МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ
КРАСНОДАРСКОГО КРАЯ

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ СЕВЕРСКИЙ РАЙОН

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №19 ПОСЕЛКА ОКТЯБРЬСКОГО МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ СЕВЕРСКИЙ РАЙОН ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА РЫЖОВА ВАСИЛИЯ КУЗЬМИЧА

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
Руководитель ШМО учителей естественно-научного цикла	Заместитель директора по УВР	Директор МБОУ СОШ №19
_____И.В.Петрова	_____И.Г. Пелих	_____С.В.Крылова
Протокол №1 от «30» августа 2024 г.	«30» августа 2024 г.	Приказ № от «30» августа 2024 г.

РАБОЧАЯ ПРОГРАММА

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

для обучающихся 7-9 классов

пос. Октябрьский, 2024 год

Пояснительная записка

Настоящая программа «Информационная безопасность» в 7-9 классах написана на основании следующих нормативных документов:

- Федерального Государственного Образовательного Стандарта (ФГОС), утвержденного приказом Министерством образования и науки Российской Федерации от 17 декабря 2010 г. № 1897;
- Примерной рабочей программы учебного курса «Цифровая гигиена» основного общего образования, рекомендованного Координационным советом учебно-методических объединений в системе общего образования.

Программа курса «Информационная безопасность» предназначена для организации по общекультурному направлению развития личности.

Основными **целями** изучения курса «Информационная безопасность» 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.

Общая характеристика основного курса

Курс «Информационная безопасность» 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.

Данный курс предполагает изучение программы «Информационная безопасность» в течение одного года для обучающихся 7-9 классов. Программа учебного курса рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение.

Личностные, метапредметные и предметные результаты освоения учебного курса

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 Интернет-ресурсы 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 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

- 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

Содержание программы курса соответствует темам предметам «Информатика» и «Основы безопасности жизнедеятельности», 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 курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся или проверочного теста. Предусмотрено оценивание достижений обучающихся по системе «зачѐт - незачѐт». Промежуточная аттестация проводится в форме проекта.

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 распростра-нения 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 час
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

Тематическое планирование 7 класс

№ п/ п	Тема	Количество часов	Характеристика основных видов деятельности
Тема 1 «Безопасность общения»			
1	Общение в социальных сетях	1	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	Руководствуется в общении социальными ценностями и установками коллектива и интернете общества в целом. Изучает правила сетевого общения
3	Пароли для аккаунтов	1	Изучает основные понятия регистрационной информации и шифрования. Умеет их социальных сетей применить.
4	Безопасный вход в аккаунты	1	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.
5	Настройки конфиденциальности социальных сетях	1	Раскрывает причины установки закрытого профиля. Меняет основные настройки в приватности в личном профиле.
6	Публикация информации социальных сетях	1	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
7	Кибербуллинг	1	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	1	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.

9	Фишинг	2	Анализ проблемных ситуаций. Разработка кейсов с примерами 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	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче
2	Распространение вредоносного кода	1	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
3	Методы защиты от вредоносных программ	2	Изучает виды антивирусных программ и правила их установки.
4	Распространение вредоносного кода для мобильных устройств	1	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	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
2	Ложная информация в Интернете	1	Определяет возможные источники необходимых сведений, осуществляет поиск информации.

			Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.
3	Безопасность при использование платежных карт в Интернете.	1	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	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
5	Резервное копирование	1	Создает резервные копии.данных
6	Основы государственной политики в области культуры информационной безопасности	2	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение формирования информации; - отражающего правовые аспекты защиты киберпространства.
7	Выполнение и защита индивидуальных и групповых проектов	3	Самостоятельная и групповая работа по созданию продукта проекта
8	Повторение. Волонтерская	3	практика
	Итого:	34 часа	

Тематическое планирование 8 класс

№ п/ п	Тема	Количество часов	Характеристика основных видов деятельности
Тема 1 «Общие сведения о безопасности ПК и Интернета»			
1	Как устроен компьютер и Интернет	1	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	Как работают мобильные. Угрозы для мобильных устройств	1	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
3	Защита персональных данных.	1	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить
4	Компьютерная и информационная безопасность. Основные угрозы безопасности информации	1	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.
5	ПР №1 «Создание газеты«Безопасность в Интернете»	1	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле
Тема 2 «Техника безопасности и экология»			
6	Правила поведения в компьютерном кабинете.	1	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
7	Компьютер и мобильные устройства в чрезвычайных ситуациях	1	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду	1	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9	Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК	1	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни знакомых. Разработка и

			распространение чек-листа (памятки) по противодействию фишингу
10	ПР №2 «Создание буклета«Техника безопасности при работе с компьютером»	1	Самостоятельная работа.
Тема 3 «Проблемы Интернет – зависимости»			
11	ЗОЖ и компьютер. Деструктивная информация в Интернете как ее избежать.	1	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
12	Психологическое воздействие информации на человека. Управление личностью через сеть	1	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
13	Интернет и компьютер зависимость (аддикция)	1	Изучает виды антивирусных программ и правила их установки.
14	Как развивается зависимость. Типы интернет – зависимости.	1	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста
15	ПР №3 «Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».	1	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 4. «Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы»			
16	Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов	1	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
17	Отличия вирусов и закладок. Как распространяются вирусы. ПР №4 «Создание презентации на тему «Разновидности вирусов. Черви трояны, скрипты»	1	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.
18	Что такое антивирусная защита. Как лечить компьютер	1	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.
19	Антивирусные программы для ПК. Выявление неизвестных вирусов. ПР №5 «Установка антивирусной программы»	1	Самостоятельная работа
20	Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.	1	Создает резервные копии.
Тема 5. «Мошеннические действия в Интернете. Киберпреступления»			
21	Виды интернет – мошенничества. Мошеннические действия в сети.	1	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
22	Предложения о разблокировании программ. Ложные антивирусы.	1	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
23	«Легкий заработок в Интернете».	1	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки. Мошенничество при распространении «бесплатного» ПО. Азартные игры. Онлайн – казино приложений на мобильные устройства для учащихся более младшего возраста.
24	Технологии манипулирования в Интернете. Техника безопасности при интернет – общении	1	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
25	ПР №6 «Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками».	1	Самостоятельная работа
Тема 6. «Сетевой этикет. Психология и сеть»			
26	Что такое этикет. Виды этикета	1	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
27	Сетевой этикет. Общие правила сетевого этикета. Этикет и безопасность	1	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.

28	Безопасная работа в сети в процессе сетевой коммуникации	1	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.
29	Психологическая обстановка в Интернете. Если вы стали жертвой компьютерной. Агрессии	1	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
30	ПР №7 «Выпуск видеоролика на тему « Как не испортить себе настроение при общении в Сети и не опуститься до уровня «веб – агрессора».	1	Самостоятельная работа
Тема 7. «Государственная политика в области кибербезопасности»			
31	Собственность в Интернете. Авторское право. Интеллектуальная собственность.	1	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности
32	Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет	1	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста
33	Как расследуются преступления Ответственность за интернет – мошенничество в сети.	1	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
34	Создание презентации «Как уберечь свою персональную информацию в Интернете, если вы общаетесь в социальных сетях».	1	Самостоятельная работа
	Итого:	34 часа	

Тематическое планирование 9 класс

№	Тема	Количество часов	Характеристика основных видов деятельности учащихся
1	Социальная инженерия: распознать и избежать	4	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска
2	Ложная информация в Интернете	6	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	4	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	4	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
5	Резервное копирование данных	4	Создает резервные копии
6	Подготовка к итоговому тесту	1	Подготовка к тесту
7	Выполнение теста	1	Выполнение теста
8	Обсуждение тем проектов	2	Обсуждают темы проектов индивидуальных и групповых
9	Выполнение и защита	4	Выполняют и защищают проекты индивидуальных и групповых проектов
10	Повторение	4	
	Итого	34 часа	

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. Определѐн объѐм 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 чѐтко 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 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.

Список литературы.

1 Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус,
2 Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс,
3 Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ,
4 Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА,
5 Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ,
6 Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ,
7 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,
8 Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ,
9 Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум,
10 Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА,
11 Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ,
12 Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ,