Муниципальное бюджетное общеобразовательное учреждение
«Карпогорская средняя школа № 118»

РАССМОТРЕНО

на педагогическом совете

протокол №1 от 30.08.2024

УТВЕРЖДАЮ
Директор МБОУ «Карпогорская СШ №118»
_____ Рашева Т.Ф.
приказ ОО от 30.08.2024 №01-271-О.Д

Дополнительная общеобразовательная
общеразвивающая программа

«Интернет безОпасности»

(техническая направленность)

Возраст обучающихся: 10-15 лет
Срок реализации: 1 год

Составитель:
Дроботова Юлия Сергеевна,
педагог дополнительного образования

с. Карпогоры
2024 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная общеразвивающая программа «Интернет безОпасности» разработана в соответствии с требованиями Федерального государственного образовательного стандарта основного общего образования на основе учебного пособия Наместникова М.С. «Информационная безопасность, или на расстоянии одного вируса 7-9 классы Просвещение 2019 год».

Программа реализуется в рамках технической направленности развития личности.

Занятия по программе проводятся на базе центра образования цифрового и гуманитарного профилей «Точка роста». Программа может быть реализована с применением электронного обучения и дистанционных образовательных технологий. Программа может быть реализована по принципу сетевого партнерства.

Актуальность:

Согласно российскому законодательству, информационная безопасность детей – это состояние защищённости детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 «436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет. Знания об Интернет - угрозах, умения различать и предотвращать их последствия, защитить от них себя и своих близких – способствуют социализации детей.

Проблема безопасного интернета становится всё более актуальной проблемой, так как год от года возрастает количество киберпреступлений. Неслучайно, что в соответствии с решением парламентского слушания Совета Федерации от 12 марта 2014 года было принято решение о проведении во всех школах Российской Федерации 30 октября Единого урока по безопасности в сети и квест по цифровой грамотности среди детей и подростков «Сетевичок».

Одной из важных тенденций развития отрасли информационных технологий в настоящее время становится многократное повышение значимости обеспечения информационной безопасности. Одной из основных целей развития отрасли информационных технологий, которую ставит перед собой Правительство Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года в рамках «Стратегии развития отрасли информационных технологий в РФ на 2014-2020 годы и на перспективу до 2025 года», является обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Исходя из этого реализация ДООП «Интернет безОпасности» направлена на формирование основ личной информационной безопасности обучающихся, информационной безопасности своей семьи и своих друзей.

Цель программы - обеспечение условий для профилактики негативных тенденций в информационной культуре обучающихся, повышения защищенности детей от информационных рисков и угроз. **Задачи программы:**

Образовательные:

- способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;
- формировать умения соблюдать нормы информационной этики;

• формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию.

• *Развивающие:*

• развивать компьютерную грамотность и информационную культуру личности в использовании информационных и коммуникационных технологий;

• развивать умение анализировать и систематизировать имеющуюся информацию;

• развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий.

Воспитательные:

• способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;

• стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.

Отличительной особенностью данной программы от существующих является использование в образовательном процессе следующих образовательных технологий:

- проблемное обучение – создание под руководством педагога проблемных ситуаций и активная самостоятельная деятельность по их разрешению; - технология использования в обучении игровых методов;

- обучение в сотрудничестве (командная, групповая работа).

Принципы построения программы:

- принцип концентрической последовательности занятий по классам от простого к сложному;

- принцип единства сознания и деятельности нацеливает на формирование у школьников глубокого понимания, устойчивого интереса, осмысленного отношения к безопасности;

- принцип наглядности предполагает максимальное использование мультимедиа продуктов при проведении занятий;

- принцип личностной ориентации. Опираясь на индивидуальные особенности учащихся, педагог планирует и прогнозирует развитие каждого ребёнка;

-принцип системности;

-принцип практической направленности проявляется во взаимосвязи знаний, умений и навыков.

Уровень сложности освоения программы – базовый.

Характеристика обучающихся по программе: программа ориентирована на обучающихся 5-9 классов, возраст детей 10-15 лет. Количество детей в группе – 12-25 человек.

Для обучения по программе специальных требований к уровню подготовленности обучающихся не предъявляется. Группы формируются из детей, которые проявляют интерес к техническому творчеству, их психологические и физические особенности соответствуют возрасту.

Объем и срок реализации программы: программа рассчитана на один год обучения, 34 часа в год, 1 час в неделю, периодичность занятий – 1 раз в неделю. Реализация программы возможна отдельными разделами (модулями).

Формы и режим занятий: занятия проводятся в теоретической и практической форме:

• теоретические занятия: основы безопасного поведения при работе с компьютерными программами, информацией в сети интернет, изучение терминов, беседы, лекции;

• практические занятия: работа с мобильными устройствами, персональными компьютерами; создание буклетов и мультимедийных презентаций.

В данной программе используется групповая форма организации деятельности обучающихся на занятии.

Формы организации деятельности: групповая, парная, индивидуальная.

Основные методы обучения:

1. Устный.
2. Проблемный.
3. Частично-поисковый.
4. Формирование и совершенствование умений и навыков (изучение нового материала, практика).
5. Обобщение и систематизация знаний (самостоятельная работа, творческая работа, дискуссия).
6. Контроль и проверка умений и навыков (самостоятельная работа).
7. Создание ситуаций творческого поиска.

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

Содержание программного материала этих тем, как в теории, так и на практических занятиях составлено с учётом возрастных особенностей обучающихся, весь материал построен по принципу от простого к сложному.

Занятия проводятся по следующему плану:

1. Организационный момент. Поверка готовности к занятию, создание психологического настроя.
2. Актуализация знаний (проверка изученного материала) по необходимости.
3. Теоретическая часть. Ознакомление с новым материалом.
4. Практическая работа. Закрепление нового материала, способов действий.
5. Итог занятия. Подведение результатов работы, выводы, оценивание, рефлексия.

Система заданий предполагает индивидуальную и групповую формы работы, составление памяток, анализ 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.

Каждый раздел программы завершается выполнением проектной работы по изученному материалу.

Ожидаемые результаты освоения программы

Предметные:

• 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.

• *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.

• *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.

• **Способы проверки результатов:**

• устный опрос;

• наблюдение,

• практическое задание,

• просмотр работ.

Формы контроля и подведения итогов:

Для оценки эффективности занятий используются следующие показатели:

– степень помощи, которую оказывает учитель обучающимся при выполнении заданий: чем помощь учителя меньше, тем выше самостоятельность учеников и, следовательно, выше развивающий эффект занятий;

– поведение обучающихся на занятиях: живость, активность, заинтересованность школьников обеспечивают положительные результаты занятий;

– косвенным показателем эффективности данных занятий может быть повышение успеваемости по разным школьным дисциплинам, а также наблюдения учителей за работой обучающихся на других уроках (повышение активности, работоспособности, внимательности, улучшение мыслительной деятельности).

Формами подведения итогов программы могут быть:

- выставки буклетов, выполненных обучающимися;
- проведение квестов;
- выступления обучающихся по актуальным вопросам информационной безопасности с собственными мультимедийными презентациями на ученических мероприятиях; - демонстрация созданных видеороликов и др.

Оценка качества предоставления образовательных услуг по данной программе соответствует системе оценки качества представления образовательных услуг, принятой в МБОУ «Карпогорская СШ № 118» (Приложение № 1).

Учебный план

№ п/п	Название раздела (модуля)	количество часов		
		всего	теория	практика
1	Безопасность общения	14	7	7
2	Безопасность устройств	8	4	4
3	Безопасность информации	12	4	8
	Итого:	34	15	19

Содержание программы

Раздел 1 (модуль 1): Безопасность общения

Тема 1-2. Общение в социальных сетях и мессенджерах

Теоретический материал: Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Практическая работа: Настраиваем профиль в социальных сетях

Тема 3-4. Безопасный вход в аккаунты

Теоретический материал: Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Практическая работа: Безопасный вход в аккаунты

Тема 5-6. Настройки конфиденциальности и публикация информации в социальных сетях

Теоретический материал: Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфидициальность в месседжерах. Персональные данные. Публикация личной информации.

Практическая работа: Настройки конфиденциальности и публикация информации в социальных сетях

Тема 7-8. Кибербуллинг

Теоретический материал: Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. **Тема 9-10. Фишинг**

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

Практическая работа: Отличие настоящих и фишинговых сайтов

Тема 11-14. Проект «Безопасность общения»

Практическая работа: Выполнение мини-проекта по безопасности в социальных сетях и мессенджерах.

Раздел 2 (модуль 2): Безопасность устройств

Тема 1-2. Что такое вредоносный код. Распространение вредоносного кода

Теоретический материал: Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов. 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.

Практическая работа: Обнаружение вредоносных кодов на устройствах

Тема 3-4. Методы защиты от вредоносных программ

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

Практическая работа: Установка антивирусной программы и активация защиты **Тема 5-6. Распространение вредоносного кода для мобильных устройств**

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

Практическая работа: Установка антивирусной программы и активация защиты

Тема 7-8. Проект «Безопасность устройств»

Практическая работа: Выполнение мини-проекта по безопасности персональных компьютеров и/или мобильных устройств.

Раздел 3 (модуль 3): Безопасность информации

Тема 1-2. Социальная инженерия: распознать и избежать

Теоретический материал: Приемы социальной инженерии. Правила безопасности в виртуальных контактах.

Практическая работа: Безопасность в Интернете

Тема 3-4. Ложная информация в Интернете

Теоретический материал: Фейковые новости. Поддельные страницы.

Практическая работа: Поиск ложной информации

Тема 5-6. Безопасность при использовании платежных карт в Интернете

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

Практическая работа: Тестирование по использованию платежных карт

Тема 7-8. Беспроводная технология связи

Теоретический материал: Уязвимости Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Практическая работа: Настройка Wi-Fi-соединений

Тема 9-10. Резервное копирование данных

Теоретический материал: Безопасность личной информации. Создание резервных копий на различных устройствах.

Практическая работа: Резервное копирование данных

Тема 11-12. Выполнение и защита индивидуальных и групповых проектов Практическая работа: Выполнение мини-проекта по безопасности информации.

Календарный учебный график

№ п/п	Дата	тема занятия	форма занятия	колво часов	место проведения	форма контроля
Раздел 1 (модуль 1) «Безопасность общения»						
1		Общение в социальных сетях и мессенджерах	беседа	1	учебный кабинет	педагогическое наблюдение
2		Общение в социальных сетях и мессенджерах	практикум	1	учебный кабинет	практическое задание
3		Безопасный вход в аккаунты	беседа	1	учебный кабинет	педагогическое наблюдение
4		Безопасный вход в аккаунты	практикум	1	учебный кабинет	практическое задание
5		Настройки конфиденциальности и публикация информации в социальных сетях	беседа	1	учебный кабинет	устный опрос
6		Настройки конфиденциальности и публикация информации в социальных сетях	практикум	1	учебный кабинет	практическое задание
7		Кибербуллинг	лекция	1	учебный кабинет	педагогическое наблюдение
8		Кибербуллинг	практикум	1	учебный кабинет	анализ ошибок и успехов
9		Фишинг	лекция	1	учебный кабинет	устный опрос
10		Фишинг	практикум	1	учебный кабинет	практическое задание
11		Проект «Безопасность общения»	проектная деятельность	1	учебный кабинет	выполнение проекта
12		Проект «Безопасность общения»	проектная деятельность	1	учебный кабинет	выполнение проекта
13		Проект «Безопасность общения»	проектная деятельность	1	учебный кабинет	выполнение проекта

14		Проект «Безопасность общения»	проектная деятельность	1	учебный кабинет	презентация проекта
Раздел 2 (модуль 2) «Безопасность устройств»						
15		Что такое вредоносный код. Распространение вредоносного кода	беседа	1	учебный кабинет	устный опрос
16		Что такое вредоносный код. Распространение вредоносного кода	практикум	1	учебный кабинет	практическое задание
17		Методы защиты от вредоносных программ	беседа	1	учебный кабинет	педагогическое наблюдение
18		Методы защиты от вредоносных программ	практикум	1	учебный кабинет	анализ ошибок и успехов
19		Распространение вредоносного кода для мобильных устройств	беседа	1	учебный кабинет	педагогическое наблюдение
20		Распространение вредоносного кода для мобильных устройств	практикум	1	учебный кабинет	практическое занятие
21		Проект «Безопасность устройств»	проектная деятельность	1	учебный кабинет	выполнение проекта
22		Проект «Безопасность устройств»	проектная деятельность	1	учебный кабинет	презентация проекта
Раздел 3 (модуль 3) «Безопасность информации»						
23		Социальная инженерия: распознать и избежать	беседа	1	учебный кабинет	педагогическое наблюдение
24		Социальная инженерия: распознать и избежать	практикум	1	учебный кабинет	тестирование
25		Ложная информация в Интернете	беседа	1	учебный кабинет	педагогическое наблюдение

26		Ложная информация в Интернете	практикум	1	учебный кабинет	практическое занятие
27		Безопасность при использовании платежных карт в Интернете	беседа	1	учебный кабинет	педагогическое наблюдение
28		Безопасность при использовании платежных карт в Интернете	практикум	1	учебный кабинет	тестирование
29		Беспроводная технология связи	беседа	1	учебный кабинет	педагогическое наблюдение
30		Беспроводная технология связи	практикум	1	учебный кабинет	практическое занятие
31		Резервное копирование данных	беседа	1	учебный кабинет	педагогическое наблюдение
32		Резервное копирование данных	практикум	1	учебный кабинет	практическое занятие
33		Проект «Безопасность информации»	проектная деятельность	1	учебный кабинет	выполнение проекта
34		Проект «Безопасность информации»	проектная деятельность	1	учебный кабинет	презентация проекта

Условия реализации программы

Технические средства обучения:

- мультимедийный проектор и демонстрационный экран или интерактивная панель;
- компьютер с выходом в Интернет;
- планшеты или смартфоны с выходом в Интернет; - магнитная доска. **Кадровое обеспечение:**

Программу реализует педагог, имеющий высшее образование или среднее профессиональное образование в рамках укрупненных групп направлений подготовки высшего образования и специальностей среднего профессионального образования «Образование и педагогические науки». **Методическое обеспечение программы:**

Методическое оснащение: методическая литература, материалы Интернет-сайтов, вспомогательные материалы.

Дидактический материал: плакаты, презентации, видеоролики.

В ходе реализации программы возможно использование различных методов и приёмов организации занятий:

- поисковые;
- объяснительно-иллюстративные;
- репродуктивные;

- проблемного изложения;
- эвристические (частично-поисковые);
- исследовательские;

Все эти методы направлены на стимулирование познавательного интереса обучающихся и формирование творческих учений и навыков. Программа кружковой деятельности основывается на принципах доступности, системности, коллективности, проектности, диалогичности.

Принцип доступности осуществляется путём такого распределения материала в течение учебного года и всего курса в целом, что школьники закрепляют и углубляют знания по информационной безопасности, знакомятся с научными знаниями с учётом психофизических и возрастных особенностей.

Принцип системности предусматривает изучение материала и построение всего курса от простого к сложному.

Принцип диалогичности предполагает, что духовно-ценностная ориентация детей и их развитие осуществляются в процессе такого взаимодействия педагога и обучающихся, содержанием которого являются обмен эстетическими ценностями, опытом. Диалогичность требует искренности и взаимного понимания, признания и принятия.

Принцип коллективности предполагает воспитание и образование школьника в детско-взрослых коллективах, даёт опыт жизни в обществе, опыт взаимодействия с окружающими.

Принцип проектности предусматривает последовательную ориентацию всей деятельности педагога на подготовку школьника к проектной деятельности, развёртываемой в логике замысел – реализация – рефлексия. При работе над проектом появляется возможность формирования у школьников компетентности разрешения проблем, а также освоение способов деятельности, составляющих коммуникативную и информационную компетентности.

Основное содержание программы представлено разделами (модулями) «Безопасность общения», «Безопасность устройств», «Безопасность информации». Возможно изучение отдельных разделов (модулей).

Система практических заданий позволяет создать условия для формирования активной позиции школьника в получении знаний и умений выявлять информационную угрозу, определять степень её опасности, предвидеть последствия информационной угрозы и противостоять им, и профилактике негативных тенденций в развитии информационной культуры обучающихся, повышения защищенности детей от информационных рисков и угроз.

Система заданий предполагает индивидуальную и групповую формы работы, составление памяток, анализ 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.

Каждый раздел программы завершается выполнением проектной работы по изученному материалу.

Список информационных ресурсов

Нормативно-локальные акты:

1. Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. №2471-р».
2. Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
3. Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27.07.2006 №152 «О персональных данных» с последними изменениями, внесенными Федеральным законом от 29.07.2017 N 223-ФЗ.

Для педагогов и родителей:

1. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агентства «Яхтсмен», 2012.
2. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2014.
3. Интернет для детей начального школьного возраста/А. Навернюк// Игра и дети. – 2013.-№2.С.30-31.
4. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. – М.: МГУЛ, 2013. – 212 с.
5. Методические рекомендации по информационной безопасности несовершеннолетних. В помощь педагогам и родителям: материалы мероприятий Единого урока по безопасности в сети «Интернет» (30 октября 2017 года): сб. лучших практик педагогов Иркутской области по информационной безопасности в сети «Интернет» / под ред. С.В. Кирдянкиной. – Иркутск: Издво ГАУ ДПО ИРО, 2017.
6. Риски и угрозы в Интернете для детей и подростков//Основы безопасности жизнедеятельности. – 2014 - № 1 –С. 41-46: 2 фот. (Информационная безопасность).

Интернет-ресурсы:

1. http://единыйурок.дети
2. http://сетевичок.рф/
3. http://bezopasnost-detej.ru/
4. http://detionline.com
5. http://igra-internet.ru/game
6. https://infourok.ru
7. http://podrostok.edu.yar.ru/
8. http://www.ligainternet.ru/

Приложение №

1 Протокол итоговой аттестации __учебный год

Наименование образовательной программы_____Год обучения _____

Группа _____

ФИО педагога ДО_____ Дата проведения _____

Форма аттестации _____

№ п/п	ФИО обучающегося	**Теоретическая подготовка**		**Практическая подготовка**		**Достижения** (победители и призеры) 1б.- гор., обл.уровень; 2б.- всерос. уровень; 3б.- междунар. уровень	Итоговый результат в баллах (среднее значение)
		Соответствие теоретических знаний программным требованиям	Осмысленность и правильность использования специальной терминологии	Соответствие практических умений и навыков программным требованиям	Отсутствие затруднений в использовании специального оборудования и оснащения		

Примечания: уровень оцениваемых результатов: низкий (минимальный) - 1 балл, средний - 2 балла, высокий (максимальный) - 3 балла.

Присутствовало обучающихся____чел..

Отсутствовало обучающихся_____чел.

Всего обучающихся, полностью освоивших образовательную программу по завершению её реализации:

на высоком уровне_____чел.,
на среднем уровне_____чел.,
на низком уровне_____чел.

Педагог /_____/

Члены аттестационной комиссии:_____/_____
_____/_____
_____/_____