**Пояснительная записка**

Программа курса «Информационная безопасность» адресована учащимся 9 классов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», метапредметным и личностным результатам).

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

* + обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от
* информационных рисков и угроз;
  + формирование навыков своевременного распознавания онлайн рисков

(технического, контентного, коммуникационного, потребительского  характера и риска интернет зависимости).  **Задачи программы:**

* сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием

информационных объектов с использованием цифровых ресурсов  (текстовых, изобразительных, аудио и видео);

* создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к

взаимодействию в современной информационно-телекоммуникационной  среде;

* + сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и
* т.п.;
  + сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета

различные повседневные задачи, связанные с конкретными жизненными  ситуациями, предполагающими удовлетворение различных потребностей;

* сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

**Общая характеристика учебного курса**

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

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 9 классов. Программа «Цифровая гигиена» реализуется в рамках внеурочной деятельности.

Форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микро-обучение), смешанный формат.

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

**Место учебного курса «Цифровая гигиена»**

**в учебном плане**

Программа учебного курса «Цифровая гигиена» рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. Учебные занятия по программе реализованы в течение одного учебного года в 9 классе. В этом случае программа рассчитана на 34 учебных часа.

Программа «Цифровая гигиена» разработана на основе программы курса «Информационная безопасность, или на расстоянии одного вируса» Наместниковой М.С.

**Характеристика личностных, метапредметных и предметных результатов освоения учебного курса «Цифровая гигиена»**

***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.*

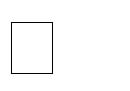
* + результате освоения учебного курса обучающийся сможет:
* выделять явление из общего ряда других явлений;
* определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины 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 учебного курса**

**«Цифровая гигиена»**

Содержание программы учебного курса «Цифровая гигиена» соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебному предмету «Информатика», а также

расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

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

Каждый раздел учебного курса «Цифровая гигиена» завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся.

Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные в ходе выполнения учебных заданий по основным темам курса.

**Содержание учебного курса «Цифровая гигиена».**

**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 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 кибербуллинга.

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

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

**Тема 9. Фишинг. 2 часа.**

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

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

**Раздел 2. «Безопасность устройств»**

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

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

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

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

**Тема 3. Методы защиты от вредоносных программ. 2 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 само презентации, 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 WiFi-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 3 часа.**

**Тематическое планирование учебного курса «Цифровая гигиена».**

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

11

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

12

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

13

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

14

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

15

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

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
* проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников
  1. 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
  2. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
  3. 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.

19

1. Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне.
2. 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.).
3. 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.
4. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.

20

**Список источников:**

* 1. Бабаш А.В. Информационная безопасность: Лабораторный практикум
* А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 c
  1. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.
  2. 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.
  3. Дети в информационном обществе // http://detionline.com/journal/about
  4. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИДАНА, 2016. – 239 c.
  5. Запечников С.В. Информационная безопасность открытых систем. В 2х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 c.
  6. Защита детей by Kaspersky // https://kids.kaspersky.ru/
  7. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 c.
  8. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 9 классы. Внеурочная деятельность. – М.: Просвещение,

2019. – 80 с.

* 1. Основы кибербезопасности. // https://www.xnd1abkefqip0a2f.xn p1ai/index.php/glava1osnovykiberbezopasnostitseliizadachikursa
  2. Стрельцов A.A. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск,

2005. – 304 c.

* 1. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. № 22(66)
  2. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.