

государственное бюджетное общеобразовательное учреждение Самарской области
средняя общеобразовательная школа с. Екатериновка
муниципального района Безенчукский Самарской области

Рассмотрена
ШМО учителей
естественно-научного цик-
ла

Протокол № 1
от «29» августа 2023 г.

Проверено
зам. директор по УВР
Сорокина Е.Ю.

«30» августа 2023 г.

Утверждаю
И.о.директора ГБОУ СОШ с.
Екатериновка м.р. Безенчукский
Семенкина Л.Н.

«30» августа 2023 г.

РАБОЧАЯ ПРОГРАММА
курса внеурочной деятельности

Предмет (курс) «Информационная безопасность»

Возраст 14 лет

Количество часов 1ч в неделю

2023

Пояснительная записка

Программа курса «Информационная безопасность» адресована учащимся 8 класса и направлена на достижение следующих планируемых результатов Федерального государственного образовательного стандарта основного общего образования:

- предметных;
- метапредметных (регулятивных, познавательных, коммуникативных);
- личностных.

Курс является важной составляющей частью работы с учащимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.), задумывающимися о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории и технологических основ информационной безопасности.

Программа курса ориентирована на выполнение требований к организации и содержанию обучающейся деятельности школьников. Ее реализация даёт возможность раскрытия индивидуальных способностей школьников, развития интереса к различным видам индивидуальной и групповой деятельности, закрепления умения самостоятельно организовать свою учебную, в том числе проектную деятельность. Кроме того, программа курса дает возможность закрепить ряд результатов обучения, предусмотренных программой учебного курса по предмету «Информатика»

Цель программы:

- формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

Задачи программы:

- дать представление о современном информационном обществе, информационной безопасности личности и государства;
- сформировать навыки ответственного и безопасного поведения в современной информационно-телекоммуникационной среде;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом;
- сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовать информационный процесс);
- дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
- познакомить со способами защиты от противоправных посягательств в сети Интернет, защиты личных данных.

Содержание программы учебного курса

Содержание программы учебного курса (Модуль 1) 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 учебного курса (Модуля 1) завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

Содержание учебного курса

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. Социальная сеть. История социальных сетей. Мессенджеры. Назначение

социальных сетей и мессенджеров. Пользовательский контент.

Тема 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.

Тема 3. Пароли для аккаунтов социальных сетей.

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

Тема 4. Безопасный вход в аккаунты.

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

Тема 5. Настройки конфиденциальности в социальных сетях. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг.

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

Тема 8. Публичные аккаунты.

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.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. 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.

Тема 3. Методы защиты от вредоносных программ.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. 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.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 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.

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

Тема 4. Беспроводная технология связи.

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

Тема 5. Резервное копирование данных.

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.

Планируемые результаты освоения учебного предмета

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; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Тематическое планирование учебного курса
1 год

№ п/п	Тема занятия	Форма проведения занятия	Коли- чество часов	ЭОР
1	Раздел 1. «Безопасность общения» Общение в социальных сетях и мессенджерах (1 ч.)	Беседа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3066/start/
2	С кем безопасно общаться в интернете (1 ч.)	Практическая работа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/1515/start/
3	Пароли для аккаунтов социальных сетей (1 ч.)	Беседа	1	http://персональныеданные.дети/personalnye_dannye/
4	Безопасный вход в аккаунты (1 ч.)	Практическая работа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3256/start/
5	Настройки конфиденциальности в социальных сетях (1 ч.)	Практическая работа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3255/start/
6	Публикация информации в социальных сетях (1 ч.)	Практическая работа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3065/start/
7	Кибербуллинг (1 ч.)	Практическая работа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3064/start/
8	Публичные аккаунты (1 ч.)	Практическая работа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3063/start/

9	Фишинг (2 ч.)	Беседа	2	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3065/start/
10	Выполнение и защита индивидуальных и групповых проектов (3 ч.)	Практическая работа	3	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3063/start/
1	Раздел 2 «Безопасность устройств» Что такое вредоносный код. (1 ч.)	Практическая работа	1	http://www.saferinternet.ru
2	Распространение вредоносного кода (1 ч.)	Практическая работа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3468/start/
3	Методы защиты от вредоносных программ (2 ч.)	Практическая работа	.2	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3117/start/
4	Распространение вредоносного кода для мобильных устройств (1 ч.)	Беседа	1	Информатика - РЭШ – 8 класс
5.	Выполнение и защита индивидуальных и групповых проектов (3 ч.)	Практическая работа	3	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3062/start/
1	Раздел 3 «Безопасность информации» Социальная инженерия: распознать и избежать (1ч.)	Беседа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3061/start/
2	Ложная информация в Интернете. (1 ч.)	Беседа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3062/start/

3	Безопасность при использовании платежных карт в Интернете. (1 ч.)	Практическая работа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/1928/start/
4	Беспроводная технология связи. (1 ч.)	Практическая работа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3061/start/
5	Резервное копирование данных. (1 ч.)	Беседа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/3254/start/
6	Основы государственной политики в области формирования культуры информационной безопасности (2 ч.)	Практическая работа	1	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/1928/start/
7	Выполнение и защита индивидуальных и групповых проектов (3 ч.)	Практическая работа	2	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/1928/start/
8	Повторение, волонтерская практика, резерв (3 ч.)	Практическая работа	3	Информатика - РЭШ – 8 класс https://resh.edu.ru/subject/lesson/1928/start/
9	Итоговое занятие	Защита проекта	2	ПК