Муниципальное бюджетное общеобразовательное учреждение
«Карсашурская основная общеобразовательная школа»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00BBEA4C1237A777ABF675EC8C07CACF81
Владелец: Митюшкина Вера Валентиновна
Действителен: с 19.07.2024 до 12.10.2025

Утверждаю
Директор
_____/Митюшкина В. В./
Приказ № 69
от «05» сентября 2024 г

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА
технической направленности

«Кибербезопасность и кибергигиена»

Возраст: 12-15 лет
Срок реализации: 1 год
стартовый уровень

Составитель: педагог
дополнительного образования
Гондырева Татьяна Михайловна

Карсашур, 2024 г.

Пояснительная записка

С учетом роста числа угроз информационной деятельности и стремительного развития информационных технологий представляется необходимым не только
«удовлетворение познавательных интересов, поиск дополнительной информации», знание
«технических устройств (в том числе компьютеров)», умение «искать информацию с применением правил поиска (построения запросов) в базах данных, компьютерных сетях, ,но и следование строгим требованиям техники безопасности, гигиены, эргономики и ресурсосбережения при работе со средствами информационных и коммуникационных технологий», знание основ кибербезопасности, умение соблюдать требования кибербезопасности в практической деятельности и организовывать безопасность личного информационного пространства.

Необходимо отметить, что в настоящее время требования ФГОС для уровней начального, общего и полного среднего образования не содержат предметной области
«Основы кибербезопасности», но в рамках метапредметных результатов и предметных умений вопросы информационной безопасности обозначены:

- требование формирования навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права;
- умения использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;
- понимание основ правовых аспектов использования компьютерных программ и работы вИнтернете.

Программа имеет **техническую направленность.**

Актуальность программы заключается в том, что она, реализуя современные требования к обучению, формирует и воспитывает информационно грамотных людей. При освоении всех базовых дисциплин с использованием интерактивных технологий и электронных ресурсов школьники смогут не только повысить скорость обучения за счет полученных знаний в области кибербезопасности и правовых основ поведения в сети, но и почувствовать себя более защищенными в киберпространстве, оперируя проверенными и изученными инструментами.

Программа знакомит учащихся с методическими основами и практикой анализа информации в интернет-пространстве и демонстрирует социальную значимость аналитической работы. В ходе освоения программы учащиеся получат навыки исследовательской деятельности и анализа информации в интернет пространстве, смогут обнаруживать источники информации, каналы и способы ее распространения. Также учащиеся научатся распознавать опасный и вредоносный контент, манипулирование сознанием и внушение потенциально опасных идей в интернет-пространстве. Полученные знания и умения позволят критически оценивать и классифицировать получаемую в интернет пространстве информацию, использовать ее в положительных целях и нейтрализовать ее негативное влияние.

Программа предоставляет учащимся возможность самостоятельно вести исследование доступных для учащихся проблем, развивать новые способности, организовывать и планировать свою работу, оценивать её результаты.

Функциональная грамотность.

Программа «Кибербезопасность и кибергигиена» позволяет развивать г**лобальные компетенции** - способности смотреть на глобальные вопросы

критически, с разных точек зрения, чтобы понимать, как различия между людьми влияют на восприятие, суждения и представления о себе и других, и участвовать в открытом, адекватном и эффективном взаимодействии с людьми разного культурного происхождения на основе взаимного уважения к человеческому достоинству.

Объем программы. Программа рассчитана на 1 год, 34 недели по 1 часу в неделю

Формы обучения - очная

Формы проведения занятия: беседа, защита проектов, конкурс, наблюдение, открытое занятие, практическое занятие, творческая мастерская.

Уровень сложности программы стартовый.

Наполняемость группы: минимальное количество – 8 человек, максимальное количество – 10 человек.

Возраст: учащиеся 12- 15 лет

Цель и задачи программы

Цель программы:

Сформировать у учащихся способности к разностороннему и комплексному анализуинформации, размещенной на различных интернет ресурсах в интересах безопасного и рационального использования интернет пространства.

Задачи программы:

Предметная – дать первичные знания в областях «кибербезопасность», «кибергигиена»: структура, типы, методы, средства поиска информации в интернет пространстве; анализ и алгоритмы распознавания опасных и вредоносных контентов в социальных сетях.

