Муниципальное бюджетное общеобразовательное учреждение
"Глазовская средняя общеобразовательная школа"
Ленинского района Республики Крым

К ООП ООО, утвержденной приказом МБОУ Глазовская СОШ от 31.05.2021 года № 188

РАССМОТРЕНО на заседании методического объединения Руководитель ШМО _____ А.В.Яковенко (протокол от 19. 08.2022 № 1)	СОГЛАСОВАНО Заместитель директора по УВР _____А.Д. Абжелова 22. 08.2022	УТВЕРЖДЕНА приказом МБОУ Глазовская СОШ 22. 08.2022 № 282

РАБОЧАЯ ПРОГРАММА
ПО ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Направление	Общекультурное
Наименование внеурочной деятельности	Информационная безопасность или на расстоянии одного вируса
Уровень образования	Основное общее образование
Классы	6-8
Учителя	Кудрицкая Яна Александровна Полий Татьяна Александровна Гордиенко Виктория Александровна
Срок реализации	2022-2023
Количество часов в неделю	6 класс – 1 час 7 класс – 1 час 8 класс – 1 час
Количество часов в год	6 класс – 34 часа 7 класс – 34 часа 8 класс – 34 часа

2022 г.

Рабочая программа по внеурочной деятельности «Информационная безопасность или на расстоянии одного вируса» для 6 – 8 классов разработана на основе следующих документов:

- Федерального государственного образовательного стандарта основного общего образования, утвержденного приказом Министерства образования и науки Российской Федерации от 17.12.2010 №1897(с изменениями);
- Учебного пособия Наместникова М.С. «Информационная безопасность, или на расстоянии одного вируса 7-9 классы, Просвещение 2019 год»

РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

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 ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационнотелекоммуникационной среде.

Метапредметные результаты.

В результате освоения учебного курса обучающийся сможет:

- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- формулировать учебные задачи как шаги достижения поставленной цели деятельности;
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- определять критерии правильности (корректности) выполнения учебной задачи;
- соотносить реальные и планируемые результаты индивидуальной образовательной деятельности и делать выводы;
- принимать решение в учебной ситуации и нести за него ответственность.

- принимать позицию собеседника, понимая позицию другого, различать в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории;
- выделять общую точку зрения в дискуссии;
- соблюдать нормы публичной речи, регламент в монологе и дискуссии в соответствии с коммуникативной задачей;
- 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, созданиепрезентаций 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.

Предметные результаты:

Научатся:

- 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;

Получат возможность Овладеть:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п;
- основами самоконтроля, соблюдения норм информационной этики и права;
- навыками самостоятельного принятия решения и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности в сети интернет.

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ С УКАЗАНИЕМ ФОРМ ОРГАНИЗАЦИИ И ВИДОВ ДЕЯТЕЛЬНОСТИ

6 КЛАСС

БЕЗОПАСНОСТЬ ОБЩЕНИЯ (14 часов)

Вводное занятие

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

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 конфидициальность в месседжерах.

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.

Тема 9. Фишинг

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

Тема 10. Выполнение и защита индивидуальных и групповых проектов

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

БЕЗОПАСНОСТЬ УСТРОЙСТВ (8 часов)

Тема 11. Что такое вредоносный код

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 12. 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 13. Методы защиты от вредоносных программ

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

Тема 14. Распространение вредоносного кода для мобильных устройств

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Тема 15. Выполнение и защита индивидуальных и групповых проектов

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

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ (9 часов)

Тема 16. Социальная инженерия: распознать и избежать

Приемы социальной инженерии. Правила безопасности в виртуальных **контактах.**

Тема 17. Ложная информация в Интернете

Фейковые новости. Поддельные страницы.

Тема 18. Безопасность при использовании платежных карт в Интернете

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

Тема 19. Беспроводная технология связи

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

Тема 20 Резервное копирование данных

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 21 Выполнение и защита индивидуальных и групповых проектов

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

Повторение (3 часа)

Форма организации внеурочной деятельности: кружок.

7 КЛАСС

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

Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Методы защиты от вредоностных программ

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 конфидициальность в месседжерах.

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.

Тема 9. Фишинг

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

Тема 10. Выполнение и защита индивидуальных и групповых проектов

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

8 КЛАСС

Тема 1 Общение в социальных сетях и мессенджерах

Тема 2 С кем безопасно общаться в интернете

Тема 3 Пароли для аккаунтов социальных сетей

Тема 4 Безопасный вход в аккаунты

Тема 5 Настройки конфиденциальности в социальных сетях.

Тема 6 Публикация информации в социальных сетях

Тема 7 Кибербуллинг

Тема 8 Публичные аккаунты

Тема 9 Фишинг

Тема 11 Что такое вредоносный код

Тема 12 Распространение вредоносного кода

Тема 13 Методы защиты от вредоносных программ

Тема 14 Распространение вредоносного кода для мобильных устройств

Тема 15 Социальная инженерия: распознать и избежать

Тема 16 Ложная информация в интернете

Тема 17 Безопасность при использовании платёжных карт в интернете

Тема 18 Беспроводная технология связи

Тема 19 Резервное копирование данных

Курс предусматривает такие виды деятельности обучающихся на занятиях, как: эвристическая беседа, виртуальная экскурсия, интеллектуальные игры, социальная реклама, работа с видеоматериалами.

Формы проведения занятий: очная (групповые, индивидуальные занятия) и дистанционная (электронная почта, сайт, отдельные веб-страницы, чат, веб-конференции и т. п.).

Для реализации программы предлагается использование методов:

Наглядные: просмотр презентаций, рассматривание наглядного материала.

Словесные: консультирование, сообщения, рассказы детей по схемам, иллюстрациям, моделированию; разбор ситуаций.

Практический метод: проведение дидактических игр, поисковые и научные исследования; наблюдения учащихся; заочные путешествия; творческие презентации; работа с документами, СМИ, другими информационными носителями; работа с компьютером

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

Тематическое планирование рабочей программы внеурочной деятельности «Информационная безопастность или на расстоянии одного вируса» составлено с учетом рабочей программы воспитания.

6 КЛАСС

№ п/п	Наименование (раздела, темы)	Количество часов
БЕЗОПАСНОСТЬ ОБЩЕНИЯ - 14 часов		
1.	Вводное занятие	1
2	Общение в социальных сетях и мессенджерах	1
3	С кем безопасно общаться в интернете	1
4	Методы защиты от вредоносных программ	1
5	Безопасный вход в аккаунты	1
6	Настройки конфиденциальности в социальных сетях	1
7	Публикация информации в социальных сетях	1
8	Кибербуллинг	1
9	Публичные аккаунты	1
10	Фишинг	1
11	Выполнение теста. Обсуждение тем проектов.	1
12	Выполнение индивидуальных и групповых проектов по тем	3
	БЕЗОПАСНОСТЬ ИНФОРМАЦИИ (8 часов	
13	Что такое вредоносный код	1
14	Распространение вредоносного кода	1
15	Методы защиты от вредоносных программ	1
16	Распространение вредоносного кода для мобильных устройств	1
17	Выполнение теста. Обсуждение тем проектов.	1
18	Выполнение индивидуальных и групповых проектов по теме	3
	БЕЗОПАСНОСТЬ УСТРОЙСТВ	**9**
19	Социальная инженерия: распознать и избежать	1
20	Ложная информация в Интернете	1
21	Безопасность при использовании платежных карт в Интернете	1
22	Беспроводная технология связи	1
23	Резервное копирование данных	1
24	Выполнение теста. Обсуждение тем проектов.	1
25	Выполнение индивидуальных и групповых проектов по теме	3
26	Повторение	3ч

7 КЛАСС

№ п/п	Тема	Количество часов
1.	Общение в социальных сетях и мессенджерах	5
2.	С кем безопасно общаться в интернете	3
4.	Методы защиты от вредоносных программ	4
5.	Безопасный вход в аккаунты	3
6.	Настройки конфиденциальности в социальных сетях	2
7.	Публикация информации в социальных сетях	2
8	Кибербуллинг	4
9.	Публичные аккаунты	2
9	Фишинг	4
10	Выполнение и защита индивидуальных и групповых проектов	5
	Итого	**34 часа**

8 КЛАСС

№ п/п	Тема урока (раздела)	Количество часов
1	Общение в социальных сетях и мессенджерах.	2
2.	С кем безопасно общаться в интернете.	1
3.	Пароли для аккаунтов социальных сетей.	1
4.	Безопасный вход в аккаунты.	2
5	Настройки конфиденциальности в социальных сетях.	1
6	Публикация информации в социальных сетях.	3
7	Кибербуллинг	2
8	Публичные аккаунты	2
9	Фишинг	2
10	Что такое вредоносный код	2
11	Распространение вредоносного кода.	3
12.	Методы защиты от вредоносных программ	3
13	Распространение вредоносного кода для мобильных устройств.	2
14	Социальная инженерия: распознать и избежать.	2
15	Ложная информация в интернете.	2
16	Безопасность при использовании платёжных карт в интернете	1
17	Беспроводная технология связи	1
18	Резервное копирование данных	2
	Итого	34