Муниципальное общеобразовательное учреждение «Тереньгульский лицей при УлГТУ»
муниципального образования «Тереньгульский район» Ульяновской области

Рассмотрено на
ШМО учителей математики

Протокол № 1 от 25. 08.2023
_____ М.В. Курникова

Согласовано
Зам. директора по УВР
30.08.2023
_____ Л.А. Кириллова

Утверждаю
Директор лицея
Приказ от 31.08.2023 № 112
_____ Е. А. Рукавишникова

Рукавишникова Елена Александровна

Подписан цифровой подписью: Рукавишникова Елена Александровна
DN: CN=Рукавишникова Елена Александровна, E=tershkola@yandex.ru
Основание: Я подтверждаю этот документ
Расположение: р. п. Тереньга
Дата: 2023.11.12 20:40:05+04'00'
Foxit PDF Editor Версия: 13.0.0

Рабочая программа
по внеурочной деятельности
общеинтеллектуального направления
«Информационная безопасность, или на расстоянии одного вируса»
для обучающихся 9-х классов

Срок реализации: 2023-2024 учебный год

Составитель:
И.В. Ечкова,
учитель информатики
высшей категории

Год составления: 2023

Аннотация к рабочей программе

Рабочая программа курса внеурочной деятельности по информатике « Информационная безопасность, или на расстоянии одного вируса» для 9 класса разработана на основе:

- Требований Федерального закона от 29 декабря 2012 года N 273-ФЗ «Об образовании в Российской Федерации» (последняя редакция);
- Требований Федерального государственного стандарта основного общего образования, утверждённого приказом Министерства образования и науки РФ от 17 декабря 2010 года № 1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования», с изменениями, утвержденными приказом Минобрнауки России от 29.12.2014 №1644, приказом Минобрнауки от 31. 12.2015 № 1577 и приказом Минпросвещения России от 11.12.2020г. №712;
- Примерной основной образовательной программы основного общего образования, одобренной решением Федерального учебно-методического объединения по общему образованию (Протокол от 08.04.2015 №1/15). В редакции протокола №1\20 от 04.02.2020 федерального учебно-методического объединения по общему образованию);
- Постановления Главного государственного санитарного врача РФ от 28 сентября 2020 г. N 28 "Об утверждении санитарных правил СП 2.4.3648-20 "Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи"" ;
- Рабочей программы воспитания «МОУ «Тереньгульский лицей при УлГТУ» на 2023-2024 учебный год, утвержденной приказом директора от 22.08.2023, №84/1;
- Плана внеурочной деятельности на 2023-2024 учебный год, утвержденного приказом директора лицея от 31.08.2023 № 112;
- Календарного учебного графика МОУ «Тереньгульский лицей при УлГТУ» на 2023-2024 учебный год, утвержденного приказом директора лицея от 31.08.2023 №109;
- Основной образовательной программы основного общего образования Муниципального общеобразовательного учреждения «Тереньгульский лицей при УлГТУ» , утвержденной директором лицея от 31.08.2023 № 116;

- Сборника рабочих программ по внеурочной деятельности начального, основного и среднего общего образования : учеб. пособие для общеобразоват. организаций. — М. : Просвещение, 2020.

Программа рассчитана на 34 часа внеурочной деятельности.

Цель программы:

- формирование активной позиции учащихся в получении знаний и умений выявлять информационную угрозу, определять степень её опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищённости 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 организовывать информационный процесс);
- дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
- познакомить со способами защиты от противоправных посягательств в Интернете, защиты личных данных.

1.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОГО КУРСА

В ходе изучения курса в основном формируются и получают развитие следующие **метапредметные результаты:**

• умение самостоятельно планировать пути достижения целей, в том числе альтернативные, осознанно выбирать наиболее эффективные способы решения учебных и познавательных задач; умение соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности в процессе достижения результата, определять способы действий в рамках предложенных условий и требований, корректировать свои действия в соответствии с изменяющейся ситуацией;

умение оценивать правильность выполнения учебной задачи, собственные возможности ее решения; владение основами самоконтроля, самооценки, умение организовывать учебное сотрудничество и совместную деятельность с учителем и сверстниками; работать индивидуально и в группе: находить общее решение и разрешать конфликты на основе согласования позиций и учета интересов; формулировать, аргументировать и отстаивать свое мнение; формирование и развитие компетентности в области использования информационно-коммуникационных технологий (далее ИКТ-компетенции).

Вместе с тем вносится существенный вклад в развитие **личностных результатов**: формирование ответственного отношения к учению, готовности и способности обучающихся к саморазвитию и самообразованию на основе мотивации к обучению и познанию, осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов, а также на основе формирования уважительного отношения к труду, развития опыта участия в социально значимом труде; формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности. В части развития **предметных результатов** наибольшее влияние изучение курса оказывает на:

формирование информационной и алгоритмической культуры; формирование представления о компьютере как универсальном устройстве обработки информации; развитие основных навыков и умений использования компьютерных устройств; формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права; формирование навыков и умений безопасного общения в сети Интернет, безопасного применения устройств компьютера и других гаджетов, безопасных путей получения и передачи информации.