Личностная – развитие умений выявлять и критически оценивать источники и каналы распространения информации, развитие навыков работы с инструментами кодирования и шифровании личной информации, отработка алгоритмов противодействия негативным воздействиям в интернет пространстве.

Метапредметная – формирование информационной культуры: ответственного отношения к информации с учетом правовых и этических аспектов её распространения, избирательного отношения к полученной информации; воспитание понимания значимости информационной безопасности для общественного прогресса.

Учебный план

№ п/п	Название раздела, темы	Количество часов			Формы аттестации/ контроля
		Всего	Теория	Практика	
1	**Вводное занятие. Правила ТБ.**	**1**	**1**		Беседа
2	**Безопасность персонального компьютера.**	**5**	**2**	**3**	Фронтальный опрос
3	**Работа в браузере. Настройки безопасности.**	**5**	**2**	**3**	Индивидуальный опрос
4	**Работа в поисковой системе.**	**12**	**2**	**10**	Беседа
4.1	Виды поисковых систем.	3	1	2	Фронтальный опрос
4.2	Принципы работы поисковых роботов.	3	1	2	Фронтальный опрос
4.3	Выдача информации в поиске.	3	1	2	Фронтальный опрос
4.4	Принципы эффективного поиска.	3	1	2	Фронтальный опрос
5	**Информация в интернет-пространстве.**	**10**	**2**	**8**	Индивидуальный опрос
5.1	Анализ источника информации.	5	1	4	Беседа
5.2	Анализ качества информации.	5	1	4	Фронтальный опрос
6	**Итоговое занятие.**	**1**		**1**	Индивидуальный опрос
	Итого	**34**	**9**	**25**	

Содержание программы

1. **Вводное занятие**. **Правила ТБ.**

Теория: Правила техники безопасности на уроках: подходить к технике с левой стороны,прикасаться к приборам только сухими руками, не трогать провода компьютера.

Практика: Включение и выключение компьютера и сетевого фильтра.

2. **Безопасность персонального компьютера.**

Теория: Понятие безопасности компьютера. Безопасность от внешних и внутренних факторов.

Практика: Правильное включение и настройка ПО. Проверка работы системы и защитных программ.

3. **Работа в браузере. Настройки безопасности.**

Теория: Виды браузеров. Особенности работы в каждом из них. Брендмауэры и фаерволы.

Практика: Запуск изученных браузеров. Проверка безопасности и корректности работы.

4. **Работа в поисковой системе.**

4.1 Виды поисковых систем.

Теория: Информационная структура интернета. Поисковые системы. Описание видов поисковых систем и принципов их работы.

Практика: Знакомство с основными поисковыми системами, изучение их интерфейса. Выявление на практике отличие одной поисковой системы от другой. Сравнение поисковой выдачи по одному запросу.

4.2 Принципы работы поисковых роботов.

Теория: Понятие поисковых роботов. Принципы их работы. Алгоритмы ранжирования информации в сети.

Практика: Демонстрация поисковой выдачи по разным видам запросов.**Формы контроля:** опрос

4.3 Выдача информации в поиске.

Теория: Алгоритм поиска нужной информации в сети Интернет. Безопасный поиск. Исключение подозрительных источников.

Практика: Демонстрация поисковой выдачи по разным запросам. Выявление подозрительных источников и информации, нерелевантной запросу.

4.4 Принципы эффективного поиска.

Теория: Принципы эффективного поиска информации в интернете. Виды поисковых запросов, правила их формирования.

Практика: Использование эффективного поиска информации в интернете. Создание правильного поискового запроса. Анализ поисковой выдачи, сортировка показанных сайтов по важности информации.

5. Информация в интернет-пространстве.

5.1 Анализ источника информации.

Теория: Виды источников информации в сети Интернет. Признаки достоверныхи недостоверных источников.

Практика: Анализ поисковой выдачи с точки зрения источников информации.

Исключение вредоносных и подозрительных сайтов.

5.2 Анализ качества информации.

Теория: Понятие достоверности информации. Понятие фейка. Основные правила выявления фейковой информации. Признаки достоверности информации.

Практика: Самостоятельный анализ информации, полученной из сети Интернет и других источников. Выявление фейков и подозрительных фактов.

Проверка достоверности информации учащимися.

6. Итоговое занятие: Обобщение и обсуждение важности изученной за год информации. Защита проектов.

Форма контроля: собеседование, тесты.

Планируемые результаты

Предметная – знают области «кибербезопасность», кибергигиена»: структуру, типы, методы, средства поиска информации в интернет пространстве; анализ и алгоритмы распознавания опасных и вредоносных контентов в социальных сетях.

Личностная – умеют выявлять и критически оценивать источники и каналы распространения информации, развитие навыков работы с инструментами кодирования и шифровании личной информации, отработка алгоритмов противодействия негативным воздействиям в интернет пространстве.

Метапредметная – знают информационную культуру: сформировано ответственное отношение к информации с учетом правовых и этических аспектов её распространения, избирательного отношения к полученной информации; понимают значимостьинформационной безопасности для общественного прогресса.

КАЛЕНДАРНЫЙ УЧЕБЫЙ ГРАФИК

Наименование группы / год обучения	**Срок учебного года (продолжительность обучения)**	**Кол-во занятий в неделю, продолж. одного занятия (мин)**	**Всего ак. ч. в год**	**Кол-во ак. часов в неделю**
«Кибербезопасность и кибергигиена»	с 1 сентября по 26 мая (34 уч. недель)	1 занятие по 45 мин (1 ак.ч.)	34	1

УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Помещение, в котором проводятся учебные занятия - проветриваемое и хорошо освещенное. Столы и стулья соответствуют возрасту учащихся. Предоставляются необходимые для занятий в объединении материально-технические средства, а также дидактические и методические материалы - видеофильмы, наглядные пособия.

Материально-технические средства:

- компьютер или ноутбук – 5 шт
- программное обеспечение:
  - Операционная система MicrosoftWindows;
  - Обозреватель GoogleChrome и другие интернет браузеры;
  - Текстовые редакторы Блокнот, WordPad, Word, текстовый редактор пакета OpenOffice;
  - Графические редакторы Paint, PaintNet, графические редакторы в составеMicrosoftOffice и OpenOffice;

- презентационное оборудование.
- дидактический и лекционный материалы:
- лекционный материал по принципам работ поисковых систем;
- лекционный материал по видам киберугроз;
- видео фильмы по защите от кибермошенников.

Формы аттестации

Для определения результативности освоения программы используются следующие виды аттестации:

- *входной контроль* – оценка исходного уровня знаний перед началом образовательного процесса, проводится с целью определения уровня развитиядетей;
- *текущий контроль* – оценка качества усвоения учащимися учебного материала,отслеживание активности учащихся;
- *промежуточный контроль* – оценка качества усвоения учащимися учебногоматериала по итогам учебного периода (этапа/года обучения);
- *итоговый контроль* – оценка уровня достижений учащимися по завершении освоения программы с целью определения изменения уровня развития детей, ихтворческих способностей: заключительная проверка знаний, умений, навыков.

Для входного контроля используются следующие формы: беседа, собеседование, практическое задание на определение умений и навыков.

Текущий контроль проводится по завершению разделов и тем. Формами текущего контроля являются: педагогическое наблюдение, практическое задание, самостоятельная работа.

Промежуточный контроль проводится 1 раз в полугодие. Формами промежуточного контроля являются опросы.

Итоговый контроль проводится в конце обучения по программе. Формой итогового является собеседование, тесты.

Контрольно-измерительные материалы

Перечень теоретических вопросов аттестации учащихся

Промежуточная аттестация за первое полугодие

Вопросы:

1. Как обеспечить безопасность компьютера?
2. С чего начинается работа в сети Интернет?
3. Какие системы безопасности есть в браузере?
4. Чем еще можно обезопасить личный компьютер?
5. Как часто обновляют ПО и антивирусные программы?
6. Какие поисковые системы бывают?
7. Как правильно ввести запрос в строку поиска?
8. Как работают поисковые роботы?
9. Что такое поисковая выдача?
10. Назовите отличия известных поисковых систем.

Ответы:

1. Важно регулярно обновлять операционную систему и антивирусные программы.Не заходить на подозрительные сайты, блокировать вредоносные программы.
2. Работа в сети Интернет начинается с загрузки браузера. Сегодня существует околопяти популярных браузеров, они отличаются друг от друга интерфейсом и совместимостью с операционными системами.
3. В браузере существуют встроенные системы активной защиты. Это комплексная система безопасности в браузере, которая оберегает от большинства неприятностейпри работе в интернете.
4. Безопасность личного компьютера обеспечивается антивирусными программами инадежными паролями.
5. Обновление рекомендуется раз в полгода.
6. В России существуют две популярные поисковые системы: Яндекс и Google.
7. Запрос в строку вводится на русском языке с учетом геолокации с максимальнойточностью формулировки.
8. Поисковые роботы работают по заданным алгоритмам поиска и предоставляютмаксимально релевантную запросу выдачу.
9. Поисковая выдача – это список страниц, которые максимально точносоответствуют введенному в строку поиска запросу.
10. Среди основных отличий: интерфейс, расположение рекламных предложений,которые не относятся к органической выдаче, инструменты геолокации.

