ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ ОСНОВНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 11 имени Героев воинов-интернационалистов города Новокуйбышевска городского округа Новокуйбышевск Самарской области
446208, Самарская область, г.о. Новокуйбышевск, ул. Гагарина, д. 4, тел. 2-02-32

РАССМОТРЕНО	**ПРОВЕРЕНО**	**УТВЕРЖДЕНО**
На заседании МС	Зам. директора по ВР	Директор ГБОУ ООШ № 11
Протокол №1	_____ И.В. Карапетова	г. Новокуйбышевска
29.08.2022 г.	29.08.2022 г.	_____ Н.Б. Левина
		30.08.2022 г.

Рабочая программа внеурочной деятельности

«***Информационная безопасность***»

(4 класс)

Разработчик: Латыпова Е.И.

Подписан: Левина Н.Б.
DN: C=RU, O=ГБОУ ООШ №11 г. Новокуйбышевска Самарской области, CN=Левина Н.Б., E=sch11_nkb@samara.edu.ru
Местоположение: место подписания
Дата: 2022-08-30 21:50:30

2022

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;
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 - 34 часа в год.

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. 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	Тема	Всего часов	Теоретические Занятия	Практические занятия
1.	Информация, компьютер и Интернет.	10	6	4
2.	Техника безопасности и экология	8	5	3
3.	Мир виртуальный и реальный. Интернет зависимость.	7	5	2
4.	Методы безопасной работы в Интернете	6	5	1

5	Потребительские опасности в Интернете	3	2	1
6.	Итого	34	22	12

СОДЕРЖАНИЕ ПРОГРАММЫ

4 класс

Тема № 1. - 10 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.).

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

Практическая работа 4. Создание электронной почты.

Тема № 2. - 8 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
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)

- Практическая работа №3 «Создание презентации «Компьютер и здоровье человека»

Тема № 3. - 7 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. Практическая работа №2. Тест «Есть у меня игровая зависимость».

Тема № 4. - 6 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:**

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

Тема № 5. - 3 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 дозировано использовать личную информацию в сети интернет.Уметь различать (распознавать) мошеннические действия.

3. Тематика практических работ:

Практическая работа №1. Квест «Покупка в интернет-магазине».

Календарно- тематическое планирование занятий на 2018-2019 учебный год

№ п/п	Тема	Планируемая дата проведения	Фактическая дата проведения	Примечание
	Тема № 1. - 10 ч. Информация, компьютер и Интернет.			
1	Что такое компьютер? Устройство компьютера.			
2	Глобальная информационная система сети «Интернет». Выход в Интернет.			
3	Практическая работа № 1.Поиск информации в сети Интернет.			
4	Мобильные устройства.			
5	Практическая работа № 2.Работа с мобильными устройствами			
6	Совместные игры в сети Интернет.			
7	Практическая работа №3. Обмен данными при совместной работе- скайп.			
8	Сохранение информации.			
9	Что такое электронная почта.			
10	Практическая работа № 4. Создание электронной почты.			
	Тема № 2. - 8 ч . Техника безопасности и экология			
11	Гигиена работы с компьютером.			
12	Правила работы на компьютере и техника безопасности .			
13	Польза и вред компьютерных игр.			
14	Вред компьютера здоровью человека.			
15	Улица и мобильные устройства.			
16	Практическая работа №1. Использование мобильного приложения «Компас»			
17	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)			
18	Практическая работа №3 «Создание презентации «Компьютер и здоровье человека»			
	Тема № 3. - 7 ч. **Мир виртуальный и реальный. Интернет зависимость**			
19	Что такое интернет сообщества.			
20	Социальные сети. Этика общения.			
21	Что такое интернет зависимость?			
22	Развлечения в сети Интернет. Игры.			
23	Признаки игровой зависимости.			
24	Практическая работа №1. Создание сообщества класса в детских социальных сетях.			
25	Практическая работа №2. Тест «Есть у меня игровая зависимость».			
	Тема № 4. - 6 ч. Методы безопасной работы в сети Интернете.			
26	Правила поиска информации.			
27	Фильтры.			
28	Вирусы и антивирусы.			
29	Практическая работа №1. Поиск вирусов (выявление признаков заражения вирусом).			
30	Электронные деньги.			

