государственное бюджетное общеобразовательное учреждение Самарской области
средняя общеобразовательная школа № 7 города Похвистнево городского округа Похвистнево Самарской области

Проверено
Зам. директора по УВР
_____ Данилина Л.И.
(подпись) (ФИО)
«_29_»___августа___2023__ г.

Утверждено
приказом № 258 - од
от «_30__»____августа____2023 г.

И.о.директора _____Назаров С.Н.
(подпись) (ФИО)

РАБОЧАЯ ПРОГРАММА

Предмет (курс) ___«Информационная безопасность или На расстоянии одного вируса»

Класс __9_____

Общее количество часов по учебному плану __34_____

Назаров Сергей Николаевич
О=ГБОУ СОШ № 7 города Похвистнево, CN=Назаров Сергей Николаевич, E=so_svu_school7@samara.edu.ru
Я подтверждаю этот документ своей удостоверяющей подписью
00b661bfd6008cc3bf
2023.11.09 09:02:35+04'00'

Рассмотрена на заседании МО _____естественно-математического цикла_____
(название методического объединения)
Протокол №_____ от «_____»_____ 2023г.
Руководитель МО_____Матвеева Н.Ю._
(подпись) (ФИО)

I. Пояснительная записка.

Рабочая программа по внеурочной деятельности «Информационная безопасность или На расстоянии одного вируса» составлена для учащихся 9 классов. Программа разработана на основе учебного пособия Наместникова М.С. «Информационная безопасность, или на расстоянии одного вируса 7-9 классы, Просвещение 2020 год» и направлена на достижение следующих планируемыхрезультатовФедеральногогосударственногообразовательногостандартаосновногообщегообразования:

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

Курсявляетсяважнойсоставляющейчастьюработысучащимися,активноиспользующимиразличныесетевыеформыобщения(социальныесети,игры,пр.),задумывающимисяосвоейличнойбезопасности,безопасностисвоейсемьиисвоихдрузей, а также проявляющими интерес к изучению истории и технологических основинформационнойбезопасности.

Направлениепрограммыкурсавнеурочнойдеятельности–общеинтеллектульное.

ПрограммакурсаориентированнавыполнениетребованийФедеральногогосударственногообразовательногостандартаосновногообщегообразованиякорганизации и содержанию внеурочной 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.

Цель программы:

- формированиеактивнойпозициишкольниковвполучениизнанийиуменийвыявлятьинформационнуюугрозу,определятьстепеньееопасности,предвидетьпоследствияинформационнойугрозыи противостоятьим;
- 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 современной информационно-телекоммуникационной среде;
- сформироватьнавыкипопрофилактикеикоррекциизависимогоповеденияшкольников,связанногоскомпьютернымитехнологиямиИнтернетом;
- 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.

Общая характеристика курса.

Данный курс предполагает организацию работы в соответствии с содержанием, предназначенных для обучающихся 9 классов. Модуль «Информационная безопасность или На расстоянии одного вируса» реализуется в рамках внеурочной деятельности обучающихся. Программа рассчитана на 34 часа, по одному часу в неделю.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОГО КУРСА

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.

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.

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. 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.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА
БЕЗОПАСНОСТЬ ОБЩЕНИЯ

Тема1.Общениевсоциальныхсетяхимессенджерах

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальныхсетейимессенджеров.Пользовательскийконтент.

Тема2.Скембезопаснообщатьсявинтернете

Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимныесоциальныесети.

Тема3.Паролидляаккаунтовсоциальныхсетей

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использованиефункциибраузерапо запоминанию паролей.

Тема4.Безопасный входваккаунты

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере сточкизрения безопасности личногоаккаунта.

Тема5.Настройкиконфиденциальностивсоциальныхсетях

Настройкиприватностиконфиденциальностивразных социальных сетях.Приватностьи конфидициальность вмесседжерах.

Тема6.Публикацияинформациивсоциальныхсетях

Персональныеданные.Публикацияличнойинформации.

Тема7.Кибербуллинг

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать?Какнестать жертвой кибербуллинга.Как помочьжертвекибербуллинга.