Критерии оценки ответов на вопросы:
Высокий уровень – учащийся ответил на 70% и более вопросов правильно, приводитпримеры, хорошо ориентируется в материале.
Средний уровень – учащийся ответил правильно на 70-50% вопросов правильно,отвечает на дополнительные вопросы.
Низкий уровень – учащийся ответил менее, чем на 50% вопросов или учащийся неответил ни на одни вопрос, не ориентируется в материале.

Промежуточная аттестация за второе полугодие

Вопросы:

1. От чего зависит эффективность поиска информации в сети?
2. С чего начать поиск нужной информации?
3. Как распознать недостоверный источник информации?
4. Что такое фейк?
5. Основные признаки фейковой информации
6. Основные признаки фейковых изображений
7. Как проверить фактическую достоверность новости?
8. Какую информацию можно использовать для учебной деятельности?
9. Как правильно использовать полученную в сети информацию?
10. Если в источнике не указан автор, можно ли использовать информацию без ссылки на источник?

Ответы:

1. Эффективность поиска зависит от качества запроса, точно формулировки и наличия данной информации на сайтах.
2. Поиск информации начинается с формулировки поискового запроса и определения его вида.
3. Недостоверные источники можно распознать по некорректности доменного имени сайта, дизайну, внешнему виду, информационному наполнению.
4. Фейк – недостоверная информация, выдаваемая за действительность с целью введения в заблуждение.
5. Признаки фейка: наличие орфографических ошибок, побудительная форма подачи, наличие фактологических ошибок.
6. Признаки фейковых изображений: использование графических редакторов, навязчивое использование рекламы, фактологические неточности.
7. Проверить достоверность информации можно путем сравнения с другими источниками, анализом самого источника и анализом информационного сообщения.
8. Для учебной деятельности можно использовать только проверенную информацию, которая не содержит признаки фейка.
9. Использовать информацию можно только при указании ссылки на ее источник.
10. Если автор текста не указан, ссылку на источник все равно необходимо использовать. В данном случае авторство закрепляется за конкретным изданием, сайтом.

Критерии оценки ответов на вопросы:

Высокий уровень – учащийся ответил на 70% и более вопросов правильно, приводит примеры, хорошо ориентируется в материале.
Средний уровень – учащийся ответил правильно на 70-50% вопросов правильно, отвечает на дополнительные вопросы.
Низкий уровень – учащийся ответил менее, чем на 50% вопросов или учащийся не ответил ни на одни вопрос, не ориентируется в материале.

Вопрос №1 Персональные данные состоят из:

1. ФИО, возраст, домашний адрес и номер телефона
2. Группа крови, отпечатки пальцев, медицинские диагнозы
3. Группа крови, отпечатки пальцев, медицинские диагнозы
4. Все вышеперечисленное. Персональные данные — это информация, по которой тебя можно идентифицировать.

Вопрос №2 Можешь ли ты контролировать размещение своих фотографий в сети Интернет, если выкладываешь их в социальные сети?

1. Да
2. Нет

Вопрос №3 Друг устраивает вечеринку в выходные, и все ваши друзья приглашены. Правильно ли будет разместить дату, время и место на сайте, потому что тогда у каждого будут детали этой встречи:

1. Да
2. Нет

Вопрос №4 Какие файлы ты разместишь в социальных сетях?

1. Все, что захочу, это смешно и интересно – моим друзьям понравится
2. Сначала подумаю. Буду ли я чувствовать себя комфортно, если родители, учителя увидят то, что я публикую?
3. Фотографии, ФИО, адрес

Вопрос №5 Может ли твой друг заходить в твой аккаунт и отправлять от твоего имени сообщения?

