х. Второй Киевский Кашарского района Ростовской области

Муниципальное бюджетное общеобразовательное учреждение

Киевская средняя общеобразовательная школа

|  |  |
| --- | --- |
|  | «Утверждаю» Директор школы Тимонов Ю.А.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_  Приказ № 50 от 29.08.2024 |

**РАБОЧАЯ ПРОГРАММА**

**курса внеурочной деятельности**

**«Информационная безопасность»**

**Класс**: 6

**Уровень образования**: основное общее образование

**Срок реализации программы:** 2024-2025 г.

**Количество часов по учебному плану**:

всего – 34 1ч/неделю

**Планирование составлено на основе:** примерной авторской программы Основы кибербезопасности» для общеобразовательных организаций авторов Тонких И.М., Комарова М.М., Ледовского В.И., Михайлова А.В

Рабочую программу составила: учитель информатики Кравченко Ольга Сергеевна

​

**х.Второй Киевский‌** **2024-2025 учебный год‌**​

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Данная рабочая программа для 6 класса соответствует требованиям федерального государственного образовательного стандарта основного общего образования и разработана на основе:

- основной образовательной программы основного общего образования МБОУ «Киевской СОШ»;

- учебного плана МБОУ «Киевской СОШ» на 2024-2025 учебный год;

- курса «Основы кибербезопасности» для общеобразовательных организаций авторов Тонких И.М., Комарова М.М., Ледовского В.И., Михайлова А.В., переработана и модифицирована.

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

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ 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 ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

**Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов).**

Как работают мобильные устройства. Угрозы для мобильных устройств.

Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).

Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).

Кто обеспечивает защиту киберпространства.

Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.

**Модуль 2. Техника безопасности и экология (5 часов).**

Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.

Компьютеры и мобильные устройства в экстремальных условиях.

Везде ли есть Интернет. ТБ при работе с мобильными устройствами.

Первая помощь при проблемах в интернете (службы помощи).

Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).

**Модуль 3. Проблемы Интернет-зависимости (2 часа).**

Виды Интернет-зависимости.

Компьютер и зрение.

**Модуль 4. Методы обеспечения безопасности ПК и Интернета.**

**Вирусы и антивирусы (8 часов).**

Вирусы и антивирусы.

Как распространяются вирусы.

Источники и причины заражения.

Скорая компьютерная помощь. Признаки заражения компьютера.

Что такое антивирусная защита. Как лечить компьютер.

Защита мобильных устройств.

Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.

Защита файлов. Что такое право доступа.

Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.

**Модуль 5. Мошеннические действия в Интернете. Киберпреступления (2 часа).**

Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.

Прослушивание разговоров. Определение местоположения телефона.

**Модуль 6. Сетевой этикет. Психология и сеть (9 часов).**

Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.

«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.

Анонимность в сети.

Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.

Как появился нетикет, что это такое. Общие правила сетевого этикета.

Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).

Этика дискуссий. Взаимное уважение при интернет-общении.

Этикет и безопасность. Эмоции в сети, их выражение.

Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.

Если вы стали жертвой компьютерной агрессии: службы помощи.

**Модуль 7. Правовые аспекты защиты киберпространства (2 часа).**

Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.

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

**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;

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Наименование темы, занятия | Кол. ч | Дата |
| 1 | Вводное занятие | 1 | 02.09 |
| 2 | Виды защиты киберпространства | 1 | 10.09 |
| 3 | Как работают мобильные устройства. Угрозы для мобильных устройств | 1 | 17.09 |
| 4 | Распространение вредоносных файлов через приложения для смартфонов и планшетов | 1 | 24.09 |
| 5 | Что такое геоинформационные системы | 1 | 01.10 |
| 6 | Компьютеры и мобильные устройства в экстремальных условиях | 1 | 08.10 |
| 7 | ТБ при работе с мобильными устройствами | 1 | 15.10 |
| 8 | Первая помощь при проблемах в интернете | 1 | 22.10 |
| 9 | Компьютер и зрение | 1 | 12.11 |
| 10 | Воздействие радиоволн на здоровье и окружающую среду | 1 | 19.11 |
| 11 | Виды Интернет-зависимости | 2 | 26.11  03.12 |
| 12 | Как распространяются вирусы | 1 | 10.12 |
| 13 | Источники и причины заражения | 1 | 17.12 |
| 14 | Признаки заражения компьютера | 1 | 24.12 |
| 15 | Что такое антивирусная защита | 1 | 14.01 |
| 16 | Защита мобильных устройств | 1 | 21.01 |
| 17 | Как защитить данные от потерь. Копирование и восстановление | 1 | 28.01 |
| 18 | Защита файлов | 1 | 04.02 |
| 19 | Защита детей в социальных сетях. ПО для родителей | 1 | 11.02 |
| 20 | Опасности мобильной связи.  Мошеннические СМС | 1 | 18.02 |
| 21 | Прослушивание разговоров. Определение местоположения телефона | 1 | 25.02 |
| 22 | Что такое личные данные | 1 | 04.03 |
| 23 | Анонимность в сети | 1 | 11.03 |
| 24 | Что такое этикет. Виды этикета | 1 | 18.03 |
| 25 | Общие правила сетевого этикета | 1 | 01.04 |
| 26 | Личное общение и общение в группе | 1 | 08.04 |
| 27 | Этика дискуссий | 1 | 15.04 |
| 28 | Этикет и безопасность | 1 | 22.04 |
| 39 | Реальная и виртуальная личность | 1 | 29.04 |
| 30 | Психологическая обстановка в Интернете | 1 | 06.05 |
| 31 | Собственность в Интернете. Авторское право | 1 | 13.05 |
| 32 | Интеллектуальная собственность. Платная и бесплатная информация | 1 | 20.05 |
|  | Итого: 32 часа |  |  |