Приложение к ООП ООО (ФГОС ООО) МБОУ "ООШ № 21",
утверждена приказом директора по учреждению
от _____ № ____
с изменениями от _____ № ___

Рабочая программа

по предмету по выбору "Информационная безопасность, или на расстоянии одного вируса"

на уровень основного общего образования

7-9 класс

ФГОС

Эгле Ксения Владимировна

учитель информатики

2020 г.

Рабочая программа к предмету по выбору «Информационная безопасность, или на расстоянии одного вируса» разработана в соответствии с требованиями к результатам освоения основной образовательной программы основного общего образования МБОУ «ООШ № 21».

Данная программа рассчитана на 102 часов. Обязательное изучение «Информационная безопасность, или на расстоянии одного вируса» по классам осуществляется в следующем объеме:

Год обучения	Количество часов	Количество учебных недель	Всего за год
7 класс	1	34	34
8 класс	1	34	34
9 класс	1	34	34
ВСЕГО:			102

Планируемые результаты

освоения обучающимися программы внеурочной деятельности

Предметные результаты:

	Информатики	ОБЖ
Выпускник научиться	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 получит возможность	Овладеть: • Приёмами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет - сервисов и т.п., • Основами соблюдения норм информационной этики и права.	Овладеть 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.

Содержание учебного предмета, курса с указанием форм организации учебных занятий, основных видов учебной деятельности.

Основное содержание по темам	Формы организации учебных предметов	Характеристика основных видов деятельности ученика (на уровне учебных действий)
Безопасность общения	Беседа Лекция Практическое занятие Контрольное занятие	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей 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 аутенфикации. 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.
Безопасность устройств	Беседа Лекция Практическое занятие Контрольное занятие	Виды вредоносных кодов. Возможности в 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.
Безопасность информации	Беседа Лекция Практическое занятие Контрольное занятие	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. Уязвимости wi-fi –

		соединений. Публичные и непубличные сети. Правила работы в публичных сетях. Безопасность личной информации. Создание резервных копий на различных устройствах.

Тематическое планирование

7 класс

№	Тема	Кол-во часов
1	«Безопасность общения»	15
2	«Безопасность устройств»	8
3	«Безопасность информации»	11
	Итого	34

8 класс

№	Тема	Кол-во часов
1	«Безопасность общения»	13
2	«Безопасность устройств»	10
3	«Безопасность информации»	11
	Итого	34

9 класс

№	Тема	Кол-во часов
1	«Безопасность общения»	13
2	«Безопасность устройств»	8
3	«Безопасность информации»	13
	Итого	34

Календарно - тематическое планирование

7 класс

№ п/п	Тема урока	Форма контроля	Количество часов	Дата	
				план	факт
Безопасность общения (13 часов)					
1	Общение в социальных сетях и мессенджерах		1		
2	С кем безопасно общаться в Интернете		1		
3-4	Пароли для аккаунтов социальных сетей		2		
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 индивидуальных и групповых проектов.		1		
12-15	Выполнение и защита индивидуальных и групповых проектов.		4		
Безопасность устройств (8 часов)					
16	Что такое вредоносный код		1		
17	Распространение вредоносного кода		1		
18	Методы защиты от вредоносных программ		1		
19	Распространение вредоносного кода для мобильных устройств		1		
20	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов		1		
21-23	Выполнение и защита индивидуальных и групповых проектов		3		
Безопасность информации (11 часов)					
24	Социальная инженерия: распознать и избежать		1		

25	Ложная информация в Интернете		1		
26	Безопасность при использовании платежных карт в Интернете		1		
27	Беспроводная технология связи		1		
28	Резервное копирование данных		1		
29-31	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов		3		
32-34	Повторение, резерв		3		

8 класс

№ п/п	Тема урока	Форма контроля	Количество часов	Дата	
				план	факт
Безопасность общения (13 часов)					
1	Общение в социальных сетях и мессенджерах		1		
2	С кем безопасно общаться в Интернете		1		
3	Пароли для аккаунтов социальных сетей		1		
4	Безопасный вход в аккаунты		1		
5	Настройки конфиденциальности в социальных сетях		1		
6	Публикация информации в социальных сетях		1		
7	Кибербуллинг		1		
8	Публичные аккаунты		1		
9	Фишинг		1		
10	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов.		1		
11-13	Выполнение и защита индивидуальных и групповых проектов.		3		
Безопасность устройств (10 часов)					
14-15	Что такое вредоносный код		2		
16	Распространение вредоносного кода		1		
17-18	Методы защиты от вредоносных программ		2		
19	Распространение вредоносного кода для мобильных устройств		1		
20	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов		1		
21-23	Выполнение и защита индивидуальных и групповых проектов		3		
Безопасность информации (11 часов)					
24	Социальная инженерия: распознать и избежать		1		
25	Ложная информация в Интернете		1		

26	Безопасность при использовании платежных карт в Интернете		1		
27	Беспроводная технология связи		1		
28	Резервное копирование данных		1		
29-31	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов		3		
32-34	Повторение, резерв		3		

9 класс

№ п/п	Тема урока	Форма контроля	Количество часов	Дата	
				план	факт
Безопасность общения (13 часов)					
1	Общение в социальных сетях и мессенджерах		1		
2	С кем безопасно общаться в Интернете		1		
3	Пароли для аккаунтов социальных сетей		1		
4	Безопасный вход в аккаунты		1		
5	Настройки конфиденциальности в социальных сетях		1		
6	Публикация информации в социальных сетях		1		
7	Кибербуллинг		1		
8	Публичные аккаунты		1		
9	Фишинг		1		
10	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов.		1		
11-13	Выполнение и защита индивидуальных и групповых проектов.		3		
Безопасность устройств (8 часов)					
14	Что такое вредоносный код		1		
15	Распространение вредоносного кода		1		
16	Методы защиты от вредоносных программ		1		
17	Распространение вредоносного кода для мобильных устройств		1		
18	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов		1		
19-21	Выполнение и защита индивидуальных и групповых проектов		3		
Безопасность информации (13 часов)					
22	Социальная инженерия: распознать и избежать		1		
23-24	Ложная информация в Интернете		2		

25	Безопасность при использовании платежных карт в Интернете		1		
26	Беспроводная технология связи		1		
27-28	Резервное копирование данных		2		
29-31	Выполнение теста. Обсуждение тем индивидуальных и групповых проектов		3		
32-34	Повторение, резерв		3		