государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа №4 п.г.т. Безенчук муниципального района Безенчукский Самарской области

Рассмотрено на заседании ШМО
ГБОУ СОШ №4 п.г.т. Безенчук
Протокол №__1__
от «_27_» августа 2021г.

Проверено
Заместитель директора по УВР
_____ Е.Б. Демидова

Утверждаю
Директор школы
_____ Л.В. Шеховцова

РАБОЧАЯ ПРОГРАММА
внеурочной деятельности курса
«Информационная безопасность, или на расстоянии одного вируса»
Уровень образования: основное общее образование (7 класс)
Срок реализации: 1 год

Учитель информатики
И.Е. Сидорова
Н.И. Быстрова
М.В. Бекетова

Безенчук, 2022

Пояснительная записка

Рабочая программа по предмету «Информационная безопасность» разработана на основе следующих документов:

1. Федеральный закон от 29.12.2012 года № 273-ФЗ «Об образовании в Российской Федерации» (ст.28, 30);
2. Федеральный государственный образовательный стандарт основного общего образования (в ред. от 31.12.2015 г.);
3. ООП ООО ГБОУ СОШ № 4 п.г.т. Безенчук Самарской области;

Курс «Цифровая гигиена» 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. Этот учебный курс состоит из двух модулей, первым из которых является модуль «Информационная безопасность».

Для реализации рабочей программы «Информационная безопасность» используется учебное пособие: «Информационная безопасность, или На расстоянии одного вируса». 7-9 классы: учебное пособие для общеобразовательных организаций/М.С. Наместникова. – М., Просвещение, 2019.

Цели изучения учебного предмета «Информационная безопасность»

Основными целями изучения «Технологии» в системе основного общего образования 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 предмета «Информационная безопасность» в базисном учебном (образовательном) плане

Программа в 7 классах рассчитана на 34 учебных часа (1 час. в неделю).

Планируемые результаты изучения предмета «Информационная безопасность»

При освоении предмета «Технология» выпускниками основной школы обеспечивается достижение ***личностных, метапредметных и предметных результатов.***

Личностными результатами освоения программы являются:

- 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.

Метапредметными результатами освоения программы являются:

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.

<u>Предметные результаты освоения программы</u>

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 Интернетресурсы и другие базы данных.

Содержание учебного курса «Информационная безопасность»

Раздел 1. «Безопасность общения» (14 часов)

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.

Темы 9-10. Выполнение и защита индивидуальных или групповых проектов (4 часа)

Выполнение и защита индивидуальных и групповых проектов.

Раздел 2. «Безопасность устройств» (9 часов)

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.

Темы 5-6. Выполнение и защита индивидуальных или групповых проектов (4 часа)

Выполнение и защита индивидуальных и групповых проектов.

Раздел 3. «Безопасность информации » (11 часов)

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 страниц.

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 часа)

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Темы 7-8. Выполнение и защита индивидуальных или групповых проектов (4 часа)

Выполнение и защита индивидуальных и групповых проектов.

Тематическое планирование

№№ п/п	Наименование разделов	Количество часов	Примечания
1.	Безопасность общения	14	
2.	Безопасность устройств	9	
3.	Безопасность информации	11	
	Итого:	34	

C=RU, O=ГБОУ СОШ № 4 п.г.т. Безенчук, CN=Шеховцова Л.В., E=bez-s4@mail.ru 00ef1f4c46e97160df 2022.03.10 08:44:46+04'00'