

Бюджетное общеобразовательное учреждение
«Русскополянская гимназия №1»
Русско-Полянского муниципального района Омской области
Центр образования цифрового и гуманитарного профилей «Точка роста»

Рассмотрено
на педагогическом совете
Протокол №1
от «30» августа 2024 г.

«Утверждаю»
Директор
БОУ «Русскополянская гимназия №1»:
О.И. Ключко
Приказ №74 от «30» августа 2024 г.



**ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ
(ОБЩЕРАЗВИВАЮЩАЯ) ПРОГРАММА
«Безопасность в сети интернет»**

Направленность: техническая

Форма освоения: очная

Уровни сложности содержания: базовый

Целевая группа – обучающиеся 8-17 лет

Общий объем - 72 часа

Автор-составитель:

Бейсембаев Ильяс Александрович,
педагог дополнительного образования



Русская Поляна, 2024

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная (общеразвивающая) программа «Интернет безопасность» имеет информационную направленность, гуманитарный профиль.

Целевая группа: обучающиеся 8-17 лет, 3 группы в количестве 10-15 человек.

Форма обучения: очная, сетевая

Срок реализации: 2024 – 2025 учебный год.

Общее количество часов - 72 часа.

Периодичность занятий каждой группы – 1 раз в неделю, по 2 часа.

Актуальность программы:

Исследование проблемы безопасности детей и подростков в сети Интернет последние годы является особенно актуальным, в связи с бурным развитием IT-технологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь).

Цель программы:

Освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства.

Задачи обучения:

1. Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;
2. Развивать умение анализировать и систематизировать имеющуюся информацию;
3. Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;

Планируемые результаты:

Личностные:

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

Метапредметные:

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

Результаты по профилю программы:

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

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Тема	Всего часов	Теоретические занятия	Практические занятия
1.	Информация, компьютер и Интернет.	14	8	6
2.	Техника безопасности и экология	10	6	4
3.	Мир виртуальный и реальный. Интернет зависимость.	10	6	4
4.	Методы безопасной работы в Интернете	11	6	5
5.	Потребительские опасности в Интернете	10	6	4
6.	Основные правила поведения сетевого взаимодействия	11	8	3
7.	Государственная политика в области в области защиты информации	6	4	2
8.	Итого	72	44	25

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема № 1. - 14 ч.

Информация, компьютер и Интернет.

1. Основные вопросы: Компьютер - как он появился, как появился Интернет. Почему компьютер нужно беречь. Где и как искать информацию для урока. Интернет - средство для поиска полезной информации. Как защитить себя от информационной перегрузки. Что такое файл. Как обращаться со своими и чужими файлами, чтобы их не потерять. Какие файлы можно скачивать, а какие нельзя. Полезные и вредные страницы Интернета. Как отличать полезную и правдивую информацию. Ненужные ссылки, ложные ссылки, реклама. Что такое вредоносные сайты. К чему ведет переход по вредоносным ссылкам. Опасная информация в сети. Возьми с собой электронного помощника. Мобильные устройства. Польза и опасности мобильной связи, Общение в Интернете - переписка, форумы, социальные сети. Совместные игры в Интернете. Обмен данными при совместной работе - скайп, IP-телефония, ICQ. Безопасный обмен данными. На каких устройствах можно сохранить информацию и как с ними правильно обращаться (диски, флэш, карты и пр.). Как работать в группе. Как передать товарищам результаты работы и не повредить их компьютерам. Что такое электронная почта.

2. Требования к знаниям и умениям:

Обучающиеся должны знать об истории появления компьютера и Интернета. Правила работы с компьютером. Научиться соблюдать правила работы с файлами. Уметь отличать безопасные сайты и ссылки от вредоносных. Знать технические и программные возможности мобильных устройств. Преимущества мобильной связи и их опасность. Понимать пользу и опасности виртуального общения, социальных сетей.

Обучающиеся должны уметь правильно работать за компьютером. Пользоваться браузером для поиска полезной информации. Внимательно прочитывать сообщения о нежелательных страницах, отказываться от их просмотра, выполнять основные действия с файлами. Копировать файлы, проверять файлы на вирусы. Уметь работать с информацией и электронной почтой. Владеть основными приемами поиска информации в сети Интернет.

3. Тематика практических работ:

Практическая работа №1. Поиск информации в сети Интернет.

