

Муниципальное общеобразовательное учреждение

«Средняя школа № 26»

Принята на заседании
Педагогического совета
« 07 » июня 2023 г.
Протокол № 10

УТВЕРЖДАЮ:
Директор _____
« 07 » июня 2023 г.



Дополнительная общеобразовательная общеразвивающая программа

естественнонаучной направленности

Безопасность в сети Интернет

Возраст обучающихся: 7 – 11 лет

Срок реализации: 3 месяца

Автор-составитель:
Калина Е.А., ПДО

г. Ярославль, 2023 г.

Содержание

№ раздела	Разделы
1	Пояснительная записка
	Цели и задачи программы
	Особенности организации образовательного процесса
2	Учебно-тематический план
3	Содержание образовательной программы
4	Обеспечение образовательной программы
5	Оценка эффективности программы
6	Список используемой литературы

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная общеразвивающая программа «Безопасность в сети Интернет» (далее программа) составлена в соответствии со следующими нормативно-правовыми документами:

- Федеральный закон от 29.12.12 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Министерства образования и науки Российской Федерации (Минобрнауки России) от 09 ноября 2018 г. № 196 г. Москва «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Концепция развития дополнительного образования детей до 2030 года и плана мероприятий по ее реализации (Распоряжение Правительства РФ от 31 марта 2022 г. N 678-р);
- Стратегия развития воспитания в Российской Федерации на период до 2025 года, утвержденной распоряжением Правительства от 29.05.2015 № 996-р;
- Санитарные правила СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организации воспитания и обучения, отдыха и оздоровления молодежи», утвержденные 28.09.2020 (Постановление № 28 Главного государственного санитарного врача РФ);
- Приказ департамента образования Ярославской области от 07.08.2018 № 19-нп «Об утверждении Правил персонифицированного финансирования дополнительного образования детей в Ярославской области»
- Устав ОО

Направленность дополнительной общеобразовательной программы - естественнонаучная.

Исследование проблемы безопасности детей 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).

Рабочая программа «Безопасность в сети Интернет» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей при организации урочной и внеурочной деятельности.

Новизна рабочей программы «Безопасность в сети Интернет» заключена в достижении метапредметных результатов и предметных умений дисциплины «Информатика» по формированию навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в сети интернет, умений соблюдать нормы информационной этики и права.

Цель программы: освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства.

Задачи обучения

Образовательные:

1. Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;

2. Формировать умения соблюдать нормы информационной этики;
3. Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию.

Развивающие:

1. Развивать компьютерную грамотность информационную культуру личности в использовании информационных и коммуникационных технологий;
2. Развивать умение анализировать и систематизировать имеющуюся информацию;
3. Развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий;

Воспитательные:

1. Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;
2. Способствовать формированию и развитию нравственных, этических, патриотических качеств личности.
3. Стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.

Данная рабочая программа рассчитана для обучающихся 1-4 классов . Объем - 12 часов.

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

Планируемые результаты:

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. Выбатывается 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.

Формы проведения занятий:

Формы организации деятельности: групповая, индивидуальная, индивидуально - групповая (3-5 человек). Занятия проводятся в комбинированной, 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; создание буклетов и мультимедийных презентаций.

Способы определения планируемых результатов - педагогическое наблюдение, тесты, педагогический анализ результатов анкетирования, тестирования, зачётов, взаимозачётов, опросов, выполнения обучающимися диагностических заданий, участия в мероприятиях, защиты проектов, решения задач поискового характера, активности обучающихся на занятиях и т.п. Для отслеживания результативности можно использовать: педагогический мониторинг, включающий контрольные задания и тесты, диагностику личностного роста и продвижения, анкетирование, педагогические отзывы, ведение журнала учета или педагогического дневника, ведение оценочной системы; мониторинг образовательной деятельности детей, включающий самооценку обучающегося, ведение зачетных книжек, ведение творческого дневника обучающегося, оформление листов индивидуального образовательного маршрута, оформление фотоотчета и т.д.

Формами подведения итогов программы «Безопасность в сети Интернет» 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.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

(начальное общее образование)

№ п/п	Тема	Всего часов	Теоретические Занятия	Практические занятия
1.	Информация, компьютер и Интернет.	3	1	2
2.	Техника безопасности и экология	2	1	1
3.	Мир виртуальный и реальный. Интернет зависимость.	2	1	1
4.	Методы безопасной работы в Интернете	3	1	2
5	Потребительские опасности в Интернете	1	1	1
6.	Итого	12	5	7

СОДЕРЖАНИЕ ПРОГРАММЫ

1-4 классы

Тема № 1.

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. Общение с использованием видеосвязи на примере Skype.

Тема № 2.

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.

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. 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)

Практическая работа №2 «Создание презентации «Компьютер и здоровье человека»

Тема № 3.

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.

Практическая работа №2. Онлайн тест «Есть у меня игровая зависимость». - <https://a-panov.ru/online-test-na-zavisimost/>

Тема № 4.

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:

Практическая работа №1. Поиск вирусов (выявление признаков заражения вирусом).

Тема № 5.

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. Квест «Покупка в интернет-магазине».

Тест. Безопасность в сети Интернет. Приложение 1.

Календарно- тематическое планирование занятий на 2022-2023 учебный год

№ п/п	Тема	Планируемая дата проведения	Фактическая дата проведения	Примечание
	Тема № 1. Информация, компьютер и Интернет.			
1	Что такое компьютер? Глобальная информационная система сети «Интернет».			
2	Практическая работа № 1. Поиск информации в сети Интернет.			
3	Практическая работа №2. Обмен данными при совместной работе- скайп.			
	Тема № 2. Техника безопасности и экология			

4	Правила работы на компьютере и техника безопасности. Практическая работа №1 Создание буклетов по темам.			
5	Вред компьютера здоровью человека. Польза и вред компьютерных игр. Практическая работа №2 «Создание презентации «Компьютер и здоровье человека»			
	Тема № 3. Мир виртуальный и реальный. Интернет зависимость			
6	Что такое интернет сообщества. Социальные сети. Этика общения. Практическая работа №1. Создание сообщества класса в детских социальных сетях.			
7	Что такое интернет зависимость? Признаки игровой зависимости. Практическая работа №2 Онлайн тест «Есть у меня игровая зависимость». - https://a-panov.ru/online-test-na-zavisimost/			
	Тема № 4. Методы безопасной работы в сети Интернете.			
8	Правила поиска информации. Фильтры.			
9	Вирусы и антивирусы. Практическая работа №1. Поиск вирусов (выявление признаков заражения вирусом).			
10	Электронные деньги. Родительский контроль.			
	Тема № 5. Потребительские опасности в Интернете			
11	Польза и опасность интернет. Правила правильного скачивания информации. Тест. Безопасность в сети Интернет. Приложение 1.			
12	Практическая работа №1. Квест «Покупка в интернет-магазине».			

СПИСОК ЛИТЕРАТУРЫ

Основная литература:

1. Бирюков А.А. Информационная безопасность защита и нападение 2. 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.45
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. Программно-аппаратные 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 - Издательство: Наука и Техника, 2015, 320 с.

Дополнительная:

1. Методическое пособие для работников системы общего образования Солдатов Г., Зотова Е., Лебешева М., Шляпников В. «Интернет: возможности, компетенции, безопасность», 2015 - 156с.
2. Сорокина Е.В., Третьяк Т.М. Здоровье и безопасность детей в мире компьютерных технологий и Интернет. [Текст] Учебно-методический комплект. - М.: СОЛОНПРЕСС, 2010. - 176 с.: ил
3. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. – Феникс, 2008.

Интернет ресурсы

1. <http://www.kaspersky.ru> – антивирус «Лаборатория Касперского»;
2. <http://www.onlandia.org.ua/rus/> - безопасная web-зона;
3. <http://www.interneshka.net> – международный онлайн-конкурс по безопасному использованию Интернета;
4. http://nto.immpu.sgu.ru/sites/default/files/3/_12697.pdf; Рыжков В.Н. Методика преподавания информатики
5. <http://www.saferinternet.ru> – портал Российского Оргкомитета по безопасному использованию Интернета;46
6. <http://content-filtering.ru> – Интернет СМИ «Ваш личный Интернет»;
7. <http://www.rgdb.ru> – Российская государственная детская библиотека
8. <http://www.saferinternet.ru/> - Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;

9. <http://www.saferunet.ru/> - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействием им в отношении пользователей;
10. <http://www.fid.su/> - Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета;
11. <http://www.microsoft.com/Rus/athome/security/kids/etusivu.html>-
12. Безопасность в Интернете. <http://www.ifap.ru>
13. <https://ligainternet.ru/metodicheskie-materialy/> Лига безопасного Интернета материалы для проведения уроков безопасного интернета в школах.

Тест по безопасности в сети Интернет
(начальное общее образование)

1. Как могут распространяться компьютерные вирусы?
 - a. Посредством электронной почты.
 - b. При просмотре веб-страниц.
 - c. Через клавиатуру.
 - d. Их распространяют только преступники.
2. Зачем нужен брандмауэр?
 - a. Он не дает незнакомцам проникать в компьютер и просматривать файлы.
 - b. Он защищает компьютер от вирусов.
 - c. Он обеспечивает защиту секретных документов.
 - d. Он защищает компьютер от пожара.
3. Всегда ли можно быть уверенным в том, что электронное письмо было получено от указанного отправителя?
 - a. Да
 - b. Да, если вы знаете отправителя
 - c. Нет, поскольку данные отправителя можно легко подделать
 - d. Может быть.
4. На компьютере отображается непонятное сообщение. Какое действие предпринять?
 - a. Продолжить Будто ничего не произошло.
 - b. Нажать кнопку «ОК» или «ДА»
 - c. Обратится за советом к учителю, родителю или опекуну.
 - d. Больше никогда не пользоваться Интернетом
5. Что нужно сделать при получении подозрительного сообщения электронной почтой?
 - a. Удалить его, не открывая.
 - b. Открыть его и выяснить, содержится ли в нем какая-нибудь важная информация.
 - c. Открыть вложение, если такое имеется в сообщении.
 - d. Отправить его родителям
6. В ящик входящей почты пришло «письмо счастья». В письме говорится, чтобы его переслали пяти друзьям. Какое действие предпринять?
 - a. Переслать его пяти друзьям.
 - b. Переслать его не пяти друзьям, а десяти друзьям.
 - c. Не пересылать никакие «письма счастья»
 - d. Ответить отправителю, что вы больше не хотите получать от него/нее письма.
7. В каких случаях можно, не опасаясь последствий, сообщать в Интернете свой номер телефона или домашний адрес?
 - a. Во всех случаях.
 - b. Когда кто-то просит об этом.
 - c. когда собеседник в чате просит об этом.
 - d. Такую информацию следует с осторожностью сообщать людям, которым вы доверяете.
8. Вы случайно прочитали пароль, который ваш друг записал на листочке бумаг. Как вы должны поступить?
 - a. Запомнить его.
 - b. Постараться забыть пароль.

с. Сообщить другу, что вы прочитали пароль, и посоветовать сменить пароль и никогда больше не записывать на листе бумаги.

d. Сообщить пароль родителям.

9. Что такое сетевой этикет?

a. Правила поведения за столом.

b. Правила дорожного движения.

с. Правила поведения в Интернете.

d. Закон, касающийся Интернета.

10. Что запрещено в интернете?

a. Запугивание других пользователей.

b. Поиск информации.

с. Игры.

d. Общение с друзьями