



**МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 1
с углубленным изучением отдельных предметов» г. Надыма**

Утверждена

Педагогическим советом
МОУ «Средняя
общеобразовательная
школа № 1 с углубленным
изучением отдельных
предметов»
Протокол № 6 от 26.04.2021
Председатель

_____ **Е.В. Сиротинова**

Согласована

с заместителем директора по
воспитательной работе

**Заместитель директора по
воспитательной работе**

_____ **М.С. Горбачева**

Введена в действие

Приказом директора МОУ
«Средняя общеобразовательная
школа № 1 с углубленным
изучением отдельных предметов»
от 28.08.2020 № 152

Директор школы

_____ **Е.В. Сиротинова**

**Дополнительная
образовательная программа
учебного объединения дополнительного образования
IT-клуб «Я в цифровом мире»**

Направленность: техническая

Возраст детей: 14-17 лет

Срок реализации программы - 1 год

Составитель: Вечерникова Валентина Александровна
Учитель Физики-информатики,

г. Надым
2021 год

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Настоящая программа дополнительного образования «Я в цифровом мире» направлена на достижение планируемых результатов:

- предметных (образовательные области «Математика и информатика», «Экология и ОБЖ»);
- метапредметных (регулятивных, познавательных, коммуникативных);
- личностных.

Курс является важной составляющей работы с учащимися, активно использующими различные сетевые формы общения (социальные сети, игры и т.п), задумывающимся о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории ,технологических основ информационной безопасности а также продуктами отечественных IT-компаний, которые могут стать альтернативой зарубежным аналогам в рамках импортозамещения.

Программа составлена на основе следующих документов:

- Закон «Об образовании» (ФЗ РФ от 29.12.12г. № 273-ФЗ);
- Основная образовательная программа основного общего образования МОУ «Средняя общеобразовательная школа № 1 с углубленным изучением отдельных предметов», утверждена решением Педагогического совета (протокол от № 6 от 26.04.2021);
- Учебный план МОУ «Средняя общеобразовательная школа №1 с углубленным изучением отдельных предметов», утверждённй решением Педагогического совета (протокол № 6 от 26.04.2021);

Направленность программы – техническая.

Актуальность программы вызвана самим временем. Обучение информационной безопасности, как одно из важнейших направлений деятельности человека в информационной среде, рассматривается на сегодняшний день как важнейший компонент образования. В наши дни информационная безопасность востребована практически во всех сферах нашей жизни, таких как информатика, бизнес и экономика, физика. Довольно часто возникает вопрос кибербезопасности, так как кибератаки происходят ежесекундно. Для осознанного пользования интернет-ресурсами, получения пользы от нахождения в социальных сетях, избежания кибератак необходимо быть информационно грамотным.

ЦЕЛЬ, ЗАДАЧИ ПРОГРАММЫ

Цели:

-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:

- 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.

Сроки реализации

Программа рассчитана на 1 год обучения. Предлагаемая программа дополнительного образования состоит из четырех модулей.

Формы и режим занятий

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 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 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.).

Формы работы: коллективная, групповая, индивидуальная, дистанционная.

Занятия проводятся в группе, состоящей из 15 человек. Группа занимается 2 раза в неделю продолжительностью 2 учебных часа в неделю (72 часа в год).

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

В основу методики проведения занятий по программе дополнительного образования «Я в цифровом мире» положены следующие специфические и общепедагогические принципы организации работы:

1. Принцип сотворчества предполагает взаимодействие педагога и воспитанников, воспитанников друг с другом. Это способствует созданию благоприятного микроклимата в группе единомышленников, когда воспитанники легко и охотно откликаются на рекомендации педагога в выполнении различных заданий. Развитие взаимодействия идет от максимальной помощи педагога воспитанникам к нарастанию собственной активности последних.

2. Принцип доступности предполагает учет особенностей развития, анализа с точки зрения возможностей воспитанников, чтобы они не испытывали интеллектуальных, моральных и физических перегрузок.

3. Принцип деятельности предполагает освоение знаний, умений, навыков в форме деятельности. Учащиеся приобретают умения и навыки общения со сверстниками, принимая участие в играх-тренингах, дискуссиях, моделировании ситуаций.

4. Принцип систематичности и последовательности предполагает, что при соблюдении логических связей материал усваивается в большом объеме и позволяет за короткое время достичь результата.

5. Принцип обратной связи – регулярный контроль процесса обучения с помощью приемов обратной связи.

Приемы и методы: Общепедагогические методы: методы стимулирования поведения и деятельности, методы организации жизни и деятельности воспитательного коллектива, методы организации общения и взаимодействия в различных ситуациях.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

Предметные:

Выпускник 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.

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 формировании современной культуры безопасности жизнедеятельности;
- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая

Интернетресурсы и другие базы данных.

Метапредметные.

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- 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.

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, 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.

В результате освоения учебного курса обучающийся сможет:

• 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 задач 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.

- 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.

СОДЕРЖАНИЕ ПРОГРАММЫ

Раздел 1. “Информационная безопасность”

Тема 1. Общение в социальных сетях и мессенджерах. (2 часа.)

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. (2 часа.)

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. (2 часа.)

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.

Тема 10. Что такое вредоносный код. (1 час.)

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 11. Распространение вредоносного кода. (2 часа.)

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 12. Методы защиты от вредоносных программ. (2 часа.)

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

Тема 13. Распространение вредоносного кода для мобильных устройств. (1 час.)

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

Тема 14. Социальная инженерия: распознать и избежать. (1 час.)

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 15. Ложная информация в Интернете. (2 часа.)

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

Тема 16. Безопасность при использовании платежных карт в Интернете. (2 часа.)

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

Тема 17. Беспроводная технология связи. (2 часа.)

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

Тема 18. Резервное копирование данных. (2 часа.)

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 19. Основы государственной политики в области формирования культуры информационной безопасности. (2 часа.)

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

Раздел 2. “ Современный компьютер и работа с ним.”

Тема 1. Персональный компьютер как незаменимый друг и помощник современного человека (2 часа)

Общее описание компьютера. Программный принцип работы компьютера. Основные компоненты персонального компьютера, их функции и основные характеристики. Стандартные программы. Общие сведения о Microsoft Office. Состав и функции программного обеспечения. (День программиста, День рождения смайлика)

Тема 2. Знакомство с формальными исполнителями. (2 часа)

Учебные исполнители: Робот, Чертежник. Моделирование в среде компьютерных исполнителей

Тема 3. Применение прикладного программного обеспечения для создания графических объектов (4 часа)

Общие сведения о программе Microsoft Paint. Создание растровых изображений. Создание изображений (7 класс-растровых, 8 класс – в среде Чертежник, 9 класс – диаграммы в электронных таблицах) Редактирование готовых изображений. Всемирный День информации, Международный День защиты информации Моделирование составных документов. Творческий проект: Поздравительная открытка к новому году. День информатики

Тема 4. Творческие текстовые проекты как форма обработка текстовой информации (4 часа)

Общие сведения о программе Блокнот, редакторе Microsoft Word. Текстовые документы и их структурные единицы (раздел, абзац, строка, слово, символ). Технология создания текстовых документов. Создание, редактирование и форматирование текстовых документов на компьютере. Стилиевое форматирование. Моделирование составных документов: включение в текстовый документ списков, таблиц, диаграмм, формул и графических объектов. День безопасного Интернета. Творческий проект: День компьютерщика. Моделирование составных документов. Творческий проект: Поздравительная открытка к 8 марта

Тема 5. Создание мультимедийных продуктов (4 часа)

Общие сведения о программе Power Point. Создание презентации. Творческий проект: День Интернета. Эффект анимации, звука. Творческий проект: Пасха. Гиперссылки. Творческий проект: 1 мая, 9 мая. Общие сведения о программе Publisher. Творческий проект: шпаргалка по информатике

Тема 6. Защита компьютера от вредоносных воздействий.(6 часов)

Установка и обновление баз антивирусной программ. Проверка компьютера на вирусы. Проверка файла на вирусы с помощью онлайн-антивирусного сервиса. Применение программ для проверки и лечения заражённого компьютера. Защита от внешних вторжений. Типовые средства борьбы со спам-рассылками.

Раздел 3. «Отечественные IT-компании. Импортозамещение.»

Тема 1. Знакомство с продуктами отечественных IT-компаний.(2 часа.)

Отечественные IT компании их история и разработки. Самые яркие IT разработки.

Тема 2.Преимущества.(2 часа.)

Возможности отечественного софта. Основные преимущества перед иностранными разработками.

Тема 3. Работа в Мой Офисс. (6 часов.)

Мой Офисс Таблица. Мой Офисс Презентация. Мой Офисс Контакты. Мой Офисс Логос. Мой Офисс Почта. Мой Офисс Документы. Мой Офисс Календарь.

Раздел 4. «Создание и защита проектов»

Тема 1. Проект. (4 часа.)

Этапы создания проекта. Как выбрать тему и защитить проект.

Тема 3. Выбор темы проекта. (2 час.)

Тема 4.Выполнение и защита проектов. (4 часа.)

УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

Дата	№ п/п	Название занятия	Количество часов		
			Всего	Теория	Практика
Раздел 1. «Информационная безопасность»					
	1.	Общение в социальных сетях и мессенджерах.	2	1	1
	2.	С кем безопасно общаться в интернете.	1	1	0
	3.	Пароли для аккаунтов социальных сетей.	2	1	1
	4.	Безопасный вход в аккаунты.	1	1	0
	5.	Настройки конфиденциальности в социальных сетях.	1	0,5	0,5

6.	Публикация информации в социальных сетях.	2	1	1
7.	Кибербуллинг.	1	1	0
8.	Публичные аккаунты.	1	1	0
9.	Фишинг.	1	1	0
10.	Выполнение теста.	1	1	0
11.	Что такое вредоносный код.	1	1	0
12.	Распространение вредоносного кода.	2	1	1
13.	Методы защиты от вредоносных программ.	2	1	1
14.	Распространение вредоносного кода для мобильных устройств.	1	1	0
15.	Выполнение теста.	1		1
16.	Социальная инженерия: распознать и избежать.	1	1	0
17.	Ложная информация в Интернете.	2	1	1
18.	Безопасность при использовании платежных карт в Интернете.	2	1	1
19.	Беспроводная технология связи.	2	1	1
20.	Резервное копирование данных.	2	1	1
21.	Выполнение теста.	1	1	0
ИТОГО:		30	19,5	10,5

Раздел 2. «Современный компьютер и работа с ним.»

22.	Стандартные программы. Общие сведения о Microsoft Office	1	1	0
23.	Проведение викторины на состав и функции программного обеспечения. (День программиста, День рождения смайлика)	1	0	1
24.	Использование формальных исполнителей Робот, Чертежник в неформальных ситуациях	1	0,5	0,5
25.	Моделирование в среде формальных исполнителей	1	0	1
26.	Общие сведения о прикладных программах, графических редакторах, программе Microsoft Paint. Создание растровых изображений на заданную тему.	1	0,5	0,5
27.	Создание изображений для иллюстраций творческих работ обучающихся	1	0,5	0,5
28.	Редактирование готовых изображений. Подготовка творческой работы для участия в конкурсе, посвященном Всемирному Дню информации,	1	0,5	0,5

		Международному Дню защиты информации			
29.		Подготовка творческого проекта: Поздравительная открытка к новому году. Конкурс проектов, приуроченных к Дню информатики	1	0,5	0,5
30.		Использование прикладного программного обеспечения для обработки текстовой информации.	1	0,5	0,5
31.		Создание, редактирование и форматирование текстовых документов для оформления выставки День безопасного Интернета	1	0,5	0,5
32.		Моделирование составных документов. Творческий проект: День компьютерщика.	1	0,5	0,5
33.		Моделирование составных документов. Творческий проект: Поздравительная открытка к 8 марта	1	0,5	0,5
34.		Новые возможности редактора презентаций Power Point	1	0,5	0,5
35.		Создание презентации. Творческий проект: День Интернета	1	0,5	0,5
36.		Эффект анимации, звука. Творческий проект: Пасха	1	0,5	0,5
37.		Гиперссылки. Творческий проект: 1 мая, 9 мая	1	0,5	0,5
38.		Общие сведения о программе Publisher. Творческий проект: шпаргалка по информатике.	1	0,5	0,5
39.		Установка и обновление баз антивирусной программы Avira AntiVir Personal Edition Classic.	1	0,5	0,5
40.		Проверка компьютера на вирусы с помощью антивирусной программы Avira AntiVir Personal Edition Classic.	1	0,5	0,5
41.		Проверка файла на вирусы с помощью онлайн-антивирусного сервиса.	1	0,5	0,5
42.		Применение программы CureIt для проверки и лечения заражённого компьютера.	1	0,5	0,5
43.		Защита от внешних вторжений (программа Agnitum Outpost).	1	0,5	0,5
ИТОГО:			22	10,5	11,5
Раздел 3. «Отечественные IT-компании. Импортозамещение.»					
44.		Отечественные IT компании их история и разработки.	1	1	0

	45.	Самые яркие IT разработки.	1	1	0
	46.	Возможности отечественного софта.	1	1	0
	47.	Основные преимущества перед иностранными разработками.	1	1	0
	48.	МойОфисс Таблица.	1	0	1
	49.	МойОфисс Презентация.	1	0	1
	50.	МойОфисс Контакты.	1	0	1
	51.	МойОфисс Документы.	1	0	1
	52.	МойОфисс Почта.	1	0	1
	53.	МойОфисс Календарь.	1	0	1
ИТОГО:			10	4	6
Раздел 4. «Создание и защита проектов»					
	54.	Этапы создания проекта.	2	1	1
	55.	Как выбрать тему и защитить проект.	2	1	1
	56.	Выбор темы проекта.	2	1	1
	57.	Выполнение проектов.	2	2	0
	58.	Защита проектов.	2	2	0
ИТОГО:			10	7	3
ВСЕГО за год:			72		

ФОРМЫ ПОДВЕДЕНИЯ ИТОГОВ РЕАЛИЗАЦИИ ПРОГРАММЫ

Контроль усвоения учебного материала проходит в течение всего периода обучения. Формами контроля к теоретическому разделу являются:

- контрольная работа;
- тестирование;
- круглый стол;
- практикум;
- творческое задание.

Формами контроля к практическому разделу являются:

– работа с программами.

К формам итогового контроля относятся:

- анализ материалов (статей, рубрик), экспертиза творческих работ;
- проекты
- мнения экспертов (членов жюри различных конкурсов,);
- награды и поощрения;

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 с точки зрения значимости для собственной проектноисследовательской 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, видео-ролик, мультфильм и т.д.).

6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать 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.

МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Компьютер, Мультимедийный проектор, Интерактивная доска, Мобильный класс, Сканер, Принтер

ЛИТЕРАТУРА

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, 2018. – 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, 2018. – 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.: ЮНИТИДАНА, 2020. – 239 с.
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 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- сайнс, 2018. – 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, 2018. – 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, 2019. – 144 с.