.

Виды деятельности обучающегося Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.

Тема 7. Кибербуллинг. 1 час.

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

Виды деятельности обучающегося Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.

Тема 8. Публичные аккаунты. 1 час.

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

Виды деятельности обучающегося Решает экспериментальные задачи.

Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.

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.

Виды деятельности обучающегося Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.

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.

Виды деятельности обучающегося Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче

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.

Виды деятельности обучающегося Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.

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.

Изучает виды антивирусных программ и правила их установки.

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

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

Виды деятельности обучающегося Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.4
Виды деятельности обучающегося Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение(точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.

Раздел 3 «Безопасность информации»

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

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Виды деятельности обучающегося Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска

Тема 2. Ложная информация в Интернете. 1 час.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Виды деятельности обучающегося Определяет возможные источники необходимых сведений, осуществляет поиск информации.

Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Виды деятельности обучающегося Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.

Тема 4. Беспроводная технология связи. 1 час.

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

Виды деятельности обучающегося Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Виды деятельности обучающегося Создает резервные копии.

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.

Виды деятельности обучающегося Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации; отражающего правовые аспекты защиты киберпространства

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Повторение. Волонтерская практика. 3 часа.

Тематическое планирование (Модуль 1)

	Тема	Количество часов		
		всего	**теория**	**проект**
1.	«Безопасность общения»	14	11	3
2.	«Безопасность устройств»	8	5	3
3.	«Безопасность информации»	10	7	3
4.	Повторение, волонтерская практика, резерв	2	0	2
	Итого	**34**	**23**	**11**

МОДУЛЬ 2 (для родителей)

Цель: оценка своих возможностей в помощи детям в Интернете.

Формами проведения мероприятий для родителей также могут являться: выступления на родительских собраниях, мини-семинары на основе технологий онлайн обучения, совместное обучение, совместные родительско-детские .

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

Тематическое планирование учебного курса (Модуль 2).

№	Название темы	Сроки проведения
1.	Цифровая гигиена: зачем это нужно? Понятия Интернет- угроз. Изменения границ допустимого в контексте цифрового образа жизни	сентябрь
2.	Изменения здоровья детей и подростков	октябрь
3.	Понятие периметра безопасности. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка.	ноябрь
4.	Атаки, связанные с компьютерной инженерией. Действия при обнаружении вредоносных кодов на устройствах	январь
5.	Груминг, кибербуллинг. Чему мы должны научить ребёнка для профилактики насилия в Сети?	февраль
6.	. Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?	март
7.	Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.	апрель
8.	Пособия и обучающие программы по формированию навыков цифровой гигиены	май