

**«ПРОВЕРЕНО»**

Заместитель директора по УВР  
ГБОУ гимназии  
им. С. В. Байменова  
города Похвистнево  
\_\_\_\_\_ / Н. А. Власова /

«30» августа 2022 г.

**«УТВЕРЖДЕНО»**

Директор ГБОУ гимназии  
им. С. В. Байменова  
города Похвистнево

\_\_\_\_\_ / Г. И. Павлова/  
Приказ № 304-од  
от «31 » августа 2022 г.

**РАБОЧАЯ ПРОГРАММА КУРСА  
ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ**

<b>Наименование курса</b>	<b>Цифровая гигиена</b>
<b>Классы</b>	<b>8</b>
<b>Количество часов</b>	<b>34</b>
<b>Составители</b>	<b>Распанамарева Е.И</b>
<b>Учителя, работающие по данной программе</b>	<b>Александров А.В.</b>

**«РАССМОТРЕНО»**

на заседании методического  
объединения учителей  
математики и информатики  
протокол № 1  
от 27 августа 2022 г.

Руководитель МО

\_\_\_\_\_ /Волоскова Т.Ю./

### **Пояснительная записка**

Программа курса «Цифровая гигиена» предназначена для учащихся 8 класса, а также родителям обучающихся всех возрастов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам. Данная программа разработана в соответствии учебным планом образовательного учреждения на основе ФГОС среднего общего образования (утвержден Приказом Минобрнауки России № 413 от 17.05.2012 г. и № 613 от 29.06. 2017 г.).

Программа внеурочной деятельности «Цифровая гигиена» направлена на то, чтобы помочь учащимся

**Направленность программы:** профориентационная.

#### **Актуальность**

**Основными целями** изучения курса «Цифровая гигиена» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

#### **Задачи программы:**

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

**Особенности реализации программы.** Программа «Цифровая гигиена» разработана на 34 часа, 1 час в неделю в 8 классе.

#### **Общая характеристика учебного курса**

Курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит

родителям выступать в качестве экспертов, передающих опыт.

Данный курс предполагает организацию работы в соответствии с содержанием 2-х модулей, предназначенных для обучающихся 8 классов и родителей обучающихся любого возраста соответственно.

### **Модуль «Информационная безопасность»**

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7-9 классов. Рекомендуется для реализации в рамках внеурочной деятельности обучающихся.

В преподавании модуля «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

#### **Место учебного курса (Модуль 1) в учебном плане**

Программа учебного курса (Модуль 1) рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. На изучение модуля «Информационная безопасность» отводится по 1 часу в неделю в 8 классе. Учебные занятия по программе могут быть реализованы в различных вариантах:

1. в течение одного учебного года в 7, 8 или 9 классах. В этом случае программа рассчитана на 34 учебных часа;
2. по одному разделу последовательно в 7, 8 и 9 классах;
3. произвольно распределены учителем в зависимости от интереса и готовности школьников.

### **Планируемые результаты освоения обучающимися программы внеурочной деятельности**

#### ***Предметные:***

*Обучающийся научится:*

- анализировать доменные имена компьютеров и адреса документов в интернете;
- безопасно использовать средства коммуникации,
- безопасно вести и применять способы самозащиты при попытке мошенничества,
- безопасно использовать ресурсы интернета.

*Обучающийся овладеет:*

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

*Обучающийся получит возможность овладеть:*

- основами соблюдения норм информационной этики и права;
- основами самоконтроля, самооценки, принятия решений и осуществления

осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;

- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет- ресурсы и другие базы данных.

### **Метапредметные:**

#### **Регулятивные универсальные учебные действия**

*Обучающийся научится:*

- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- принимать решение в учебной ситуации и нести за него ответственность.

#### **Познавательные универсальные учебные действия**

*Обучающийся научится:*

- выделять явление из общего ряда других явлений;
- определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- критически оценивать содержание и форму текста;
- определять необходимые ключевые поисковые слова и запросы.

#### **Коммуникативные универсальные учебные действия**

*Обучающийся научится:*

- строить позитивные отношения в процессе учебной и познавательной деятельности;
- критически относиться к собственному мнению, с достоинством признавать

- ошибочность своего мнения (если оно таково) и корректировать его;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
  - делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.
  - целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
  - выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
  - использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
  - использовать информацию с учетом этических и правовых норм;
  - создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

### **Личностные универсальные учебные действия**

*У обучающегося будет формироваться:*

- осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

### **Учебно-тематический план**

№ п/п	Название раздела	Количество часов	
		Теория	Практика
1	Безопасность общения	5	8
2	Безопасность устройств	3	5
3	Безопасность информации	5	8
	<b>Итого</b>	<b>13</b>	<b>21</b>

### **Содержание программы учебного курса.**

Содержание программы учебного курса соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и

корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

## **Содержание учебного курса (Модуль 1).**

### **Раздел 1. «Безопасность общения»**

#### **Тема 1. Общение в социальных сетях и мессенджерах. 1 час.**

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

#### **Тема 2. С кем безопасно общаться в интернете. 1 час.**

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

#### **Тема 3. Пароли для аккаунтов социальных сетей. 1 час.**

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

#### **Тема 4. Безопасный вход в аккаунты. 1 час.**

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

#### **Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.**

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

#### **Тема 6. Публикация информации в социальных сетях. 1 час.**

Персональные данные. Публикация личной информации.

#### **Тема 7. Кибербуллинг. 1 час.**

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

#### **Тема 8. Публичные аккаунты. 1 час.**

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

#### **Тема 9. Фишинг. 2 часа.**

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

### **Выполнение и защита индивидуальных и групповых проектов. 3 часа.**

### **Раздел 2. «Безопасность устройств»**

#### **Тема 1. Что такое вредоносный код. 1 час.**

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

#### **Тема 2. Распространение вредоносного кода. 1 час.**

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

#### **Тема 3. Методы защиты от вредоносных программ. 2 часа.**

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

**Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.**

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

**Выполнение и защита индивидуальных и групповых проектов. 3 часа.**

**Раздел 3 «Безопасность информации»**

**Тема 1. Социальная инженерия: распознать и избежать. 1 час.**

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

**Тема 2. Ложная информация в Интернете. 1 час.**

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

**Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.**

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

**Тема 4. Беспроводная технология связи. 1 час.**

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

**Тема 5. Резервное копирование данных. 1 час.**

Безопасность личной информации. Создание резервных копий на различных устройствах.

**Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.**

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

**Выполнение и защита индивидуальных и групповых проектов. 3 часа.**

**Повторение. Волонтерская практика. 3 часа.**

## КАЛЕНДАРНО-ТЕМАТИЧЕСКИЙ ПЛАН ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ В 8 КЛАССЕ «ЦИФРОВАЯ ГИГИЕНА»

№ п/п	Тема	Количество часов	Дата	Виды деятельности	Форма подведения итогов
<b>Тема 1. «Безопасность общения» 13 часов</b>					
1	<b>Общение в социальных сетях и мессенджерах</b> Назначение социальных сетей и мессенджеров. Пользовательский контент.	1	1 неделя	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.	Защита индивидуальных и групповых проектов
2	<b>С кем безопасно общаться в интернете</b> Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	1	2 неделя	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.	
3	<b>Пароли для аккаунтов социальных сетей</b> Сложные пароли. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	1	3 неделя	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.	
4	<b>Безопасный вход в аккаунты</b> Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта	1	4 неделя	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.	
5	<b>Настройки конфиденциальности в социальных сетях</b> Настройки приватности и конфиденциальности в разных социальных сетях.	1	5 неделя	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.	
6	<b>Публикация информации в социальных сетях</b> Персональные данные. Публикация личной информации	1	6 неделя	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.	



7	<b>Кибербуллинг</b> Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как помочь жертве кибербуллинга.	1	7 неделя	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.	
8	<b>Публичные аккаунты</b> Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	1	8 неделя	Решает экспериментальные задачи. Самостоятельно создает источники информации различного типа и для разных аудиторий, соблюдая правила информационной безопасности.	
9-10	<b>Фишинг</b> Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Как защититься от фишеров в социальных сетях и мессенджерах.	2	9-10 неделя	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.	
11-13	<b>Выполнение и защита индивидуальных и групповых проектов</b>	3	11-13 неделя	Самостоятельная работа.	
<b>Тема 2. «Безопасность устройств» 8 часов</b>					
14	<b>Что такое вредоносный код</b> Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	1	14 неделя	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.	Защита индивидуальных и групповых проектов
15	<b>Распространение вредоносного кода</b> Способы доставки вредоносных кодов. Действия при обнаружении вредоносных кодов на устройствах.	1	15 неделя	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.	
16-17	<b>Методы защиты от вредоносных программ</b> Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	2	16-17 неделя	Изучает виды антивирусных программ и правила их установки.	
18	<b>Распространение вредоносного кода для мобильных устройств</b> Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	1	18 неделя	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.	

19-21	<b>Выполнение и защита индивидуальных и групповых проектов</b>	3	19-21 неделя	Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.	
<b>Тема 3 «Безопасность информации» 13 часов</b>					
22	<b>Социальная инженерия: распознать и избежать</b> Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	1	22 неделя	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.	Защита индивидуальных и групповых проектов
23	<b>Ложная информация в Интернете</b> Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	1	23 неделя	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.	
24	<b>Безопасность при использовании платежных карт в Интернете</b> Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	1	24 неделя	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.	
25	<b>Беспроводная технология связи</b> Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	1	25 неделя	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.	
26	<b>Резервное копирование данных</b> Безопасность личной информации. Создание резервных копий на различных устройствах	1	26 неделя	Создает резервные копии.	
27-28	<b>Основы государственной политики в области формирования культуры информационной безопасности</b> Доктрина национальной информационной безопасности. Основные направления государственной политики в области	2	27-28 неделя	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации;	

29-31	<b>Выполнение и защита Индивидуальных и групповых проектов</b>	3	29-31 неделя	- формирования отражающего правовые аспекты защиты киберпространства.	
32-34	<b>Повторение, волонтерская практика, резерв</b>	3	32-34 неделя		
	Итого	34			

## Модуль 2.

При работе с родителями важнейшей задачей является преодоление «цифрового разрыва» и обучение родителей правильной оценке своих возможностей в помощи детям в Интернете – возможностей, которые достаточно велики.

Разработчики курса предполагают, что родители с большей готовностью включатся в программу развития цифровой гигиены, предлагающую им общение, совместный поиск и развивающие игры и т.п.

Вместе с тем, формами проведения мероприятий для родителей также могут являться: лектории, выступления на родительских собраниях, микрообучение на основе технологий онлайн обучения, геймификация, создание чек-листов, совместное обучение, совместные родительско-детские проекты и пр.

Практические материалы для реализации данного модуля представлены в приложении 2 к данной рабочей программе. **Разработчики курса «Цифровая гигиена» предлагают использовать вышеуказанное приложение в качестве конструктора при подготовке к мероприятиям.**

### Тематическое планирование учебного курса (Модуль 2).

Тема 1. История возникновения Интернета. Понятия Интернетугроз. Изменения границ допустимого в контексте цифрового образа жизни

Тема 2. Изменения нормативных моделей развития и здоровья детей и подростков.

Тема 3. Цифровая гигиена: зачем это нужно? Понятие периметра безопасности. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка. Баланс ценностей развития и ценностей безопасности.

Тема 4. Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 5. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребёнка для профилактики насилия в Сети?

Тема 6. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?

Тема 7. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.

Тема 8. Пособия и обучающие программы по формированию навыков цифровой гигиены.

## Требования к содержанию итоговых проектно-исследовательских работ

### *Критерии содержания текста проектно-исследовательской работы*

1. Во введении сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована, но при этом четко определена, в необходимости исследования есть аргументы.
2. Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соответствуют теме работы
3. Есть планирование проектно-исследовательской деятельности, корректировка ее в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта – распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен корректно
4. Используется и осмысливается междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников
5. Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов точки зрения значимости для собственной проектно-исследовательской работы, выявлена его новизна, библиография и интернет ресурсы грамотно оформлены
6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
7. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях.

### *Критерии презентации проектно-исследовательской работы (устного выступления)*

1. Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержание работы, достаточная осведомленность в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.
2. Умение чётко отвечать на вопросы после презентации работы.
3. Умение создать качественную презентацию. Демонстрация умения использовать IT-технологии и создавать слайд презентацию на соответствующем его возрасту уровне.
4. Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне.
5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видеоролик, мультфильм и т.д.).
6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность наметить пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение четко обозначить пути создания сетевого продукта.
7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.

**Список источников:**

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.
4. Дети в информационном обществе // <http://detionline.com/journal/about>
5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2016. – 239 с.
6. Запечников С.В. Информационная безопасность открытых систем. В2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.
7. Защита детей by Kaspersky // <https://kids.kaspersky.ru/>
8. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Ру-сайтс, 2017. – 64 с.
9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.
10. Основы кибербезопасности. // <https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa>
11. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
12. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. № 22(66)
13. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.