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)57271

Принято на заседании Педагогического совета Протокол № 1 от « 30 » августа 2023 г.	«Проверено» Зам. директора по ВР _____ О.В.Подледнова	«Утверждаю» Директор ГБОУ ООШ № 17 _____ А. С. Чевелёв Приказ № 148 - ОД от « 30» августа 2023 г.

ЭП

C=RU, O=ГБОУ ООШ № 17 г.Новокуйбышевск, CN=Чевелёв Алексей Сергеевич, E=so_sch17_nkb@samara.edu.ru
00fdf8c39a6e5b1ee7
2023-08-30 18:00:21

Рабочая программа курса внеурочной деятельности

«Информационная безопасность»

9 класс

(внеурочная деятельность по обеспечению жизни и здоровья обучающихся)

Составитель:
Георгиева Е.А.

Планируемые результаты освоения курса внеурочной деятельности:

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.

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.

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;

Содержание курса внеурочной деятельности

№	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. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чу-жом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.
Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах
Тема 6. Публикация информации в социальных сетях. 1 час.
Персональные данные. Публикация личной информации.
Тема 7. Кибербуллинг. 1 час.
Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.
Тема 8. Публичные аккаунты. 1 час.
Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.
Тема 9. 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.
Тема 10. Выполнение и защита индивидуальных и групповых проектов. 3 часа

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. Распространение вредоносного кода.1 час.
Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.
Тема 2. Распространение вредоносного кода. 1 час.
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 3. Методы защиты от вредоносных программ. 2 часа.
Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.
Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.
Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.
Тема 5. Выполнение и защита индивидуальных и групповых проектов. 3 часа

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. 1 час.

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

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. 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.

Тема 7. Выполнение и защита индивидуальных и групповых проектов. 3 часа

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		**13**	**5**	**8**
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.	**1**	0,5	0,5
4	Безопасный вход в аккаунты	**1**	0,5	0,5
5	Настройки конфиденциальности в социальных сетях	**1**	0,5	0,5
6	Публикация информации в социальных сетях	**1**	0,5	0,5
7	Кибербуллинг	**1**	0,5	0,5
8	Публичные аккаунты	**1**	0,5	0,5
9	Фишинг	**2**	1	1
10	Выполнение и защита индивидуальных и групповых проектов	**3**		3
Раздел 2. Безопасность устройств		**8**	**2,5**	**5,5**
11	Что такое вредоносный код.	**1**	0,5	0,5
12	Распространение вредоносного кода	**1**	0,5	0,5

10	Методы защиты от вредоносных программ	**2**	1	1
11	Распространение вредоносного кода для мобильных устройств	**1**	0,5	0,5
12	Выполнение и защита индивидуальных и групповых проектов	**3**		3
Раздел 3. Безопасность информации		**13**	**3,5**	**9,5**
13	Социальная инженерия: распознать и избежать	**1**	0,5	0,5
14	Ложная информация в Интернете	**1**	0,5	0,5
15	Безопасность при использовании платежных карт в Интернете	**1**	0,5	0,5
16	Беспроводная технология связи.	**1**	0,5	0,5
17	Резервное копирование данных	**1**	0,5	0,5
18	Основы государственной политики в области формирования культуры информационной безопасности	**2**	1	1
19	Выполнение и защита индивидуальных и групповых проектов	**3**		3
20	Повторение изученного материала.	**2**		2
21	Зачет	**1**		1
Всего		**34**	**11**	**23**