государственное бюджетное общеобразовательное учреждение Самарской области
основная общеобразовательная школа № 17 города Новокуйбышевска городского округа
Новокуйбышевск Самарской области

446213, Самарская область, г.о. Новокуйбышевск, ул. Киевская д. 15, тел. 8(84635)44181

Принято	«Проверено»	«Утверждаю»
на заседании	Зам. директора по ВР	Директор ГБОУ ООШ № 17
Педагогического совета		_____ А. С. Чевелёв
Протокол № 1		Приказ №138-ОД
от «31» августа 2020г.	Подледнова О.В.Подледнова	от «31» августа 2020 г.

Рабочая программа курса внеурочной деятельности

«Информационная безопасность»

9 класс

(социальное направление)

Составитель:

Георгиева Е.А.

2020-2021 учебный год

Результаты освоения курса внеурочной деятельности:

Предметные:

- анализировать доменные имена компьютеров и адреса документов в интернете;
- использовать безопасно средства коммуникации,
- применять способы самозащиты при попытке мошенничества,
- безопасно использовать ресурсы интернета.

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.
- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет – сервисов;

Метапредметные:

- 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;
- 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.
- 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 курса внеурочной деятельности

9 класс

№	Разделы	Кол-во часов
1	Безопасность общения	8
2	Безопасность устройства	3
3	Безопасность информации	6
Всего		**17**

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час.
Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.
Тема 2. С кем безопасно общаться в интернете. 1 час.
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. Безопасный вход в аккаунты 1 час.
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.
Тема 4. Настройки конфиденциальности в социальных сетях. 1 час.
Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.
Тема 5. Публикация информации в социальных сетях. 1 час.
Персональные данные. Публикация личной информации.
Тема 6. Кибербуллинг. 1 час.
Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.
Тема 7. Публичные аккаунты. 1 час.
Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.
Тема 8. Фишинг. 1 час
Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. Распространение вредоносного кода.1 час.
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.
Тема 2. Методы защиты от вредоносных программ. 1 час.
Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.
Тема 3. Распространение вредоносного кода для мобильных устройств. 1 час.
Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час. 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. 1 час.
Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.
Тема 4. Беспроводная технология связи. Резервное копирование данных. 1 час.
Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях. Безопасность личной информации. Создание резервных копий на различных устройствах.
Тема 5. Основы государственной политики в области формирования культуры информационной безопасности. 1 час.
Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Формы проведения занятий:

- Работа в парах
- Индивидуальная работа
- Самостоятельная работа
- Групповые занятия под руководством учителя (обучение в сотрудничестве)
- Проектная работа (индивидуальная / групповая)
- Тесты

Тематическое планирование 9 класс

№	Название темы	Количество часов		
		Всего	Теория	Практика
Раздел 1. Безопасность общения		**8**	**4**	**4**
1	Общение в социальных сетях и мессенджерах	**1**	0,5	0,5

2	С кем безопасно общаться в интернете	**1**	0,5	0,5
3	Пароли для аккаунтов социальных сетей. Безопасный вход в аккаунты	**1**	0,5	0,5
4	Настройки конфиденциальности в социальных сетях	**1**	0,5	0,5
5	Публикация информации в социальных сетях	**1**	0,5	0,5
6	Кибербуллинг	**1**	0,5	0,5
7	Публичные аккаунты	**1**	0,5	0,5
8	Фишинг	**1**	0,5	0,5
Раздел 2. Безопасность устройств		**3**	**1,5**	**1,5**
9	Что такое вредоносный код. Распространение вредоносного кода	**1**	0,5	0,5
10	Методы защиты от вредоносных программ	**1**	0,5	0,5
11	Распространение вредоносного кода для мобильных устройств	**1**	0,5	0,5
Раздел 3. Безопасность информации		**6**	**3**	**3**
12	Социальная инженерия: распознать и избежать	**1**	0,5	0,5
13	Ложная информация в Интернете	**1**	0,5	0,5
14	Безопасность при использовании платежных карт в Интернете	**1**	0,5	0,5
15	Беспроводная технология связи. Резервное копирование данных	**1**	0,5	0,5
16	Основы государственной политики в области формирования культуры информационной безопасности	**1**	1	
17	Повторение пройденного материала. Проектная работа.	**1**		1
Всего		**17**	**8,5**	**8,5**