

Муниципальное бюджетное общеобразовательное учреждение
«Шеметовская средняя общеобразовательная школа»
Сергиево-Посадский городской округ
Московская область

УТВЕРЖДАЮ:
Директор МБОУ «Шеметовская средняя
общеобразовательная школа» Л.В. Иванова
«30 августа» 2023



Рабочая программа внеурочной деятельности
кружка «Безопасный и полезный интернет»
интеллектуальные марафоны
9-е классы

2023 год

Данная рабочая программа кружка «Безопасный и полезный Интернет» для 9 класса соответствует требованиям федерального государственного образовательного стандарта основного общего образования и разработана на основе:

- основной образовательной программы основного общего образования МБОУ «Шеметовская средняя общеобразовательная школа»;
- учебного плана МБОУ «Шеметовская средняя общеобразовательная школа» на 2023-2024 учебный год;
- авторской программы Тонких И.М., Комарова М.М., Ледовского В.И., Михайлова А.В. «Основы кибербезопасности» для общеобразовательных организаций, переработана и модифицирована.

Программа рассчитана на 34 часа (1 час в неделю).
Авторская программа реализуется в полном объеме.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Предметные:

1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;
2. Сформированы умения соблюдать нормы информационной этики;
3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

Метапредметные:

1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий;
2. Развиваются умения анализировать и систематизировать имеющуюся информацию;
3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.

Личностные:

1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;
2. Формируются и развиваются нравственные, этические, патриотические качества личности;
3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Модуль 1. Общие сведения о безопасности ПК и Интернета

Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности.

Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации.

Что такое защищенная информационная среда. Защита каналов передачи данных, средства предотвращения утечки информации, защита информации от НСД (антивирусная защита, средства контроля защищенности, средства обнаружения и предупреждения атак), средства аутентификации.

Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления.

Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).

Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi.

Угрозы информации (техногенные, случайные и преднамеренные; природные). Неосторожность пользователя как одна из угроз для информационной безопасности.

Меры кибербезопасности для конечных пользователей. Использование рекомендованных версий операционных систем и приложений, использование антивирусных средств, настройка веб-браузеров, блокировка скриптов, использование фильтров фишинга, межсетевых экранов. Автоматическое обновление ПО.

Модуль 2. Техника безопасности и экология

Кибератаки на инфраструктуру.

Компьютер в режиме труда и отдыха. Информационная перегрузка.

Влияние компьютера на репродуктивную систему.

Модуль 3. Проблемы Интернет-зависимости

Интернет- и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость.

Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости).

Модуль 4. Методы обеспечения безопасности ПК и Интернета.

Вирусы и антивирусы

Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты.

Проверка подлинности (аутентификация) в Интернете.

Меры безопасности для пользователя WiFi. Настройка безопасности.

Вирусы для мобильных устройств (мобильные банкиры и др.).

Настройка компьютера для безопасной работы.

Ошибки пользователя (установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.).

Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления

Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы.

Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.

Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды.

Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег.

Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса.

Платные предложения работы. Платный просмотр видеоматериалов.

Технологии манипулирования в Интернете.

Модуль 6. Сетевой этикет. Психология и сеть

Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Сетевой этикет. Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др.

Модуль 7. Правовые аспекты защиты киберпространства

Как расследуются преступления в сети.

Ответственность за интернет-мошенничество.

Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

Модуль 8. Государственная политика в области кибербезопасности

Доктрина информационной безопасности

Формы организации внеурочной деятельности:

- познавательная беседа;
- изучение терминов;
- интерактивная игра;
- проектная деятельность;
- лекции.


Основные виды внеурочной деятельности:

- ответы на вопросы;
- разгадывание ребусов;
- разгадывание кроссвордов;
- защита проекта;
- тестирование.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Наименование темы, занятия	Количество часов, отводимых на освоение темы
1	Вводное занятие	1
2	Общие сведения о безопасности ПК и Интернета	10
3	Техника безопасности и экология	3
4	Проблемы Интернет-зависимости	2
5	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	6
6	Мошеннические действия в Интернете. Киберпреступления	7
7	Сетевой этикет. Психология и сеть	1
8	Правовые аспекты защиты киберпространства	3
9	Государственная политика в области кибербезопасности	1
	ИТОГО	34

СОГЛАСОВАНО
на заседании ШМО
начальных классов
Протокол № 1
от «30» августа 2023 г.

СОГЛАСОВАНО
Заместитель директора по ВР

_____ О.В.Исмайлова
«30» августа 2023 г.