

Муниципальное бюджетное образовательное учреждение

Гаханская средняя общеобразовательная школа

«Рассмотрено»

«Согласовано»

«Утверждаю»

На заседании ШМО

Зам. по УВР

Директор школы

Протокол №1

 /Измайлова О.О./



/Доржиев Е.Б.

Рабочая программа по внеурочной деятельности

«Инфобезопасность»

для 5-11 классов

«ТОЧКА РОСТА»

Составитель: Шобохонов С.Ю.

Бадагуй 2022 год

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

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

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".

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;
 1. 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 5-11 классов. Объем – 36 часов.

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

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. 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.

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 по внеурочной деятельности «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	Название темы	Всего часов	Теоретические Занятия	Практические занятия
1.	Информация, компьютер и Интернет.	6	1	1

2.	Техника безопасности и экология	6	1	1
3.	Мир виртуальный и реальный. Интернет зависимость.	6	1	1
4.	Методы безопасной работы в Интернете	6	1	1
5	Потребительские опасности в Интернете	6	1	1
6.	Итого	30	5	5

СОДЕРЖАНИЕ ПРОГРАММЫ

5-11 классы

Тема № 1. - 2 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.

1. 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.

1. Тематика практических работ:

Практическая работа №1. Поиск информации в сети Интернет. Создание электронной почты.

Тема № 2. – 2 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

- 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 №2 «Создание презентации «Компьютер и здоровье человека»

Тема № 3. - 2 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.

1. **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.

Отличать вредные игры от полезных.

1. **Тематика практических работ:**

Практическая работа №3. Создание сообщества класса в детских социальных сетях.

Тема № 4. - 2 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?

1. **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

1. **Тематика практических работ:**

Практическая работа №4. Поиск вирусов (выявление признаков заражения вирусом).

Тема № 5. – 2 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.

1. 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.

1. Тематика практических работ:

Практическая работа №5. Квест «Покупка в интернет-магазине».

Календарно- тематическое планирование занятий на 2020-2021 учебный год

№ п/п	Тема	Планируемая дата проведения	Фактическая дата проведения	Примечание
1	Информация, компьютер и Интернет.			
2	Практическая работа №1. Поиск информации в сети Интернет. Создание электронной почты.			
3	Техника безопасности и экология			
4	Практическая работа №2 «Создание презентации «Компьютер и здоровье человека»			
5	Мир виртуальный и реальный. Интернет зависимость			

6	Практическая работа №3. Создание сообщества класса в детских социальных сетях			
7	Методы безопасной работы в сети Интернет.			
8	Практическая работа №4. Поиск вирусов			
9	Потребительские опасности в Интернете			
10	Практическая работа №5. Квест «Покупка в интернет- магазине».			

ПРИЛОЖЕНИЕ 1

Тест по безопасности в сети Интернет (начальное общее образование)

1. Как могут распространяться компьютерные вирусы?
 1. Посредством электронной почты.
 2. При просмотре веб-страниц.
 3. Через клавиатуру.
 4. Их распространяют только преступники.
2. Зачем нужен брандмауэр?
 1. Он не дает незнакомцам проникать в компьютер и просматривать файлы.
 2. Он защищает компьютер от вирусов.
 3. Он обеспечивает защиту секретных документов.
 4. Он защищает компьютер от пожара.
3. Всегда ли можно быть уверенным в том, что электронное письмо было получено от указанного отправителя?
 1. Да
 2. Да, если вы знаете отправителя
 3. Нет, поскольку данные отправителя можно легко подделать

4. Может быть.
4. На компьютере отображается непонятное сообщение. Какое действие предпринять?
 1. Продолжить Будто ничего не произошло.
 2. Нажать кнопку «ОК» или «ДА»
 3. Обратится за советом к учителю, родителю или опекуну.
 4. Больше никогда не пользоваться Интернетом
5. Что нужно сделать при получении подозрительного сообщения электронной почтой?
 1. Удалить его, не открывая.
 2. Открыть его и выяснить, содержится ли в нем какая-нибудь важная информация.
 3. Открыть вложение, если такое имеется в сообщении.
 4. Отправить его родителям
6. В ящик входящей почты пришло «письмо счастья». В письме говорится, чтобы его переслали пяти друзьям. Какое действие предпринять?
 1. Переслать его пяти друзьям.
 2. Переслать его не пяти друзьям, а десяти друзьям.
 3. Не пересылать никакие «письма счастья»
 4. Ответить отправителю, что вы больше не хотите получать от него/нее письма.
1. В каких случаях можно, не опасаясь последствий, сообщать в Интернете свой номер телефона или домашний адрес?
 1. Во всех случаях.
 2. Когда кто-то просит об этом.
 3. когда собеседник в чате просит об этом.
 4. Такую информацию следует с осторожностью сообщать людям, которым вы доверяете.
2. Вы случайно прочитали пароль, который ваш друг записал на листочке бумаг. Как вы должны поступить?
 1. Запомнить его.
 2. Постараться забыть пароль.