Практическая работа №2. Работа с мобильными устройствами (2 ГИС, Госуслуги, Википедия, эл.книги, фотоколлаж, Компас, диктофон, Калькулятор и пр.).
2 часа

Практическая работа №3. Общение с использованием видеосвязи на примере Skype. 2 часа

Практическая работа 4. Создание электронной почты

Тема № 2 . - 1 0 ч.

Техника безопасности и экология

1. Основные вопросы: Гигиена при работе с компьютером. Правила работы с ПК, электронными книгами и мобильными устройствами. Сколько времени можно проводить за компьютером. Как правильно сидеть за компьютером. Как защитить компьютер от повреждений, Компьютеру тоже нужна забота, Компьютер и среда обитания (растения, животные, другие члены семьи). Везде ли есть Интернет? Может ли компьютер заменить компас. Как мобильные устройства помогают ориентироваться на местности. Воздействие компьютера на зрение и др. органы. Физическое и психическое здоровье. Польза и вред компьютерных игр. Компьютер и недостаток движения. Что делать с компьютером в чрезвычайных ситуациях. Улица и мобильные устройства. Компьютер (мобильные устройства) в грозу.

2. Требования к знаниям и умениям: Обучающиеся должны знать основные правила работы с ПК, электронными книгами и мобильными устройствами в условиях окружающей среды, основные навыки ухода за ПК, опасности при работе с электрическими приборами.

Обучающиеся должны уметь соблюдать технику безопасности и гигиену при работе за ПК. Владеть основными приемами навигации в файловой системе.

3. Тематика практических работ:

Практическая работа №1. Использование мобильного приложения Компас (2 часа).

Практическая работа №2. Создание буклетов по темам:

- «Как может помочь компьютер в сложных чрезвычайных ситуациях»
- «Правила поведения на улице с мобильными устройствами»
- «Компьютеру тоже нужна забота» (как ухаживать за ПК и мобильными устройствами) 2 часа

Тема № 3 . - 1 0 ч.

Мир виртуальный и реальный. Интернет зависимость.

1. Основные вопросы: Что такое Интернет-сообщество. Как не превратить свою жизнь в виртуальную? Социальные сети. Детские социальные сети. Какую информацию о себе следует выкладывать в сеть? Какая информация принадлежит вам? Не слишком ли много у вас друзей в социальной сети? Если слишком долго находиться в Интернете: что такое интернет-зависимость? Виртуальная личность - что это такое. Сайты знакомств. Незнакомцы в Интернете. Превращение виртуальных знакомых в реальных. Развлечения в Интернете. Игры полезные и вредные. Признаки игровой зависимости.

2. Требования к знаниям и умениям:

Обучающиеся должны знать виды общения в Интернете. Правила безопасной работы при интернет - общении.

Обучающиеся должны уметь пользоваться основными видами программ для общения в сети. Чего не следует делать при сетевом общении.

Уметь применять программу Skype для общения, создание контактов.

Отличать вредные игры от полезных.

3. Тематика практических работ:

Практическая работа №1. Создание сообщества класса в детских социальных сетях (2 часа)

Практическая работа №2. Тест «Есть у меня игровая зависимость». Квест «Я умею говорить «Нет» в сети Интернет» (2 часа)

Тема № 4 . 1 1 ч.

Методы безопасной работы в Интернете.

1. Основные вопросы: Ищите в Интернете только то, что вам требуется. Как защититься от вредного контента. Что такое контент-фильтры, движение в Интернете (серфинг). Знаки Интернета, рассказывающие об опасной информации. Правильно ли работает компьютер? Признаки работы вирусов. Вирусы и антивирусы. Обновление баз. Что такое электронные деньги, как с ними правильно обращаться. Почему родители проверяют, что ты делаешь в Интернете?

2. Требования к знаниям и умениям:

Обучающиеся должны знать основные понятия о компьютерных вирусах и контент-фильтрах.

Обучающиеся должны уметь использовать приемы работы с антивирусными программами, запускать программы-антивируса для сканирования компьютера и внешних носителей информации, устанавливать и сканировать антивирусной программой. Детские контент-фильтры.

3. Тематика практических работ:

Исследовательская работа №1 «Колобанга в поисках вируса» (выявление признаков заражения вирусом)- 5 часов.

Тема № 5 . 1 0 ч.

