Департамент образования Администрации г. Дзержинска
Нижегородской области
Муниципальное бюджетное общеобразовательное учреждение
«Средняя школа № 3»

Принята
на заседании педагогического совета
МБОУ «Средняя школа № 3»

Протокол № 12 от 30.08 2020

Утверждена
приказом директора МБОУ
«Средняя школа № 3»

Приказ от 31.08.2020 г № 175-п

Дополнительная общеобразовательная (общеразвивающая) программа Социально – гуманитарной направленности «Дети и сети: поможем подросткам выжить в Интернете»

Возраст обучающихся: **с 12 лет**
Срок реализации: **2 года**

Автор-составитель: Чистякова Е.В.,
педагог дополнительного образования высшей
квалификационной категории

г. Дзержинск
2020 год

Содержание

1. Пояснительная записка

Дополнительная общеобразовательная программа «Школа безопасности. Интернет» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков при организации урочной и внеурочной деятельности. Программа разработана для следующих уровней общего образования: начального общего образования, основного общего и среднего общего образования. Данная 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.

Направленность дополнительной общеобразовательной программы - социальная.

Программа разработана с учетом требований законов Российской Федерации: «Об образовании в Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» и "Санитарно-эпидемиологических требований к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей". требованиях ФГОС к предметным результатам освоения курса информатики для уровней начального, основного общего и среднего общего образования отсутствует предметная область «Основы безопасности в Интернете», но в рамках метапредметных результатов и предметных умений дисциплины «Информатика» вопросы информационной безопасности обозначены.

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.

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.

Актуальность программы «Школа безопасности. Интернет» заключается в исследовании проблем безопасности детей и подростков в сети Интернет, в связи с бурным развитием IT-технологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь).

Отличительной особенностью программы является то, что она способствует разностороннему раскрытию индивидуальных способностей учащихся, развитию у них интереса к различным видам деятельности, желанию активно участвовать в практической деятельности, умению самостоятельно организовывать свое свободное время.

Новизна дополнительной общеобразовательной программы «Школа безопасности. Интернет» заключается в достижении метапредметных результатов и предметных умений дисциплины 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.

Дополнительная общеразвивающая программа «Школа безопасности. Интернет» рассчитана на 34 часа, 1 час в неделю.

В процессе реализации дополнительной общеразвивающей программы «Школа безопасности. Интернет» используются следующие формы работы:

- 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; закупки в интернет магазине; квесты; создание буклетов и мультимедийных презентаций

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

Практические работы в содержании программы возможно использовать в качестве вариативных, индивидуальных практических заданий разного уровня углубленности, доступности и степени сложности исходя из диагностики и стартовых возможностей каждого из участников рассматриваемой программы.

Личностные и метапредметные результаты освоения программы

Личностные:

1. Вырабатывается 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.

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.

Формы подведения итогов реализации программы - 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.

Планируемые результаты:

Учащиеся будут знать/понимать:

- об истории появления компьютера и Интернета.; правила работы с компьютером; технические и программные возможности мобильных устройств; преимущества мобильной связи и их опасность; соблюдать правила работы с файлами; отличать безопасные сайты и ссылки от вредоносных; понимать пользу и опасности виртуального общения, социальных сетей;

- 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;

- виды общения в Интернете; правила безопасной работы при интернет – общении; чего не следует делать при сетевом общении;

- основные понятия о компьютерных вирусах и контент-фильтрах;

- принципы работы интернет - магазинов, понятие «электронные деньги»;

- правила сетевого этикета;

- политику государство в области защиты информации.

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; работать с информацией и электронной почтой; владеть основными приемами поиска информации в сети Интернет;

- соблюдать технику безопасности и гигиену при работе за ПК; владеть основными приемами навигации в файловой системе;

- пользоваться основными видами программ для общения в сети; применять программу Skype для общения, создания контактов; отличать вредные игры от полезных;

- использовать приемы работы с антивирусными программами, запускать программы-антивируса для сканирования компьютера и внешних носителей информации, устанавливать и сканировать антивирусной программой;

- дозировано использовать личную информацию в сети интернет; различать (распознавать) мошеннические действия;

- корректно общаться в сети Интернет;

- защищать свои информационные данные от внешнего воздействия (интернет и вирусы, вирусы и злоумышленники).

2. Учебный план

Наименование	1 год		2 год		Итого		Формы аттестации
	теория	практика	теория	практика	теория	практика	
Информация. Интернет	1	1	1				Промежуточная аттестация 1 раз (май) в форме тестирования после каждого года обучения.
Техника безопасности	1		1		2		
Мир виртуальный и реальный	1	2	1	2	2	4	
Проблемы Интернет-зависимости	1	2		2	1	4	
Мошеннические действия в Интернете	2	1		2	4	1	
Киберпреступления	1			2	1	2	
Сетевой этикет. Психология и сеть	2	1		2	2	3	
Методы безопасной работы в Интернете	1	2	1	3	2	5	
Потребительские опасности в Интернете	2	1		2	2	3	
Основные правила поведения сетевого взаимодействия	1	1		2	1	3	
Биометрия и защита персональных данных	1	1		2	1	3	
Личное и публичное	1			3	1	3	
Кибербулинг	2			3	2	3	
Безопасный чат. Мессенджеры	1			2	1	2	
Соц.сети и безопасность	1	1		2	1	3	
Государственная политика в области кибербезопасности	1	1	1		1	2	
Круглый стол: «Дети и сети»	1			1	1	1	

Промежуточная атеестация. Тест «Интернет и я».		1		1		2	

3. Содержание программы

Раздел 1. Информация. Интернет.(3 часа)

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.

Раздел 2. Техника безопасности. (2 часа)

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.

Раздел 3. Мир виртуальный и реальный. (6 часов)

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 Виртуальная личность - что это такое. Сайты знакомств. Незнакомцы в Интернете. Превращение виртуальных знакомых в реальных.

Раздел 4. Проблемы Интернет-зависимости (5 часов)

Интернет – зависимость. Классификация. Влияние интернет – зависимости на здоровье подростка. Как противостоять интернет – зависимости?

Раздел 5. Мошеннические действия в Интернете. (5 часов)

Что такое мошенничество? 5 главных предлогов для обмана! Основные виды интернет – мошенничества. Как не стать жертвой мошенников.

Раздел 6. Киберпреступления. (3 часа)

Фишинг. Похищение цифровой личности. Спам. Хакерство. Телекоммуникационные преступления.

Раздел 7. Сетевой этикет. Психология и сеть. (5 часов)

Этика сетевого общения. Основные понятия, используемые в сети Интернет. Изучение правил сетевого этикета. Создание памятки «12 заповедей Интернета» и памятки «Безопасный Интернет»

Раздел 8. Методы безопасной работы в Интернете. (7 часов)

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?

Раздел 9. Потребительские опасности в Интернете. (5 часов)

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.

Раздел 10. Основные правила поведения сетевого взаимодействия. (4 часа)

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

Раздел 11. Биометрия и защита персональных данных.

Общие понятия информационной безопасности. Анализ угроз информационной безопасности. Юридические основы информационной безопасности. Основные методы защиты информации. Обеспечение достоверности и сохранности информации в автоматизированных системах. Методы разграничения доступа. Криптографические методы защиты данных. Контроль защиты информации. Ответственность за нарушение правил работы с персональными данными

Раздел 12. Личное и публичное

Личное пространство и мир приватного. Публичная сфера и публичные пространства. Состояние границы между личным и публичным пространством: анализ некоторых подходов. Визуализация личного и публичного пространства в Instagram. Сеть Instagram: пространство визуальных самопрезентаций частных лиц

Раздел 13. Кибербулинг

Теоретические особенности влияния кибербуллинга на формирование личности подростка. Что такое кибербуллинг, его виды, средства. Основные действия кибербуллинга. Причины возникновения кибербуллинга. Факторы риска

Раздел 14. Безопасный чат. Мессенджеры

WatsApp. Viber. Telegramm. Основные возможности программ. Преимущества и недостатки. Интерфейс. Доступность. Принципы работы.

Раздел 15. Соц. Сети и безопасность.

Определение понятия «социальная сеть». Сущность информационной безопасности. Социальные сети как угроза информационной безопасности. Методы защиты информации в социальных сетях.

Раздел 16. Государственная политика в области защиты информации. (2 часа)

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

Раздел 17.Круглый стол: «Дети и сети»

4. Методическое обеспечение

Материально-техническое обеспечение реализации включает следующий перечень необходимого оборудования:

п/п

- Средства ИКТ
- Универсальный портативный компьютер
- Мультимедийный проектор.
- Интерактивная доска.
- Доступ к сети Интернет.

Список литературы:

1. Бирюков А.А. Информационная безопасность защита и нападение 2 е 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 защитыинформации: 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.