Государственное казенное общеобразовательное учреждение Ростовской области
«Николаевская специальная школа - интернат»

Рассмотрено и рекомендовано
на заседании педсовета
Протокол №1
«26» августа 2024г.

Утверждаю: _____
Директор А.А. Острянская
Приказ № 176
«26» августа 2024г.

Подписано
цифровой подписью:
Острянская Анна
Алексеевна
Дата: 2024.12.11
12:22:20 +03'00'

Программа технологического кружка «Информационная безопасность»

Составитель: учитель высшей квалификационной категории Белов Иван Викторович

Пояснительная записка

Рабочая программа составлена на основе следующих нормативных документов и методических рекомендаций:
1. Федеральный закон от 29 декабря 2012 г. N 273-ФЗ "Об образовании в Российской Федерации" с дополнениями и изменениями, в том числе статья 79 ФЗ;
2. Концепция развития дополнительного образования детей до 2030 года (утверждена распоряжением Правительства Российской Федерации от 31 марта 2022 г. №678-р).
3. Федеральный государственный образовательный стандарт начального общего образования и на основе основной образовательной программы начального общего образования «Информационная безопасность».

Основными целями изучения курса «Информационная безопасность» являются:
• обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;

Задачи программы:
1. сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
2. 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;
3. 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.;
4. 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;
5. сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Общая характеристика учебного курса

Курс внеурочной деятельности «Информационная безопасность» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.
Программа учебного курса рассчитана на 34 учебных часа. На изучение курса внеурочной деятельности «Информационная безопасность» отводится по 1 часу в неделю в 8-11 классах. Оценочный вид деятельности

Личностные, метапредметные и предметные результаты освоения учебного курса

Предметные:

Обучающийся 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.
Обучающийся овладеет:
• приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
Обучающийся 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:
• 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
• 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;

• 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.;

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;

Содержание программы
Содержание разделов учебной дисциплины «Информационная безопасность»

№ п.п.	Наименование разделов дисциплины	Содержание разделов
	5-7 класс	
1	**Правила безопасной работы в сети Интернет с мобильным телефоном.** **Угрозы в сети Интернет и мобильных сетях связи**	Угрозы в мобильных сетях связи. Угрозы из СМС сообщений. Угрозы от незнакомых лиц. Ложные сообщения и просьбы. Проблемы хулиганства по телефону. Правила безопасной работы с мобильным телефоном. Телефоны экстренных служб. Выход в Интернет, беспроводную сеть. Защита устройства мобильной связи от входа, код входа
2	**Правила безопасной работы в сети Интернет с планшетом или на компьютере**	Правила безопасной работы в сети Интернет с планшетом или на компьютере при получении и передаче информации. Электронная почта. Спам. Вредоносные программы. Личные данные и правила их защиты. Защита входа в устройство. Пароль и логин. Регистрация на сайтах. Личные данные.
3	**Сеть Интернет**	Поиск информации в сети Интернет. Позитивный Интернет. Сайты для учебы, досуга, творчества, чтения книг, виртуальных путешествий.
4	**Правила безопасной работы в социальной сети.**	Правила безопасной работы в социальной сети. Этикет общения. Социальные сети. Детские социальные сети. Аватар и его выбор. ≪Друзья≫ в сети. Опасности общения в социальной сети с виртуальными ≪друзьями≫. Этикет общения. Реакция на негативные сообщения, угрозы, агрессию, уговоры и опасные предложения. Отключение от нежелательных контактов. Поддержка семьи для устранения проблем общения детей в социальных сетях

8-11 класс		
1.	**«Безопасность общения»**	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 бербуллинга. 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.
2	**«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.
3	**«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 знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности

Содержание учебного предмета, курса:

№ п/п	Наименование разделов, тем дисциплины	Количество часов		
		Всего	**Теория**	**Лабораторно практические**
5-8 класс				
1	**Правила безопасной работы в сети Интернет с мобильным телефоном.** **Угрозы в сети Интернет и мобильных сетях связи**	**9**	**5**	**4**

2	**Правила безопасной работы в сети Интернет с планшетом или на компьютере**	**10**	**6**	**4**
3	**Сеть Интернет**	**3**	**2**	**1**
4	**Правила безопасной работы в социальной сети.**	**12**	**8**	**4**
	Итого	**34**	**21**	**13**
8-11 класс				
1	**«Безопасность общения»**	**19**	**16**	**3**
2	**«Безопасность устройств»**	**7**	**5**	**2**
3	**«Безопасность информации»**	**8**	**6**	**2**
	Итого	**34**	**27**	**7**