Потребительские опасности в Интернете

1. Основные вопросы:

Интернет и экономика - польза и опасность. Кто и как может навредить в Интернете. Электронная торговля - ее опасности. Поиск информации: если у вас требуют личную информацию при скачивании данных. Что такое личная информация. Если вам сообщают о выигрыше в лотерею. Если вам предлагают установить новое приложение. Сколько стоят ошибки в интернете.

2. Требования к знаниям и умениям:

Обучающиеся должны знать принципы работы интернет - магазинов, понятие «электронные деньги». Обучающиеся должны уметь дозированно использовать личную информацию в сети интернет.

Уметь различать (распознавать) мошеннические действия.

3. Тематика практических работ:

Практическая работа №1. Прохождение интерактивного курса. «Мошеннические действия в Интернете. Киберпреступления» 2 часа

Практическая работа №2. Квест «Покупка в интернет-магазине» 2 часа

Тема № 6. 1 1 ч.

Основные правила поведения сетевого взаимодействия.

1. Основные вопросы: Что такое интернет-этикет. Как вести себя в гостях у «сетевых» друзей.

2. Требования к знаниям и умениям:

Обучающиеся должны знать правила сетевого этикета.

Обучающиеся должны уметь корректно общаться в сети Интернет.

3. Тематика практических работ:

Практическая работа №1. «Пишу письмо другу» 2 часа

Практическая работа №2. «Пишу письмо семье»

Тема №7. 6 ч.

Государственная политика в области защиты информации.

1. Основные вопросы: Как государство защищает киберпространство. Войны нашего времени. Что такое кибервойна. Почему государство защищает информацию. Защита государства и защита киберпространства.

2. Требования к знаниям и умениям:

Обучающиеся должны знать политику государство в области защиты информации.

Обучающиеся должны уметь защищать свои информационные данные от внешнего воздействия (интернет и вирусы, вирусы и злоумышленники).

3. Тематика практических работ:

Практическая работа №1 Квест «Война миров» 2 часа

Контрольно – оценочные средства

Оценка уровня образовательных результатов дополнительной общеобразовательной (общеразвивающей) программы «Интернет Безопасность»

Виды контроля	Период	Объект контроля	Форма контроля	Диагностический инструментарий
<i>Входящий</i>	начало освоения программы	уровень образовательных результатов	<ul style="list-style-type: none"> • тестирование 	<ul style="list-style-type: none"> • тест «Общие понятия Безопасности»
<i>Текущий</i>	после освоения каждой темы	личностные результаты	<ul style="list-style-type: none"> • педагогическое наблюдение; • опрос; • тестирование; • взаимооценка; • самооценка 	<ul style="list-style-type: none"> • карта наблюдения (<i>личностных, метапредметных результатов</i>) • тесты • оценочные листы
		метапредметные результаты		
		результаты по профилю программы		
<i>Итоговый</i>	по итогам освоения программы	уровень образовательных результатов	<ul style="list-style-type: none"> • тестирование 	<ul style="list-style-type: none"> • тест «ИБ в обычной жизни»

Условия реализации программы

Материально-техническое обеспечение	<ul style="list-style-type: none"> • ПАК «Цифровая образовательная среда» • Точка доступа в Интернет (100 М/б) • Комплект ПК – 10 шт • Демонстрационная доска • Бумага офисная
Информационно-образовательные ресурсы	<ul style="list-style-type: none"> • Сборник видеолекций, задач и практик, 2018 • Сборник видеороликов Безопасность в интернете, 2020
Учебно-методическое обеспечение	<ul style="list-style-type: none"> • Онлайн программа для начинающих; • Методическое пособие "Безопасный Интернет"
Кадровое обеспечение	<p>Педагог дополнительного образования, реализующий дополнительную общеобразовательную программу «Интернет безопасность», имеет среднее специальное образование, по специальности техник информационных систем.</p> <p>Прошел обучение в ФГАУ «Фонд новых форм развития образования» по курсу «Гибкие компетенции в проектной деятельности»</p>

Список литературы

1. Бирюков А. А. Информационная безопасность защита и нападение 2е издание: Издательство: ДМК-Пресс., 2017, 434 с.
2. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2012, 474 с.
3. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с.
4. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с.
5. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасностьсетей: Издательство: М.: НОУ "Интуит", 2016,571 с.
6. Платонов В.В. Программноаппаратные средства защиты информации: учебник для студ. Учрежд.высш. проф. образования / В. В.Платонов. — М.: Издательский центр «Академия», 2013,336 с.
7. Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2014, 192 с.
8. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2012, 100 с.
9. Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с.