

**Государственное бюджетное общеобразовательное учреждение
Самарской области
средняя общеобразовательная школа №10 имени Героя России Сергея Анатольевича Хихина
городского округа Чапаевск Самарской области**

Рассмотрено на заседании МО
Руководитель МО
_____ Пономаренко О.С...
Протокол № _____ от _____

Проверено
Зам. директора по ВР
_____ Артюхина М.А.

Утверждаю
Директор ГБОУ СОШ №10
г.о. Чапаевск

Пылева Н.В.

**Рабочая программа внеурочной деятельности
«Информационная безопасность»
ФГОС ООО
(из курса «Цифровая гигиена»)
7 класс**

2024 – 2025 учебный год
Чапаевск, 2024 г.

Пояснительная записка

Актуальность данной программы определена тем, что она является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация программы создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Программа реализует обще интеллектуальное направление во внеурочной деятельности.

Данная рабочая программа «Информационная безопасность» разработана на основе:

- примерной рабочей Программы учебного курса «Цифровая гигиена», рекомендованной координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019)
- учебного пособия для общеобразовательных организаций «Информационная безопасность, или на расстоянии одного вируса» 7 – 9 классы. Внеурочная деятельность /М.С. Наместникова. –М.: Просвещение, 2019.

Цель программы:

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.

Срок реализации программы – 1 год.

Участники программы: обучающиеся 7-х классов.

Объем курса – 35 часов (один час в неделю), из них 22 часа – учебных занятий, 7 часов – подготовка и защита учебных проектов, 4 часа – повторение.

Место проведения: программа составлена с учетом санитарно-гигиенических требований, возрастных особенностей учащихся и рассчитана на работу в учебном компьютерном классе, в котором 16 учебных мест и одно рабочее место – для преподавателя.

Формы организации внеурочной деятельности: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс- методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микро- обучение), смешанный формат.

Необходимое оборудование:

1. Компьютерное учебное место: - 16 штук, для учителя - 1. Все компьютеры имеют выход в Интернет.
2. Мультимедиа проектор и экран.
4. Интерактивная доска SMART Board.
5. Принтер.
6. Сканер.
7. Доска маркерная.

Взаимосвязь с программой воспитания

Программа курса внеурочной деятельности «Информационная безопасность» разработана с учётом рекомендаций Примерной программы воспитания. Это позволяет на практике соединить обучающую и воспитательную деятельность педагога, ориентировать её не только на интеллектуальное, но и на нравственное, социальное развитие учащегося

Особенности работы педагога по программе

Задача педагога состоит в том, чтобы сопровождать процесс профессиональной ориентации школьника, раскрывая потенциал каждого через вовлечение в многообразную деятельность, организованную в разных формах. При этом результатом работы педагога в первую очередь является личностное развитие учащегося. Личностных результатов педагог может достичь, увлекая учащегося совместной и интересной им общей деятельностью, устанавливая во время занятий доброжелательную, поддерживающую атмосферу, насыщая занятия ценностным содержанием.

Планируемые результаты освоения учебного модуля «Информационная безопасность»

Личностные результаты.

- 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.

Предметные:

Ученик 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.

Ученик овладеет:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Ученик 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 результаты:

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.

Содержание программы

Содержание программы учебного курса «**Информационная безопасность**» соответствует темам примерной основной образовательной программы основного общего образования (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.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации». Каждый раздел данного учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

Система контролирующих материалов для оценки планируемых результатов

В течение всего курса обучения проводятся:

- ✓ конкурсы работ учащихся по созданию тематических презентаций, видеороликов;
- ✓ выставки лучших работ, выполненных в виде брошюр, листовок, буклетов, плакатов;
- ✓ защита промежуточных проектов

Основой для оценивания практической деятельности учеников выступают результаты анализа созданных ими проектов. Итоговый контроль

осуществляется в конце всего курса. Он имеет форму зачета творческих работ.

Оценка выражается различными способами: устные суждения учителя, ведение протокола защиты проектов. Протокол может заполняться как учителем, так и учениками, кроме тех, кто выступает на данный момент. Затем подсчитывается сумма баллов и объявляется общий итог.

Оценка результативности учащихся осуществляется по следующим критериям:

- высокий уровень – успешное освоение учащимся более 70% содержания программы, подлежащего аттестации;
- средний уровень - успешное освоение учащимся от 50% до 70% содержания программы, подлежащего аттестации;
- низкий уровень – успешное освоение учащимся менее 50% содержания программы, подлежащего аттестации.

Итоги аттестации фиксируются педагогом в журнале внеурочной деятельности.

Уровень развития у учащихся личностных качеств определяется на основе сравнения результатов их диагностики в начале и конце курса.

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 часа.

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. 4 часа.

Тематическое планирование

№	Название темы	Всего	Форма деятельности	Электронные образовательные ресурсы
1	Безопасность общения	13	Беседы, диалоги, дискуссии.	https://www.kaspersky.ru/ http://www.threatpost.ru/
2	Безопасность устройств	8	Круглый стол, беседы, диалоги, дискуссии	https://www.kaspersky.ru/ http://www.threatpost.ru/
3	Безопасность информации	10	Диалоги, беседы, дискуссии	https://www.kaspersky.ru/ http://www.threatpost.ru/
4	Повторение	4	Круглый стол, беседы, диалоги, дискуссии	https://www.kaspersky.ru/ http://www.threatpost.ru/
	Итого:	35		