Муниципальное бюджетное общеобразовательное учреждение
городского округа Тольятти
«Школа с углубленным изучение отдельных предметов №45»

Утверждено
Директор МБУ «Школа № 45» Е.Н.Ошкина
(Приказ от «01» 09. 2022 г. №151/10-ОД)

Принято
Протокол педагогического совета
№ 12 от 31.08.2022 г.

O="МБУ ""Школа №. 45""",
CN="Е.Н. Ошкина, директор
", E=school45@edu.tgl.ru
0096f255233a6dbbf9
2022.10.02 22:05:02+04'00'

РАБОЧАЯ ПРОГРАММА
ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«Цифровая гигиена»
модуль «Информационная безопасность»

8 класс

Составитель:
учитель информатики
Калашина Алла Александровна

2022

Пояснительная записка

Рабочая программа по курсу внеурочной деятельности «Информационная безопасность» разработана на основании нормативных документов:

1. Федеральный закон РФ «Об образовании в Российской Федерации» от 29 декабря 2012 г. N 273-ФЗ;
2. Письмо Минобрнауки России от 18.08.2017 No 09-1672 «О направлении Методических рекомендаций по уточнению понятия и содержания внеурочной деятельности в рамках реализации основных общеобразовательных программ, в том числе в части проектной деятельности»;
3. Письмо Министерства образования и науки Самарской области от 17.02.2016 No МО-16-09-01/173-ту «О внеурочной деятельности»
4. Основная образовательная программа основного общего образования МБУ «Школа № 45»

Место курса внеурочной деятельности в плане внеурочной деятельности.

На изучение курса «Информационная безопасность» 34 часа, 8 классы по 34 часа.

1. Планируемые результаты курса

Программа внеурочной деятельности «Информационная безопасность» ориентирована на достижение обучающимися комплекса следующих личностных, метапредметных и предметных результатов:

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.

В результате освоения учебного курса 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

В результате освоения учебного курса 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.

В результате освоения учебного курса 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.

. 2. Содержание курса «Информационная безопасность»

«Безопасность общения» - 13 часов

Общение в социальных сетях и мессенджерах.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

С кем безопасно общаться в интернете.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Пароли для аккаунтов социальных сетей.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Безопасный вход в аккаунты.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Настройки конфиденциальности в социальных сетях.

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Публикация информации в социальных сетях.

Персональные данные. Публикация личной информации.

Кибербуллинг.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Публичные аккаунты.

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Фишинг.

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

Выполнение и защита индивидуальных и групповых проектов.

«Безопасность устройств»

Что такое вредоносный код.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

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.

Методы защиты от вредоносных программ.

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

Распространение вредоносного кода для мобильных устройств.

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

Выполнение и защита индивидуальных и групповых проектов.

«Безопасность информации»

Социальная инженерия: распознать и избежать.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Ложная информация в Интернете.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Безопасность при использовании платежных карт в Интернете.

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

Беспроводная технология связи.

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

Резервное копирование данных.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Основы государственной политики в области формирования культуры информационной безопасности.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение и защита индивидуальных и групповых проектов.

Повторение.

3. Тематическое планирование курса «Информационная безопасность»

№	Тема	Кол/ч
I	**Безопасность общения**	**13**
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	2
10	Выполнение и защита индивидуальных и групповых проектов	3
II	**Безопасность устройств**	**8**
11	Что такое вредоносный код	1
12	Распространение вредоносного кода	1
13	Методы защиты от вредоносных программ	2

14	Распространение вредоносного когда для мобильных устройств	1
15	Выполнение и защита индивидуальных и групповых проектов	3
III	**Безопасность информации**	**13**
16	Социальная инженерия: распознать и избежать	1
17	Ложная информация в Интернете	1
18	Безопасность при использовании платежных карт в Интернете	1
19	Беспроводная технология связи	1
20	Резервное копирование данных	1
21	Основы государственной политики в области формирования культуры информационной безопасности	2
22	Выполнение и защита индивидуальных и групповых проектов	3
23	Повторение	3
	Итого	**34**