1. Безопасность общения

Обучающийся научится: Использовать функции браузера по запоминанию паролей, работать на чужом компьютере с точки зрения безопасности личного аккаунта, использовать настройки приватности и конфиденциальности в разных социальных сетях.

Обучающийся получит возможность научиться: Избегать кибербуллинга, настроивать приватность публичных страниц, защите от фишеров в социальных сетях и мессенджерах

2.Безопасность устройств

Обучающийся научится: Распознавать вредоносные коды, функции вредоносных кодов, способы доставки вредоносных кодов, распознавать исполняемые файлы , вредоносные рассылки, вредоносные скрипты, способам выявления наличия вредоносных кодов на устройствах.

Обучающийся получит возможность научиться:

Действиям при обнаружении вредоносных кодов на устройствах, способам защиты устройств от вредоносного кода, правилам защиты от вредоносных кодов, правилам безопасности при установке приложений на мобильные устройства.

3.Безопасность информации

Обучающийся научится: Приемам социальной инженерии, правилам безопасности при виртуальных контактах.

Обучающийся получит возможность научиться: Правилам совершения онлайн покупок, правилам работы в публичных сетях, создавать резервные копии на различных устройствах.

2.Содержание учебного курса

Тема 1. ***Безопасность общения*** , 13 часов

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах. Персональные данные. Публикация личной информации. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать. Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. Настройки приватности публичных страниц. Правила ведения публичных страниц. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Тема 2. ***Безопасность устройств, 8 часов***

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов. 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. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Тема 3. ***Безопасность информации*** , 10 часов

Приемы социальной инженерии. Правила безопасности при виртуальных контактах. Фейковые новости. Поддельные страницы. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов. Публичные и непубличные сети. Правила работы в публичных сетях. Безопасность личной информации. Создание резервных копий на различных устройствах.

Повторение, 2 часа

Формы и методы проведения заданий.

Реализация программы предусматривает использование в качестве методологической основы системно- деятельностного подхода проведение занятий в форме лекций, семинаров, практических работ с использованием соответствующего оборудования, поисковых исследований, различных видов проектной и творческой деятельности.

Проведение занятий возможно на базе учебного кабинета, оснащённого оборудованием для использования информационно- коммуникационных технологий.

Виды деятельности учащихся в рамках программы:

- Слушание объяснений учителя.
- Слушание и анализ выступлений своих товарищей.
- Самостоятельная работа с учебником.
- Работа с научно-популярной литературой;
- Отбор и сравнение материала по нескольким источникам.
- Написание рефератов и докладов.
- Выполнение заданий по разграничению понятий.
- Систематизация учебного материала.
- Работа с книгой
- Анализ проблемных ситуаций.

.

Приложение

Календарно-тематическое планирование

Класс	№ п.п	Разделы программы и темы занятий	Кол-во часов	Дата проведения по плану	Фактическая дата проведения
	Тема 1 Безопасность общения				
9	1	Общение в социальных сетях и мессенджерах.	1	07.09	
	2	С кем безопасно общаться в интернете.	1	14.09	
	3	Пароли для аккаунтов социальных сетей.	1	21.09	
	4	Безопасный вход в аккаунты.	1	28.09	
	5	Настройки конфиденциальности в социальных сетях.	1	05.10	
	6	Публикация информации в социальных	1	19.10	

		сетях.			
	7-8	Кибербуллинг.	2	26.10 02.11	
	9	Публичные аккаунты.	1	09.11	
	10	Фишинг	1	16.11	
	11	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов	1	30.11	
	12-13	Выполнение и защита индивидуальных и групповых проектов	3	07.12 14.12 21.12	
9	Тема 2 Безопасность устройств				
	14	Что такое вредоносный код.	1	28.12	
	15	Распространение вредоносного кода.	1	11.01	
	16-17	Методы защиты от вредоносных программ.	2	18.01 25.01	
	18	Распространение вредоносного кода для мобильных устройств.	1	01.02	
	19	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов	1	08.02	

	20-21	Выполнение и защита индивидуальных и групповых проектов	2	15.02 29.02	
9	Тема 3 Безопасность информации				
	22-23	Социальная инженерия: распознать и избежать.	2	07.077 14.03	
	24-25	Ложная информация в Интернете.	2	21.03 28.03	
	26	Безопасность при использовании платежных карт в Интернете.	1	04.04	
	27	Беспроводная технология связи.	1	11.04	
	28	Резервное копирование данных.	1	25.04	
	29	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов	1	02.05	
	30-31	Выполнение и защита индивидуальных и групповых проектов	2	16.05 16.05	
	32-33	Повторение, резерв	2	23.05 23.05	