Приложение к ООП ООО

**ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ**

**«Информационная безопасность»**

**Срок реализации 1 год**

**7 класс**

1. **Результаты освоения курса внеурочной деятельности «Информационная безопасность»**

***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.

***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 получениязапланированных 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 достоверностиинформации;

• 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 иобосновывать его.

• целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач спомощью средств ИКТ;

• выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных иформальных 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.

1. **Содержание курса внеурочной деятельности с указанием форм организации и видов деятельности**

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств»», «Безопасность информации».

Система учебных заданий, предложенная в учебном курсе, позволяет создать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им, и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз.

Система заданий предполагает индивидуальную и групповую формы работы, составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы. Предлагаемые задания направлены на формирование критичного мышления школьников, формирование умений решать проблемы, работать в команде, высказывать и защищать собственную позицию, приобретение основ безопасной работы с информацией в виртуальном мире. В учебном пособии предложены следующие виды заданий: задания для подготовки устного ответа; задания, выполняемые с помощью интернета; задания, выполняемые на заранее учителем подготовленных листах.

Для проведения занятий могут быть использованы презентации, проекты, памятки, подготовленные в ходе выполнения заданий по темам пособия. Программа учебного курса рассчитана на 34 учебных часа, из них 27 часов - учебных занятий, 3 часа - проверка знаний, 4 часа - подготовка и защита учебных проектов.

Содержание программы:

**Раздел 1. «Безопасность общения»**

*Тема 1. Общение в социальных сетях и мессенджерах.*

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

*Тема 2. 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.

*Тема 3. Пароли для аккаунтов социальных сетей.*

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

*Тема 4. Безопасный вход в аккаунты.*

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

*Тема 5. Настройки конфиденциальности в социальных сетях.*

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

*Тема 6. Публикация информации в социальных сетях.*

Персональные данные. Публикация личной информации.

*Тема 7. Кибербуллинг.*

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

*Тема 8. Публичные аккаунты. 1 час*

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

*Тема 9. Фишинг.*

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

**Раздел 2. «Безопасность устройств»**

*Тема 1. Что такое вредоносный код.*

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

*Тема 2. 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.

*Тема 3. Методы защиты от вредоносных программ.*

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

*Тема 4. Распространение вредоносного кода для мобильных устройств*

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

**Раздел 3 «Безопасность информации»**

*Тема 1. Социальная инженерия: распознать и избежать.*

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

*Тема 2. Ложная информация в Интернете.*

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

Фейковые новости. Поддельные страницы.

*Тема 3. Безопасность при использовании платежных карт в Интернете.*

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

*Тема 4. Беспроводная технология связи.*

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

*Тема 5. Резервное копирование данных.*

Безопасность личной информации. Создание резервных копий на различных устройствах.

*Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.*

1. **Тематическое планирование**

|  |  |  |
| --- | --- | --- |
| **№** | **Темы** | **Кол-во часов** |
| **Раздел 1. «Безопасность общения» (13 ч.)** | | |
|  | Общение в социальных сетях и мессенджерах | 1 |
|  | С кем безопасно общаться в Интернете | 1 |
|  | Пароли для аккаунтов социальных сетей | 1 |
|  | Безопасный вход в аккаунты | 1 |
|  | Настройки конфиденциаль ности в социальных сетях | 1 |
|  | Публикация информации в социальных сетях | 1 |
|  | Кибербуллинг | 1 |
|  | Публичные аккаунты | 1 |
|  | Фишинг | 2 |
|  | Выполнение и защита индивидуальных и групповых проектов | 3 |
| **Раздел 2. «Безопасность устройств» (8 ч.)** | | |
|  | Что такое вредоносный код? | 1 |
|  | Распространение вредоносно го кода | 1 |
|  | Методы защиты от вредоносных программ | 2 |
|  | Распространение вредоносного кода для мобильных устройств | 1 |
|  | Выполнение и защита индивидуальных и групповых проектов | 3 |
| **Раздел 3 «Безопасность информации» (13 ч.)** | | |
|  | Социальная инженерия: распознать и избежать | 1 |
|  | Ложная информация в Интернете | 1 |
|  | Безопасность при использовании платежных карт в Интернете | 1 |
|  | Беспроводная технология связи | 1 |
|  | Резервное копирование данных | 1 |
|  | Основы государственной политики в области информирования культуры информационной безопасности | 2 |
|  | Выполнение и защита индивидуальных и групповых проектов | 3 |
|  | Повторение, волонтерская практика, резерв | 3 |
|  | Итого | 34 |