31	Родительский контроль.			
	Тема № 5. - 3 ч.Потребительские опасности в Интернете			
32	Польза и опасность интернет.			
33	Правила правильного скачивания информации .			
34	Практическая работа№1. Квест «Покупка в интернет-магазине».			

Тест по безопасности в сети Интернет

(начальное общее образование)

1. Как могут распространятся 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.

c. 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.

c. Правила поведения в Интернете.

d. Закон, касающийся Интернета.

10. Что запрещено в интернете?

a. Запугивание других пользователей.

b. Поиск информации.

c. Игры.

d.Общение с друзьями

ПРИЛОЖЕНИЕ 2.

План - конспект занятия

Виды Интернет - общения. Безопасно ли общение в Интернете?

(начальное общее образование)

Тематическое планирование: Правила этикета в общении. Формулы приветствия и прощания. Этикет общения по телефону. Правила поведения в общественном транспорте.

В процессе изучения темы рассматриваются вопросы интернет - общения.

Задачи:

образовательные:

познакомить с видами общения в Интернете

выяснить степень осведомленности учащихся о безопасной работе в сети познакомить с правилами безопасной работы при Интернет-общении

развивающие:

способствовать формированию информационной культуры учащихся

воспитательные:

воспитывать ответственное отношение к общению в сети **Знания:**

основные виды программ для общения в сети; чего не следует делать при сетевом общении.

Умения:

основные приемы работы с программой Skype.

Навыки:

Создание контактов в Skype

Тип занятия: изучение нового материала.

Методы и формы обучения: словесный (рассказ), видеометод, наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

Программно-дидактическое обеспечение: презентации «Как можно общаться в Интернете», «Средства для общения в Интернете», «Проблемы при общении в Интернете».

Этапы занятия:

1) Постановка цели урока и актуализация знаний (2 мин).

2) Изучение нового материала (5 мин).

Объяснение нового материала.

Просмотр презентации.

3) Практическая работа (3 мин).

Информация о домашнем задании. Технические

средства: проектор, компьютеры. Ход занятия

1) Постановка цели занятия.

Деятельность учителя: Вы узнали о том, что такое правила общения. Общаться можно не только лично, но и в Интернете. Вы наверняка уже общались так со своими друзьями и близкими и знаете, что Интернет позволяет передавать письма, рисунки, фотографии, музыку, фильмы, а также речь.

2) Актуализация знаний

Деятельность учителя: Расскажите, что такое электронная почта? Что можно пересылать с электронными письмами? Назовите почтовые программы, которые вы знаете.

Деятельность учащихся: вспомнить о программах для передачи электронной почты, о правилах пересылки вложенных файлов и т.п.

3) Изучение нового материала

Деятельность учащихся: просмотр презентации «Как можно общаться в Интернете».

Деятельность учителя(пояснения при просмотре презентаций): Интернет позволяет связать между собой любых людей в мире, поэтому, как только он появился, стали создаваться разные способы для общения в Интернете (Skype, Viber, Телеграмм, ICQ, QIP, Мэйл Агент и т.п.).

Общение в Интернете может преследовать разные цели: простая передача информации, диалог, общение в группе, совместная работа, самовыражение. В зависимости от того, с какой целью люди общаются в Интернете, они выбирают средства общения. Если нужно провести совместное обсуждение - используются конференции, позволяющие видеть и слышать друг друга, как если бы участники находились в одном помещении, хотя они могут при этом быть и в разных странах. Если достаточно только обмениваться короткими сообщениями, используются чаты.

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);

6. Федеральный компонент государственных образовательных стандартов начального общего, основного общего и среднего (полного) общего образования (1-4 классы) (с изменениями на 7 июня 2017 года).

7. 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)

   // http://www.consultant.ru/; http://www.garant.ru/

8. Приказ Министерства образования и науки Российской Федерации № 336 от 30.03.2016 «Об утверждении средств обучения и воспитания, необходимых для реализации образовательных программ начального общего, основного общего и среднего общего образования, соответствующих современным условиям обучения, необходимого для оснащения образовательных организаций, в целях реализации мероприятий по содействию созданию в

субъектах Российской Федерации (исходя из прогнозируемой потребности) новых мест в общеобразовательных организациях, критериев его формирования и требований к функциональному оснащению, а так же

норматива стоимости оснащения одного места http://минобрнауки.рф/документы/8163

9. Приказ Минобрнауки России от 15 июня 2016 г. № 715 «Об утверждении Концепции развития школьных информационно-библиотечных центров» // http://www.consultant.ru/;http://www.garant.ru/