Тема8.Публичныеаккаунты

Настройкиприватностипубличныхстраниц.Правилаведенияпубличныхстраниц.

Тема9.Фишинг

Фишинг как мошеннический прием. Популярные варианты распространения фишинга.Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетяхимессенджерах.

Тема10.Выполнениеизащитаиндивидуальныхигрупповыхпроектов

Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи,SMART.Защитапроекта.

БЕЗОПАСНОСТЬУСТРОЙСТВ

Тема1.Чтотакоевредоносныйкод

Видывредоносныхкодов.Возможностиидеструктивныефункциивредоносныхкодов.

Тема2.Распространениевредоносногокода

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка.Вредоносныескрипты.Способывыявленияналичиявредоносныхкодовнаустройствах.Действияприобнаружениивредоносныхкодовнаустройствах.

Тема3.Методызащитыот вредоносныхпрограмм

Способы защиты устройств от вредоносного кода. Антивирусные программы и иххарактеристики. Правилазащиты отвредоносныхкодов.

Тема4.Распространениевредоносногокодадлямобильныхустройств

Расширение вредоносных кодов для мобильных устройств. Правила безопасности приустановкеприложенийнамобильные устройства.

Тема5.Выполнениеизащитаиндивидуальныхигрупповыхпроектов

Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи,SMART.Защитапроекта.

БЕЗОПАСНОСТЬИНФОРМАЦИИ

Тема1.Социальнаяинженерия:распознатьиизбежать

Приемы социальной инженерии. Правила безопасности в виртуальных контактах.

Тема2.ЛожнаяинформациявИнтернете

Фейковые новости. Поддельные страницы.

Тема3.Безопасностьприиспользованииплатежныхкарт вИнтернете

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасностьбанковскихсервисов

Тема4.Беспроводнаятехнологиясвязи

Уязвимости Wi-Fi-соединений. Публичные и непубличные сети. Правила работы впубличных сетях.

Тема5.Резервноекопированиеданных

Безопасностьличнойинформации.Созданиерезервныхкопийнаразличных устройствах.

Тема6.Выполнениеизащитаиндивидуальныхигрупповыхпроектов

Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи,SMART.Защитапроекта.

ТЕМАТИЧЕСКОЕПЛАНИРОВАНИЕ

№ п/п	Содержание	Общее количество часов	Теория	Практика
БЕЗОПАСНОСТЬОБЩЕНИЯ				
1.	Тема 1. Общение в социальных сетях и мессенджерах	2	1	1
2.	Тема2.С кем безопасно общаться в интернете	1	0,5	0,5
3.	Тема 3. Методы защиты от вредоносных программ	2	1	1
4.	Тема4.Безопасный вход в аккаунты	2	1	1
5.	Тема 5. Настройки конфиденциальности в социальных сетях	2	1	1
6.	Тема6.Публикация информации в социальных сетях	2	1	1
7.	Тема7.Кибербуллинг	1	1	
8.	Тема8.Публичные аккаунты	1	0,5	0,5
9.	Тема9.Фишинг	1	1	
10.	Тема 10. Выполнение и защита индивидуальных и групповых проектов	3	1	2
БЕЗОПАСНОСТЬИНФОРМАЦИИ				
1.	Тема1.Что такое вредоносный код	1	1	
2.	Тема2.Распространение вредоносного кода	1	1	
3.	Тема 3. Методы защиты от вредоносных программ	2	1	1
4.	Тема4.Распространение вредоносного кода для мобильных устройств	2	1	1
5.	Тема 5. Выполнение и защита индивидуальных и групповых проектов	3	1	2
БЕЗОПАСНОСТЬУСТРОЙСТВ				
1.	Тема 1. Социальная инженерия: распознать и избежать	1	1	
2.	Тема2.Ложная информация в Интернете	1	0,5	0,5
3.	Тема 3. Безопасность при использовании платежных карт в Интернете	1	0,5	0,5
4.	Тема4.Беспроводная технология связи	1	1	
5.	Тема5.Резервное копирование данных	1	0,5	0,5
6.	Тема 6. Выполнение и защита индивидуальных и групповых проектов	3	1	2
	Итого:	**34**	**18,5**	**15,5**