# Муниципальное общеобразовательное бюджетное учреждение «Средняя общеобразовательная школа № 4» Пожарского муниципального района

**ПРИМЕРНАЯ РАБОЧАЯ ПРОГРАММА УЧЕБНОГО КУРСА**

**«ЦИФРОВАЯ ГИГИЕНА»**

Пгт Лучегорск 2021 год

Пояснительная записка

Программа курса «Цифровая гигиена» адресована учащимся 7-9 классов, а также родителям обучающихся всех возрастов и учитывает тре- бования, выдвигаемые федеральным государственным образовательным стан- дартом основного общего образования к предметным (образовательные обла- сти «Математика и информатика», «Физическая культура и основы безопасно- сти жизнедеятельности»), метапредметным и личностным результатам.

Основными целями изучения курса «Цифровая гигиена» являются:

обеспечение условий для профилактики негативных тенденций в инфор- мационной культуре учащихся, повышения защищенности детей от информа- ционных рисков и угроз;

формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского харак- тера 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 информаци- онных объектов с использованием цифровых ресурсов (текстовых, изобрази- тельных, аудио и видео);

создать условия для формирования умений, необходимых для различ- ных форм коммуникации (электронная почта, чаты, блоги, форумы, социаль- ные сети и др.) с различными целями и ответственного отношения к взаимо- действию в современной информационно-телекоммуникационной среде;

сформировать знания, позволяющие эффективно и безопасно использо- вать 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, позволя- ющие решать с помощью цифровых устройств и интернета различные повсе- дневные задачи, связанные с конкретными жизненными ситуациями, предпо- лагающими удовлетворение различных потребностей;

сформировать навыки по профилактике и коррекции зависимого пове- дения школьников, связанного с компьютерными технологиями и Интерне- том.

Общая характеристика учебного курса

Курс «Цифровая гигиена» является важной составляющей работы с обу- чающимися, активно использующими различные сетевые формы общения (со- циальные 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 цифро- вого разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Данный курс предполагает организацию работы в соответствии с содер- жанием 2-х модулей, предназначенных для обучающихся 7-9 классов и роди- телей обучающихся любого возраста соответственно.

Модуль 1. «Информационная безопасность»1

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

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

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять инфор- мационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тен- денций в развитии информационной культуры учащихся, повышения защи- щенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электрон- ных 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 про- ектов, 3 часа – повторение. На изучение модуля 1 «Информационная безопас- ность» отводится по 1 часу в неделю в 7, 8 или 9 классах. Учебные занятия по программе могут быть реализованы в различных вариантах:

в течение одного учебного года в 7, 8 или 9 классах. В этом случае про- грамма рассчитана на 34 учебных часа;

по одному разделу последовательно в 7, 8 и 9 классах;

произвольно распределены учителем в зависимости от интереса и готовно- сти школьников.

1 Программа модуля «Информационная безопасность» разработана на основе программы курса «Информаци- онная безопасность, или на расстоянии одного вируса» Наместниковой М.С.

Характеристика личностных, метапредметных и предметных результа- тов освоения учебного курса (Модуль 1) *2*

Предметные:

*Выпускник научится:*

анализировать доменные имена компьютеров и адреса документов в интер- нете;

безопасно использовать средства коммуникации,

безопасно вести и применять способы самозащиты при попытке мошенни- чества,

безопасно использовать ресурсы интернета.

*Выпускник овладеет:*

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

*Выпускник 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 форми- ровании 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.*

В результате освоения учебного курса обучающийся сможет:

идентифицировать собственные проблемы и определять главную про- блему;

выдвигать версии решения проблемы, формулировать гипотезы, предвос- хищать конечный результат;

ставить цель деятельности на основе определенной проблемы и существу- ющих возможностей;

выбирать из предложенных вариантов и самостоятельно искать сред- ства/ресурсы для решения задачи/достижения цели;

составлять план решения проблемы (выполнения проекта, проведения ис- следования);

описывать свой опыт, оформляя его для передачи другим людям в виде тех- нологии решения практических задач определенного класса;

2 Примерная основная образовательная программа основного общего образования (http://fgosreestr.ru)

оценивать свою деятельность, аргументируя причины достижения или от- сутствия планируемого результата;

находить достаточные средства для выполнения учебных действий в изме- няющейся ситуации и/или при отсутствии планируемого результата;

работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных ха- рактеристик продукта/результата;

принимать решение в учебной ситуации и нести за него ответственность.

*Познавательные универсальные учебные действия.*

В результате освоения учебного курса обучающийся сможет:

выделять явление из общего ряда других явлений;

определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способ- ные быть причиной данного явления, выявлять причины и следствия явле- ний;

строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;

излагать полученную информацию, интерпретируя ее в контексте решае- мой 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.*

В результате освоения учебного курса обучающийся сможет:

строить позитивные отношения в процессе учебной и познавательной дея- тельности;

критически относиться к собственному мнению, с достоинством призна- вать ошибочность своего мнения (если оно таково) и корректировать его;

договариваться о правилах и вопросах для обсуждения в соответствии с по- ставленной перед группой задачей;

делать оценочный вывод о достижении цели коммуникации непосред- ственно после завершения коммуникативного контакта и обосновывать его.

целенаправленно искать и использовать информационные ресурсы, необ- ходимые 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 язы- ков в соответствии с условиями коммуникации;

использовать компьютерные технологии (включая выбор адекватных за- даче инструментальных программно-аппаратных средств и сервисов) для

решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, со- здание 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 безопас- ности.

Личностные.

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 вирту- альных собеседников;

готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире про- фессий и профессиональных предпочтений, с учетом устойчивых познава- тельных интересов;

освоенность социальных норм, правил поведения, ролей и форм социаль- ной жизни в группах и сообществах;

сформированность понимания ценности безопасного образа жизни; инте- риоризация правил индивидуального и коллективного безопасного поведе- ния в информационно-телекоммуникационной среде.

Содержание программы учебного курса (Модуль 1).

Содержание программы учебного курса (Модуль 1) соответствует те- мам примерной основной образовательной программы основного общего об- разования (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.), позво- ляет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

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

Каждый раздел учебного курса (Модуля 1) завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

За счет часов, предусмотренных для повторения материала (4 часа), возможно проведение занятий для учащихся 4-6 классов. Эти занятия в каче- стве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные в ходе выполнения учеб- ных заданий по основным темам курса.

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 паро- лей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чу- жом компьютере с точки зрения безопасности личного аккаунта.

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

Настройки приватности и конфиденциальности в разных социальных се- тях. 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 кибер- буллинга.

Тема 8. Публичные аккаунты. 1 час.

Настройки приватности публичных страниц. Правила ведения публич- ных страниц. Овершеринг.

Тема 9. Фишинг. 2 часа.

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

Выполнение и защита индивидуальных и групповых проектов3. 3 часа.

3 Требования к содержанию итоговых проектно-исследовательских работ содержатся в приложении 1 к дан- ной рабочей программе

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вре- доносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

Способы доставки вредоносных кодов. Исполняемые файлы и расшире- ния вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Спо- собы выявления наличия вредоносных кодов на устройствах. Действия при об- наружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 час.

Способы защиты устройств от вредоносного кода. Антивирусные про- граммы 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 без- опасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.4 Раздел 3 «Безопасность информации»

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

Приемы социальной инженерии. Правила безопасности при виртуаль- ных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

Цифровое пространство как площадка самопрезентации, эксперименти- рования и освоения различных социальных ролей. Фейковые новости. Под- дельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интер- нете. 1 час.

Транзакции и связанные с ними риски. Правила совершения онлайн по- купок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. 1 час.

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

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на раз- личных устройствах.

Тема 6. Основы государственной политики в области формирова- ния 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 информацион- ной безопасности.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.5

Повторение. Волонтерская практика. 3 часа.

4 Требования к содержанию итоговых проектно-исследовательских работ содержатся в приложении 1 к дан- ной рабочей программе

5 Требования к содержанию итоговых проектно-исследовательских работ содержатся в приложении 1 к дан- ной рабочей программе

# Тематическое планирование учебного курса (Модуль 1).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Тема** | **Количество часов** | **Основное содержание** | **Характеристика основных видов учебной деятельности**  **обучающихся** |
| **Тема 1. «Безопасность общения»** | | | | |
| 1 | Общение в социальных сетях и мессенджерах | 1 | Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров.  Пользовательский контент. | 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. |
| 2 | С кем безопасно общаться в интернете | 1 | Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные  социальные сети. | Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения. |
| 3 | Пароли для аккаунтов социальных сетей | 1 | Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей.  Использование функции браузера по запоминанию  паролей. | Изучает основные понятия регистрационной информации и шифрования. Умеет их применить. |
| 4 | Безопасный вход в  аккаунты | 1 | Виды аутентификации.  Настройки безопасности | Объясняет причины  использования безопасного |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта. | входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного  входа. |
| 5 | Настройки  конфиденциальности в социальных сетях | 1 | Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в  мессенджерах. | Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле. |
| 6 | Публикация информации в социальных сетях | 1 | Персональные данные.  Публикация личной информации. | Осуществляет поиск и использует информацию, необходимую для выполнения  поставленных задач. |
| 7 | Кибербуллинг | 1 | Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь  жертве кибербуллинга. | Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников. |
| 8 | Публичные аккаунты | 1 | Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг. | Решает экспериментальные задачи.  Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила  информационной безопасности. |
| 9 | Фишинг | 2 | Фишинг как мошеннический  прием. Популярные варианты | Анализ проблемных ситуаций.  Разработка кейсов с примерами |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и  мессенджерах. | из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу. |
| 10 | Выполнение и защита индивидуальных и  групповых проектов | 3 |  | Самостоятельная работа. |
| **Тема 2. «Безопасность устройств»** | | | | |
| 1 | Что такое вредоносный код | 1 | Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов. | Соблюдает технику безопасности при эксплуатации компьютерных систем.  Использует инструментальные программные средства и сервисы адекватно задаче. |
| 2 | Распространение вредоносного кода | 1 | 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. | Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов. |
| 3 | Методы защиты от вредоносных программ | 2 | Способы защиты устройств от вредоносного кода.  Антивирусные программы и их | Изучает виды антивирусных программ и правила их  установки. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | характеристики. Правила защиты  от вредоносных кодов. |  |
| 4 | Распространение вредоносного кода для мобильных устройств | 1 | Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства. | Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего  возраста. |
| 5. | Выполнение и защита индивидуальных и групповых проектов | 3 |  | 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. |
| **Тема 3 «Безопасность информации»** | | | | |
| 1 | Социальная инженерия: распознать и избежать | 1 | Приемы социальной инженерии. Правила безопасности при виртуальных контактах. | Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует  получаемую информацию в процессе поиска. |
| 2 | Ложная информация в Интернете | 1 | Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей.  Фейковые новости. Поддельные страницы. | Определяет возможные  источники необходимых сведений, осуществляет поиск информации.  Отбирает и сравнивает материал по нескольким источникам. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | Анализирует и оценивает  достоверность информации. |
| 3 | Безопасность при использовании платежных карт в Интернете | 1 | Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов. | 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. |
| 4 | Беспроводная технология связи | 1 | Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях. | Используя различную  информацию, определяет понятия. Изучает особенности и стиль ведения личных и  публичных аккаунтов. |
| 5 | Резервное копирование данных | 1 | Безопасность личной  информации. Создание резервных копий на различных  устройствах. | Создает резервные копии. |
| 6 | Основы государственной политики в области формирования культуры информационной  безопасности | 2 | Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной  политики в области | Умеет привести выдержки из законодательства РФ:  - обеспечивающего конституционное право на поиск, получение и распространение информации; |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | формирования культуры информационной безопасности. | - отражающего правовые аспекты защиты  киберпространства. |
| 7 | Выполнение и защита  индивидуальных и групповых проектов | 3 |  |  |
| 8 | Повторение, волонтерская  практика, резерв | 3 |  |  |
|  | Итого | 34 |  | |

**Модуль 2.**

При работе с родителями важнейшей задачей является преодоление

«цифрового разрыва» и обучение родителей правильной оценке своих возмож- ностей в помощи детям в Интернете – возможностей, которые достаточно ве- лики.

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

Вместе с тем, формами проведения мероприятий для родителей также могут являться: лектории, выступления на родительских собраниях, микро- обучение 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 Интернет- угроз. 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.

Приложение 1

# 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 осмысляется 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 с 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, ил- люстративность. Предоставлен качественный творческий продукт (макет, прораммный продукт, стенд, статья, наглядное пособие, литературное произведение, видео-ролик, мультфильм и т.д.).
6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудни- чества 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 созда-ния 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 практи- кум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 c
  2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и за- кон, 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 c.
  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 c.
  6. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 c.
  7. Защита детей by Kaspersky // https://kids.kaspersky.ru/
  8. Кузнецова А.В. Искусственный интеллект и информационная без- опасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Ру- сайнс, 2017. – 64 c.
  9. Наместникова М.С. Информационная безопасность, или На расстоя- нии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.
  10. Основы кибербезопасности. // https://[www.xn--d1abkefqip0a2f.xn--](http://www.xn--d1abkefqip0a2f.xn--/) p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa
  11. Стрельцов A.A. Правовое обеспечение информационной безопасно- сти России: теоретические и методологические основы. – Минск, 2005. – 304 c.
  12. Сусоров И.А. Перспективные технологии обеспечения кибербез- опасности // Студенческий: электрон. научн. журн. 2019. № 22(66)
  13. Цифровая компетентность подростков и родителей. Результаты все- российского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.