государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа №11
им. Героя Советского Союза Аипова Махмута Ильячевича
городского округа Октябрьск Самарской области

Рассмотрена	**Проверена**	**Утверждена**
на заседании методического объединения учителей Протокол № 1 от «29» августа 2024 г.	Заместитель директора по УВР _____Л.С. Райник «30» августа 2024 г.	Приказом № 541 от «30» августа 2024г. Директор школы _____ О.А. Дунова

DN: O=ГБОУ СОШ №11 г.о. Октябрьск, CN=Дунова Ольга Анатольевна, E=zu_school11_okt@63edu.ru
Дата: 2024.08.30 15:57:27+04'00'

РАБОЧАЯ ПРОГРАММА
КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«Цифровая гигиена»

Нормативной базой для разработки рабочей программы «Информационная безопасность. Цифровая гигиена» по внеурочной деятельности является:

1. Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;
2. Примерная рабочая программа учебного курса «Цифровая гигиена». Основное общее образование.- Самара, 2019. Рекомендована Координационным советом учебно – методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019);
3. Основная образовательная программа основного общего образования ГБОУ СОШ № 11 г. о. Октябрьск;
4. План внеурочной деятельности ГБОУ СОШ № 11 г. о. Октябрьск.

«Цифровая гигиена» изучается в основной школе в 7/8/9 классе (в соответствии с учебным планом школы). Общее количество часов 34.

Результаты освоения курса «Цифровая гигиена»

Личностные результаты:

- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.; - сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;

-сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интерне-том. Характеристика личностных, метапредметных и предметных результатов освоения учебного курс

Предметные результаты:

-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 результаты:

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.

Содержание курса
«Цифровая гигиена»

1. Безопасность общения.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. Персональные данные как основной капитал личного пространства в цифровом мире.

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 аутентификации. 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. Овершеринг.

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.

2. Безопасность устройств.

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.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.

3. Безопасность информации.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

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

новости. Поддельные страницы.

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

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

Безопасность личной информации. Создание резервных копий на различных устройствах.

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

Формы организации и виды деятельности: работа с Интернет- ресурсами, презентации, проекты.

Тематическое планирование

№ урок а	**Наименование раздела, темы**	**Количество часов на изучение**
1.	**«Безопасность общения» - (13)**	
1.1	Общение в социальных сетях и мессенджерах	1
1.2	С кем безопасно общаться в интернете	1
1.3	Пароли для аккаунтов социальных сетей	1
1.4	Безопасный вход в аккаунты	1
1.5	Настройкиконфиденциальности в социальных сетях	1
1.6	Публикация информации в социальных сетях	1
1.7	Кибербуллинг	1
1.8	Публичные аккаунты	1
1.9 1.10	Фишинг	2
1.11 1.12 1.13	Выполнение и защита Индивидуальных проектов групповых проектов	2

2.	**«Безопасность устройств» - (8)**	
2.1	Что такое вредоносный код	1
2.2	Распространение вредоносного кода	1
2.3 2.4	Методы защиты от вредоносных программ	2
2.5	Распространение вредоносного кода для мобильных устройств	1
2.6 2.7 2.8	Выполнение и защита индивидуальных и групповых проектов	3
3.	**«Безопасность информации» - (14)**	
3.1	Социальная инженерия: распознать и избежать	1
3.2	Ложная информация в Интернете	1
3.3	Безопасность при использовании платежных карт в Интернете	1
3.4	Беспроводная технология связи	1
3.5	Резервное копирование данных	1
3.6 3.7	Основы государственной политики в области формирования культуры информационной безопасности	2
3.8 3.9 3.10	Выполнение и защита индивидуальных и групповых проектов	3
3.11 3.12 3.13	Повторение, волонтерская практика, резерв	4