1. Да, потому что он мой друг, и я ему доверяю
2. Нет. Имея доступ к твоему аккаунту, друг может иметь доступ не только к тем файлам, которые ты разрешил смотреть, но и ко всем остальным данным

Вопрос №6 При заполнении онлайн-формы для ввода данных, которые будут опубликованы, какие данные не стоит указывать?

1. Никнэйм или псевдоним
2. ФИО
3. Адрес, где ты живешь
4. Адрес, где ты учишься * - Допускается несколько вариантов ответа

Вопрос №7 Какие последствия могут наступить, если ты отметишь друга на фото:

1. Массовое распространение фотографии в сети, если не настроена приватность учетной записи
2. Никаких последствий не будет
3. Ничего не случится, мой друг просто станет популярнее

Вопрос №8 Если у тебя есть сомнения, дать ли людям, с которыми общаешься в сети больше личной информации о себе, что ты сделаешь:

1. Расскажешь взрослому и попросишь совет
2. Расскажешь другу (подруге) и попросишь совет
3. Отправишь личные данные и посмотришь, что будет
4. Не отправишь личные данные

* - Допускается несколько вариантов ответа 7

Блок 2

Вопрос №1 К правовым методам, обеспечивающим информационную безопасность, относятся:

1. Разработка аппаратных средств обеспечения правовых данных

2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Вопрос №2 Основными источниками угроз информационной безопасности являются все указанное в списке:

1. Хищение жестких дисков, подключение к сети, инсайдерство
2. Перехват данных, хищение данных, изменение архитектуры системы
3. Хищение данных, подкуп системных администраторов, нарушение регламента работы

Вопрос №3 Виды информационной безопасности:

1. Персональная, корпоративная, государственная
2. Клиентская, серверная, сетевая
3. Локальная, глобальная, смешанная

Вопрос №4 Цели информационной безопасности – своевременное обнаружение, предупреждение:

1. несанкционированного доступа, воздействия в сети
2. инсайдерства в организации
3. чрезвычайных ситуаций

Вопрос №5 Основные объекты информационной безопасности:

1. Компьютерные сети, базы данных
2. Информационные системы, психологическое состояние пользователей
3. Бизнес-ориентированные, коммерческие системы

Вопрос №6 Основными рисками информационной безопасности являются:

1. Искажение, уменьшение объема, перекодировка информации
2. Техническое вмешательство, выведение из строя оборудования сети
3. Потеря, искажение, утечка информации

Вопрос №7 К основным принципам обеспечения информационной безопасности относится:

1. Экономической эффективности системы безопасности
2. Много платформенной реализации системы
3. Усиления защищенности всех звеньев системы

Вопрос №8 Основными субъектами информационной безопасности являются:

1. руководители, менеджеры, администраторы компаний
2. органы права, государства, бизнеса
3. сетевые базы данных, файрволлы

Вопрос №9 К основным функциям системы безопасности можно отнести все перечисленное:

1. Установление регламента, аудит системы, выявление рисков
2. Установка новых офисных приложений, смена хостингкомпании
3. Внедрение аутентификации, проверки контактных данных пользователей

Вопрос №10 Принципом информационной безопасности является принцип недопущения:

1. Неоправданных ограничений при работе в сети (системе)
2. Рисков безопасности сети, системы
3. Презумпции секретности

Вопрос №11 Принципом политики информационной безопасности является принцип:

1. Невозможности миновать защитные средства сети (системы)
2. Усиления основного звена сети, системы
3. Полного блокирования доступа при риск-ситуациях

Вопрос №12 Принципом политики информационной безопасности является принцип:

1. Усиления защищенности самого незащищенного звена сети (системы)
2. Перехода в безопасное состояние работы сети, системы
3. Полного доступа пользователей ко всем ресурсам сети, системы

Вопрос №13 Принципом политики информационной безопасности является принцип:

1. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
2. Одноуровневой защиты сети, системы
3. Совместимых, однотипных программно-технических средств сети, системы

Вопрос №14 К основным типам средств воздействия на компьютерную сеть относится:

1. Компьютерный сбой
2. Логические закладки («мины»)
3. Аварийное отключение питания

Вопрос №15 Когда получен спам по e-mail с приложенным файлом, следует:

1. Прочитать приложение, если оно не содержит ничего ценного – удалить
2. Сохранить приложение в парке «Спам», выяснить затем IPадрес генератора спама
3. Удалить письмо с приложением, не раскрывая (не читая) его

Вопрос №16 Принцип Кирхгофа:

1. Секретность ключа определена секретностью открытого сообщения
2. Секретность информации определена скоростью передачи данных
3. Секретность закрытого сообщения определяется секретностью ключа

Вопрос №17 ЭЦП – это:

1. Электронно-цифровой преобразователь
2. Электронно-цифровая подпись
3. Электронно-цифровой процессор

Вопрос №18 Наиболее распространены угрозы информационной безопасности корпоративной системы:

1. Покупка нелицензионного ПО
2. Ошибки эксплуатации и неумышленного изменения режима работы системы
3. Сознательного внедрения сетевых вирусов

Вопрос №19 Наиболее распространены угрозы информационной безопасности сети:

1. Распределенный доступ клиент, отказ оборудования
2. Моральный износ сети, инсайдерство
3. Сбой (отказ) оборудования, нелегальное копирование данных

Вопрос №20 Наиболее распространены средства воздействия на сеть офиса:

1. Слабый трафик, информационный обман, вирусы в интернет
2. Вирусы в сети, логические мины (закладки), информационный перехват
3. Компьютерные сбои, изменение администрирования, топологии

Вопрос №21 Утечкой информации в системе называется ситуация, характеризуемая:

1. Потерей данных в системе
2. Изменением формы информации
3. Изменением содержания информации

Вопрос №22 Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

1. Целостность
2. Доступность
3. Актуальность

Вопрос №23 Угроза информационной системе (компьютерной сети) – это:

1. Вероятное событие
2. Детерминированное (всегда определенное) событие
3. Событие, происходящее периодически

Вопрос №24 Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

1. Регламентированной
2. Правовой
3. Защищаемой

Вопрос №25 Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

1. Программные, технические, организационные, технологические
2. Серверные, клиентские, спутниковые, наземные
3. Личные, корпоративные, социальные, национальные

Вопрос №26 Окончательно, ответственность за защищенность данных в компьютерной сети несет:

1. Владелец сети
2. Администратор сети
3. Пользователь сети

Вопрос №27 Политика безопасности в системе (сети) – это комплекс:

1. Руководств, требований обеспечения необходимого уровня безопасности
2. Инструкций, алгоритмов поведения пользователя в сети
3. Нормы информационного права, соблюдаемые в сети

Вопрос № 13 Наиболее важным при реализации защитных мер политики безопасности является:

1. Аудит, анализ затрат на проведение защитных мер
2. Аудит, анализ безопасности
3. Аудит, анализ уязвимостей, риск-ситуаций

Список литературы

1. Говор С.А., Теделури М.М., Шулаева О.В. Рабочая программа по направлению «Кибергигиена». – Москва, 2019 г.
2. Дополнительная общеобразовательная программа «Кибергигиена и работа с большими данными», автор: Жалыбина Юлия Витальевна, Малыгин Александр Александрович, г. Михайловск, 2020 год.
3. Ефимова Л.Л., Кочерга С.А. Информационная безопасность детей: российскийи зарубежный опыт: Монография. М.: ЮНИТИ-ДАНА, 2013.
4. Рабочая программа «Основы кибербезопасности», автор: Киселева Наталья Александровна, Верхнесоленовская СОШ, Ростовская область, 2018 год.

Интернет ресурсы:

www.metod-kopilka.ru – Методическая копилка учителя информатики
http://www.klyaksa.net/ - Информатика и ИКТ в школе. Компьютер на уроках

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

Методы обучения: словесный, наглядный практический; объяснительно-иллюстративный, репродуктивный, исследовательский, проектный, убеждение, поощрение, стимулирование, мотивация.
Формы организации образовательного процесса: индивидуальная, индивидуально-групповая и групповая.
Формы организации учебного занятия - беседа, практическое занятие, презентация.
Педагогические технологии - технология индивидуализации обучения, технология группового обучения, технология коллективного взаимообучения, технология программированного обучения, технология дифференцированного обучения, технология разноуровневого обучения, технология развивающего обучения, технология проблемного обучения, технология проектной деятельности.

Календарный план воспитательной работы

№	Мероприятие	Срок проведения	Ответственный
1	Урок безопасности	Сентябрь, январь	Гондырева Т.М.
2	Урок цифры	Сентябрь-апрель	Гондырева Т.М.
3	День Интернета	Сентябрь	Гондырева Т.М.
4	День информатики в России	Декабрь	Гондырева Т.М.