10. Постановление Главного государственного санитарного врача Российской Федерации от 29.12.2010 № 189 (ред. от 25.12.2013 г.) «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» (Зарегистрировано в Минюсте России 03.03.2011 г. № 19993), (в ред. Изменений № 1, утв. Постановлением Главного государственного санитарного врача Российской Федерации от 29.06.2011 № 85, Изменений № 2, утв. Постановлением Главного государственного санитарного врача Российской Федерации от 25.12.2013 г. № 72, Изменений № 3, утв. Постановлением Главного государственного санитарного врача РФ от 24.11.2015 г. № 81) // http://www.consultant.ru/; http://www.garant.ru/

11. Постановление Главного государственного санитарного врача Российской Федерации от 10.07.2015 г.№ 26 «Об утверждении СанПиН 2.4.2.3286-15«Санитарно-эпидемиологические требования к условиям и организации обучения и воспитания в организациях, осуществляющих образовательную деятельность по адаптированным основным общеобразовательным програм мам для обучающихся с ограниченными возможностями здоровья» (Зарегистрировано в Минюсте России 14.08.2015 г. № 38528) // http://www.consultant.ru/; http://www.garant.ru/

12. Закон «Об образовании в Республике Башкортостан» от 1 июля 2013 года № 696-з принятый Государственным собранием-Курултаем Республики Башкортостан 27 июня 2013 года. (с изменениями и дополнениями от 26.12.2014 г., от 27.02.2015 г., 01.07.15 г., 18.09.15 г.)

13. Государственная программа "Развитие образования в Республике Башкортостан"», утверждённая постановлением Правительства Республики Башкортостан от 21 февраля 2013 года № 54.

14. Концепция развития электронного образования в Республике Башкортостан на период 2015-2020 годов.

***Основная литература*:**

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. Программно-

аппаратные 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.

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 Солдатова 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;

5) http://www.saferinternet.ru – портал Российского Оргкомитета по безопасному использованию Интернета;

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-

Безопасность в Интернете. "Основы безопасности детей и молодежи в 30 Интернете"

— интерактивный курс по Интерент-безопасности, предлагаемый российским офисом Microsoft в рамках глобальных инициатив Microsoft "Безопасность детей в Интернете" и "Партнерство в образовании". В разделе для учащихся (7-16 лет) предлагается изучить проблемы информационной безопасности посредством рассказов в картинках. В разделе для родителей и учителей содержится обновленная информация о том, как сделать Интернет для детей более безопасным, а также изложены проблемы компьютерной безопасности;

12) http://www.ifap.ru

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;

2) 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;

3) 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;

4) http://www.ifap.ru/library/book099.pdf - «Безопасность детей в Интернете»,

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

5) 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»;

7) http://www.rgdb.ru/innocuous-internet - Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов для безопасного Интернета. Как защититься от Интернет-угроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в Сети;

8) https://www.google.ru/safetycenter/families/start/basics/ - Центр безопасности. Краткие рекомендации помогут обеспечить безопасность членов семьи в Интернете, даже если вечно не хватает времени;

9) https://ege.yandex.ru/security/ - Тесты по безопасности;

10) http://www.slideshare.net/shperk/ss-47136465 - Безопасность в Интернете.

Анатолий Шперх;

11) http://shperk.ru/v-seti/prokrustovo-lozhe.html - Прокрустово ложе для информационной картины. Как мы читаем тексты в интернете;

12) http://shperk.ru/sovety/avtoritet.html - Как отличить фейк от настоящего материала? Дело о летающем дьяке Крякутном;

13) http://habrahabr.ru/company/mailru/blog/252091/ - Советы по безопасности.
http://www.ifap.ru

Полезные ссылки для взрослой аудитории. Социальные ролики

1. Вы знаете, что делают ваши дети в Интернете?
http://www.youtube.com/watch?v=d2OwtGPEdh4&feature=related

2. Защищайте детей в Интернете
http://www.youtube.com/watch?v=bdnXmTpZX04&feature=related

3. Линия помощи "Дети онлайн

" http://www.youtube.com/watch?v=qivz1wJoxk4

4. А что Ваш ребенок видит в Сети?
http://www.youtube.com/watch?v=duiiFqoGI1U&feature=related

5. Воздействие на детей
http://www.youtube.com/watch?v=8nc_ISb9C8g&feature=related

Интернет-площадки, на которых проводятся обсуждения по выбранным темам, называются Интернет-форумами. Еще одно удобное средство мгновенного обмена текстовыми сообщениями - Интернет-пейджеры, такие как ICQили QIP. Эта программа позволяет в любой момент узнать, кто из ваших постоянных собеседников находится в сети и готов к общению. Еще более удобная программа - Skype, которая позволяет совершать звонки по Интернет-телефону (в том числе и видеозвонки), а также вести переписку и проводить конференции. Кроме того, общение в сети возможно с помощью многочисленных программ для смартфонов (Fringи др.).

Все эти программы очень удобны и полезны. Но проблемы живого чело-веческого общения перешли и в Интернет. Недостатки воспитания, стремление солгать, навредить окружающим, оскорбить, оклеветать или унизить, желание заявить

о себе в духе старухи Шапокляк «Хорошими делами прославиться нельзя» - все это есть и в сети. Общение в сети может не только нанести обиду или поссорить людей - есть и более опасные последствия необдуманных поступков. И здесь тоже «все как в жизни»: незнакомые люди могут дать вам дурной совет, они могут предложить вам безобидные с виду, но очень опасные по последствиям развлечения, наконец, просто оказаться преступниками.

Самая распространенная проблема, которую создают себе люди при общении в сети, объясняется их неразборчивостью и легкомыслием. Если вы знаете человека, которого хотите включить в свой список контактов для общения - это хорошо; но часто вам предлагают стать собеседником совершенно незнакомых людей. В сети человек зачастую не виден, он скрыт псевдонимом, как маской. Создать контакт очень легко, а вот во что выльется сетевое общение - известно не всегда. Хорошо, если проблему удастся решить простым удалением нежелательного контакта. Ваш собеседник в сети может вас обманывать и притворяться тем, кем в действительности не является. Но и для вас есть опасность увлечься своей кажущейся невидимостью и безнаказанностью и самому начать обманывать или унижать людей, что уж конечно не сделает вас лучше. Можно спросить: а почему тогда не сообщить в сети все сведения о себе, которые позволили бы людям общаться именно с тобой, а не с твоим ником? Это, конечно, было бы очень хорошим решением, если бы вашей информацией не смогли воспользоваться киберпреступники. Ведь если ваши личные данные станут достоянием злоумышленника, то возможны любые неприятности: преступник сможет действовать от вашего имени, он сможет подменять вашу информацию другой, вредной для вас; наконец, он может узнать сведения о членах вашей семьи. Поэтому при всех недостатках псевдонимов ими приходится пользоваться.

Кроме того, многие программы для интернет-общения предлагают рекламу, или установку новых программ, или ссылки на какие-то новые ресурсы. Как можно знать,

какие из них полезны? Помните простое правило - не подбирайте что попало в Интернете, как и на улице. Все эти предложения могут привести к довольно печальным последствиям, из которых заражение вашего компьютера или смартфона вирусами будет еще не самым страшным.

Ну и конечно, очень просто увлечься сетевым общением и начать тратить на него даже то время, которое необходимо для важных дел - уроков, спорта, работы по дому, общения с родными и вполне реальными друзьями.

С какими из перечисленных проблем вам, возможно, уже приходилось сталкиваться?

4) Практическая работа

Деятельность учителя: сейчас мы запустим программу Skypeи посмотрим, что такое контакт и как им управлять (удаление, блокирование, разблокирование, черный список и т.д.).

Деятельность учащихся: изучение контактов в Skype.

5) Закрепление изученного материала

Опрос:

1) назвать как можно больше известных инструментов для сетевого общения

2) перечислить известные опасности интернет-общения

3) привести правила безопасности для сетевого общения

Деятельность учителя: Сегодня мы рассмотрели некоторые способы общения в интернете. Их, конечно, гораздо больше. И опасностей тоже гораздо больше. Нужно хорошо запомнить основные правила безопасности и всегда выполнять их, как правила дорожного движения. Дома спросите родителей о том, какими программами для общения вам разрешается пользоваться и расскажите о тех правилах безопасности, которые вы узнали. Обсудите их с родителями. Найдите новую информацию по запросу «Правила безопасности при работе в сети».