3. Сообщить другу, что вы прочитали пароль, и посоветовать сменить пароль и никогда больше не записывать на листе бумаги.
 4. Сообщить пароль родителям.
3. Что такое сетевой этикет?
1. Правила поведения за столом.
 2. Правила дорожного движения.
 3. Правила поведения в Интернете.
 4. Закон, касающийся Интернета
4. Что запрещено в интернете?
1. Запугивание других пользователей.
 2. Поиск информации.
 3. Игры.
- d. Общение с друзьями

СПИСОК ЛИТЕРАТУРЫ

Нормативно правовые документы:

1. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. № 436-ФЗ - <https://rg.ru/2010/12/31/deti-inform-dok.html>;
2. Федеральный закон Российской Федерации от 21 июля 2011 г. № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» - <http://base.garant.ru/12188176/>;
3. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с изм., внесенными Федеральными законами от 04.06.2014 г. № 145-ФЗ, от 06.04.2015 г. № 68-ФЗ) // <http://www.consultant.ru/>; <http://www.garant.ru/>
4. Федеральный государственный образовательный стандарт начального общего образования (1-4 классы) (Приказ Министерства образования и науки РФ от 6 октября 2009 г. N 373 "Об утверждении и введении в действие федерального государственного образовательного стандарта начального общего образования" С изменениями и дополнениями от: 26 ноября 2010 г., 22 сентября 2011 г., 18 декабря 2012 г., 29 декабря 2014 г., 18 мая, 31 декабря 2015 г. <http://base.garant.ru/197127/#ixzz4tOU3n8rF>);
5. Федеральный государственный образовательный стандарт начального общего образования обучающихся с ограниченными возможностями здоровья (Приказ Министерства образования и науки РФ от 19 декабря 2014 г. N 1598 "Об утверждении федерального государственного образовательного стандарта начального общего образования обучающихся

с ограниченными возможностями

здоровья" <http://base.garant.ru/70862366/#ixzz4tOz0KaU2>);

1. Федеральный компонент государственных образовательных стандартов начального общего, основного общего и среднего (полного) общего образования (1-4 классы) (с изменениями на 7 июня 2017 года).
2. Приказ Министерства образования и науки Российской Федерации от 30.08.2013 г. № 1015 (в ред. Приказов Минобрнауки России от 13.12.2013 г. №1342, от 28.05.2014 г. № 598, от 17.07.2015 г. № 734) «Об утверждении Порядка организации и осуществления образовательной деятельности по основным общеобразовательным программам – образовательным программам начального общего, основного общего и среднего общего образования» (Зарегистрировано в Минюсте России 01.10.2013 г. № 30067)

Основная литература:

1. Бирюков А.А. Информационная безопасность защита и нападение 2-е издание: Издательство: ДМК-Пресс., 2017, 434 с.
 1. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с.
 2. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасностьсетей: Издательство: М.: НОУ "Интуит", 2016,571 с.
3. 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.
 1. Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2014, 192 с.
 2. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2012, 100 с.
7. Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с.

Дополнительная:

1. "Березовый лес" или "лес березовый" /П. Лауфер//Юный эрудит. - 2014. - № 3. - С. 24-26
2. Доценко С.М., Шпак В.Ф. Комплексная информационная безопасность объекта. От теории к практике, Издательство: ООО «Издательство Полигон», 2000, 215 с.
3. Клепа и железный друг//Клепа. - 2014. - № 8. - С. 1-33.Электронная версия журнала: <http://klepa.ru>.
4. Методическое пособие для работников системы общего образования Солдатов Г., Зотова Е., Лебешева М., Шляпников В. «Интернет: возможности, компетенции, безопасность», 2015 - 156с.
5. 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
6. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. – Феникс, 2008.

Интернет ресурсы

Полезные ссылки для учителя:

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. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/_12697.pdf;

Полезные ссылки для обучающихся:

1. http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=c_s_teach_kids – ClubSymantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля;
1. <http://www.nachalka.com/bezopasnost> - Nachalka.com предназначен для учителей, родителей, детей, имеющих отношение к начальной школе. Статья «Безопасность детей в Интернете». Советы учителям и родителям;
2. <http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html>-

Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным;

1. <http://www.ifap.ru/library/book099.pdf> - «Безопасность детей в Интернете»,

компания Microsoft. Информация для родителей: памятки, советы, рекомендации;

1. <http://www.interneshka.net/children/index.phtml> - «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет;

6) <http://www.oszone.net/6213/> - OS.zone.net - Компьютерный

информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль».