государственное бюджетное общеобразовательное учреждение Самарской области
«Самарский казачий кадетский корпус"

Рассмотрено на заседании МО воспитателей Протокол № 1 «29» авг. 2019г.	ПРОВЕРЕНО Заместитель директора по УМР _____ М.А.Карпук 29 авг. 2019г.	УТВЕРЖДАЮ Директор ГБОУ "Самарский казачий кадетский корпус" _____ А.Ю.Рябов «30» августа 2019 г.

ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ОБУЧАЮЩИХСЯ
«Информационная безопасность»

Направление: общеинтеллектуальное
Форма организации: кружок
Класс: 9
Срок реализации:1 год

Составитель: Романова И.В.

Пояснительная записка.

Программа курса внеурочной деятельности «Информационная безопасность» для обучающихся 9 классов разработана на основе примерной рабочей программы учебного курса «Цифровая гигиена»: основное общее образование. - Самара, 2019, программы курса «Информационная безопасность, или на расстоянии одного вируса» Наместниковой М.С., ООП ООО ГБОУ «Самарский казачий кадетский корпус», Положения о внеурочной деятельности обучающихся в ГБОУ «Самарский казачий кадетский корпус».

Программа курса «Информационная безопасность» 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.

Актуальность

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.

В преподавании курса 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 создает 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 обучающихся, 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.).

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:

- 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.

Результаты освоения курса.

Предметные:

- 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.
- приемам безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
- основам соблюдения норм информационной этики и права;
- основам 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.
- 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.

Воспитательные результаты

Первый уровень результатов –	**В сфере личностных универсальных учебных действий у обучающихся будут сформированы:**	**В сфере регулятивных универсальных учебных действий обучающиеся научатся:**	**В сфере познавательных универсальных учебных действий обучающиеся научатся:**	**В сфере коммуникативных универсальных учебных действий обучающиеся научатся:**
приобретут: - социально-значимые знания, которые помогут выполнять базовые операции при использовании мессенджеров и социальных сетей. Создадут свой образ в сети Интернет. изучат историю и социальную значимость личных аккаунтов в сети Интернет. изучат правила сетевого общения, основные понятия регистрационной информации и шифровании и сумеют их применить.	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;	адекватно воспринимать оценку своих работ окружающими; вносить необходимые коррективы в действие после его завершения на основе оценки и характере сделанных ошибок. 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	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;	учитывать разные мнения и интересы и обосновывать собственную позицию. 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;

		задачи/достижения цели;		
Второй уровень результатов –	**В сфере личностных универсальных учебных действий у обучающихся будут сформированы:**	**В сфере регулятивных универсальных учебных действий обучающиесянаучатся:**	**В сфере познавательных универсальных учебных действий обучающиесянаучатся:**	**В сфере коммуникативных универсальных учебных действий обучающиеся научатся:**
- получат позитивное отношение к базовым ценностям общества социально значимые отношения, которые планируется развивать у обучающихся; способность к самооценке на основе критерия успешности деятельности.	-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. 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;	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.	строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям; излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;	-сотрудничать и оказывать взаимопомощь, доброжелательно и уважительно строить свое общение со сверстниками и взрослыми. 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;

Третий уровень результатов –	**В сфере личностных универсальных учебных действий у обучающихся будут сформированы:**	**В сфере регулятивных универсальных учебных действий обучающиеся научатся:**	**В сфере познавательных универсальных учебных действий обучающиеся научатся:**	**В сфере коммуникативных универсальных учебных действий обучающиеся научатся:**
получить кадетами опыт самостоятельного общественного действия, т.е. тот опыт социально значимого действия, приобретение которого обучающимися планируется организовать. Разработать и создать разнообразные проекты: информационные, исследовательские, социальные. -школьник приобретает опыт публичного выступления по проблемным вопросам; -опыт интервьюирования и проведения опросов общественного мнения; -опыт общения с представителями других социальных групп; - -опыт организации совместной деятельности с другими детьми.	-навык самостоятельной работы и работы в группе при выполнении творческих работ; -заложены основы личностных и нравственных качеств. 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;	выполнять проекты, 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;	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.	формировать собственное мнение и позицию. 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;

	сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.			создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Программа курса внеурочной деятельности «Информационная безопасность» для обучающихся 9 классов рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение.

Формы подведения итогов - тестирование по темам курса; защита групповых и (или) индивидуальных проектов.

Содержание курса

№п/п	Раздел программы	Содержание	Формы организации занятия
Раздел 1. «Безопасность общения»			
1.	Тема 1. Общение в социальных сетях и мессенджерах. 1 час.	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров.Пользовательский контент.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением,

			беседы с элементами диалога
2.	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.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
3.	Тема 3. Пароли для аккаунтов социальных сетей. 1 час.	Сложные пароли. Онлайн генераторы паролей. Правила хранения паро-лей. Использование функции браузера по запоминанию паролей.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
4.	Тема 4. Безопасный вход в аккаунты. 1 час.	Виды аутентификации. Настройки безопасности аккаунта. Работа на чу-жом компьютере с точки зрения безопасности личного аккаунта.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
5.	Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
6.	Тема 6. Публикация информации в социальных сетях. 1 час.	Персональные данные. Публикация личной информации.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
7.	Тема 7. Кибербуллинг. 1 час.	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибер-буллинга.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с

			последующим обсуждением, беседы с элементами диалога
8.	Тема 8. Публичные аккаунты. 1 час.	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
9-10	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.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
11-13	Выполнение и защита индивидуальных и групповых проектов. 3 часа.	Сбор информации в библиотеке и медиатеке в сети Интернет, обработка и анализ информации, самостоятельная работа, работа в парах и группах для подготовки и защиты проекта.	Предзащита проектов. Защита групповых проектов.
Раздел 2. «Безопасность устройств»			
14	Тема 1. Что такое вредоносный код. 1 час.	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
15	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.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
16-17	Тема 3. Методы защиты от	Способы защиты устройств от вредоносного кода. Антивирусные	Интерактивные познавательные,

	вредоносных программ. 2 час.	про-граммы и их характеристики. Правила защиты от вредоносных кодов.	тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
18	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.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
19-21	Выполнение и защита индивидуальных и групповых проектов. 3 часа.4	Сбор информации в библиотеке и медиатеке в сети Интернет, обработка и анализ информации, самостоятельная работа, работа в парах и группах для подготовки и защиты проекта.	Предзащита проектов. Защита групповых проектов
Раздел 3 «Безопасность информации»			
22	Тема 1. Социальная инженерия: распознать и избежать. 1 час.	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
23	Тема 2. Ложная информация в Интернете. 1 час.	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
24	Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением,

			беседы с элементами диалога
25	Тема 4. Беспроводная технология связи. 1 час.	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
26	Тема 5. Резервное копирование данных. 1 час.	Безопасность личной информации. Создание резервных копий на различных устройствах.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
27-28	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 информационной безопасности.	Интерактивные познавательные, тематические беседы демонстрация видеофильмов с последующим обсуждением, беседы с элементами диалога
29-31	Выполнение и защита индивидуальных и групповых проектов. 3 часа.	Сбор информации в библиотеке и медиатеке в сети Интернет, обработка и анализ информации, самостоятельная работа, работа в парах и группах для подготовки и защиты проекта.	Предзащита проектов. Защита проектов.
32-34	Повторение. Волонтерская практика. 3 часа.	Разработка занятий для обучающихся 5-6 классов по информационной безопасности.	Проведение занятий для обучающихся 5-6 классов в качестве волонтерской практики могут обучающимися, освоившими программу

Список литературы, используемой педагогом для разработки программы и организации образовательного процесса

1. Внеурочная деятельность: теория и практика. 1—11 классы / сост. А. В. Енин. — М.: ВАКО, 2015. — 288 с.
2. Григорьев Д. В., Степанов П. В. Внеурочная деятельность школьников. Методический конструктор: пособие для учителя. — М.: Просвещение, 2013.
3. Моделируем внеурочную деятельность обучающихся [Текст] : методические рекомендации. — М. : Просвещение, 2014.
4. ООП ООО ГБОУ «Самарский казачий кадетский корпус»
5. Положения о внеурочной деятельности обучающихся в ГБОУ «Самарский казачий кадетский корпус»

Список литературы для родителей и учащихся

1. Бабаш А.В. Информационная безопасность: Лабораторный практи-кум / 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 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 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. 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 byKaspersky // 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, 2017. – 64 с.

9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение,
10. 2019. – 80 с.

11. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xn-- p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa

12. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.

13. Сусоров И.А. Перспективные технологии обеспечения кибербез-опасности // Студенческий: электрон.научн. журн. 2019. № 22(66)

14. 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.

Тематическое планирование

№ занятия	Разделы и темы	Общее количество часов	Теоретические занятия	Практические занятия
Тема 1. «Безопасность общения» - 13				
1	Общение в социальных сетях и мессенджерах.	1	1	
2	С кем безопасно общаться в интернете	1	0.2	0.8

3	Пароли для аккаунтов социальных сетей	1	0.2	0.8
4	Безопасный вход в аккаунты	1	0.2	0.8
5	Настройки конфиденциальности всоциальных сетях	1	0.8	0.2
6	Публикация информации в социальных сетях.	1	0.8	0.2
7	Кибербуллинг.	1	0.8	0.2
8	Публичные аккаунты	1	0.8	0.2
9-10	Фишинг	2	1	1
11-13	Выполнение и защита индивидуальных и групповых проектов	3	0.6	2.4
Тема 2. «Безопасность устройств» - 8				
14	Что такое вредоносный код	1	0.2	0.8
15	Распространение вредоносного кода	1	0.2	0.8
16-17	Методы защиты от вредоносных программ	2	1	1
18	Распространение вредоносного кода для мобильных устройств	1	0.8	0.2
19-21	Выполнение и защита индивидуальных и групповых проектов	3	0.6	2.4
Тема 3 «Безопасность информации» - 13				
22	Социальная инженерия: распознать и избежать.	1	0.2	0.8
23	Ложная информация в Интернете	1	0.2	0.8
24	Безопасность при использовании платежных карт в Интернете.	1	0.2	0.8

25	Беспроводная технология связи.	1	0.2	0.8
26	Резервное копирование данных	1	0.2	0.8
27-28	Основы государственнойполитики в области формирования культуры информационной безопасности.	2	1	1
29-31	Выполнение и защита индивидуальных и групповых проектов	3	0.6	2.4
32-34	Повторение, волонтерская практика, резерв	3	0.6	2.4
	Итого:	**34**	**12.4 – 36.4%**	**21.6 – 63.6%**

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, 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.