государственное бюджетное общеобразовательное учреждение самарской области средняя общеобразовательная школа пос. Комсомольский муниципального района Кинельский Самарской области

Рассмотрено на заседании методического объединения учителей_____ Протокол № 1от «29» августа 2023г.	**Проверено** заместитель директора по УВР _____Громко И.А. «31» августа 2023г.	**Утверждено:** Директор школы: _____/А.Н. Фенюк/ Приказ №288-ОД от «31» августа 2023г

Программа курса внеурочной деятельности «Цифровая гигиена»

Направление: Общекультурное
Возраст школьников: 13-15 лет
Разработчик: Дмитриева А.Д.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00a5b63ce7cce9728f
Владелец: Фенюк А. Н. ГБОУ СОШ пос. Комсомольский
Email: koms_sch_knl@samara.edu.ru
Действителен: с 03.08.2022 по 02.08.2027

Пояснительная записка

Данная программа курса «Цифровая гигиена» для обучающихся 7—9 классов составлена в соответствии с:

- Федеральным государственным образовательным стандартом основного общего образования,
- Примерной рабочей программы учебного курса «Цифровая гигиена» основного общего образования, рекомендованной Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019). Самара,2019.
- Основной образовательной программы основного общего образования ГБОУ СОШ пос. Комсомольский, разработанная на основе ФГОС и ФОП.

Цель программы:

- формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков иугроз.

Задачи программы:

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации иее 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 формкоммуникации (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 решатьс помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведенияшкольников, связанного с компьютерными технологиями и Интернетом.

Место курса в учебном плане.

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

Курс рассчитан на 34 часа в год в 7,8,9 классах (по 1 часу в неделю).

В ГБОУ СОШ ПОС. Комсомольский в соответствии с положением о «Внеурочной деятельности» предусмотрено оценивание достижений обучающихся по системе « зачет-незачет». Форма промежуточной аттестации - в виде тестирования.

Планируемые результаты

Предметные:

Выпускник научится:

- ✓ анализировать доменные имена компьютеров и адреса документов в интернете;

- ✓ безопасно использовать средства коммуникации;
- ✓ безопасно вести и применять способы самозащиты при попытке мошенничества;
- ✓ безопасно использовать ресурсы интернета.

Выпускник овладеет:

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

Выпускник получит возможность овладеть:

- ✓ основами соблюдения норм информационной этики и права;
- ✓ основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
- ✓ использовать для решения коммуникативных задач в области безопасностижизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

Метапредметные.

Регулятивные универсальные учебные действия.

Обучающийся сможет:

- ✓ идентифицировать собственные проблемы и определять главную проблему;
- ✓ выдвигать версии решения проблемы, формулировать гипотезы, предвосхищатьконечный 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 технологиирешения 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.

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 частныхявлений к общим закономерностям;
- ✓ излагать полученную информацию, интерпретируя ее в контексте решаемойзадачи;
- ✓ самостоятельно указывать на информацию, нуждающуюся в проверке, предлагатьи применять способ проверки достоверности информации;

- ✓ критически оценивать содержание и форму текста;
- ✓ определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

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 послезавершения 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 вреальном 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 ипрофессиональных 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 поведенияв информационно-телекоммуникационной среде.

Содержание курса

Содержание программы курса соответствует темам основной образовательной программы основного общего образования (ООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

1 ВАРИАНТ

На изучение модуля 1 «Информационная безопасность» отводится по 1 часу в неделю в 7, 8, 9 классах.

Учебные занятия по программе реализованы по одному разделу последовательно в 7, 8 и 9 классах:

7 класс - раздел «Безопасность общения»,

8 класс – раздел «Безопасность устройств»,

9 класс – раздел «Безопасность информации».

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

Содержание программы 7 класс

Раздел 1 «Безопасность общения»

№	Тема	Кол-во часов	Характеристика основных видов деятельности
Тема 1. Общение в социальных сетях и мессенджерах.			
1.	Социальная сеть.	1	Выполняет базовые операции при использовании месседжеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2.	История социальных сетей.	1	
3.	Мессенджеры.	1	
4.	Назначение социальных сетей и мессенджеров.	1	
5.	Пользовательский контент.	1	
Тема 2. С кем безопасно общаться в интернете.			
6	Персональные данные как основной капитал личного пространства в цифровом мире.	1	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
7	Правила добавления друзей в социальных сетях.	1	
8	Профиль пользователя. Анонимные социальные сети.	1	
Тема 3. Пароли для аккаунтов социальных сетей.			
9	Сложные пароли. Онлайн генераторы паролей.	1	Изучает основные понятия регистрационной информации и шифрования. Умеет их применять.
10	Правила хранения паролей.	1	
11	Использованиефункции браузера по запоминанию паролей.	1	

Тема 4. Безопасный вход в аккаунты.			
12	Виды аутентификации	1	Объясняет причины безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.
13	Настройки безопасности аккаунта	1	
14	Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	1	
Тема 5. Настройки конфиденциальности в социальных сетях.			
15	Персональные данные.	1	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.
16	Настройки приватности и конфиденциальности в разных социальных сетях.	1	
17	Приватностьи конфиденциальность в мессенджерах.	1	
Тема 6. Публикация информации в социальных сетях.			
18	Публикация личной информации.	1	Осуществляет поиск и использует сетях. личной информации. информацию, необходимую для выполнения поставленных задач.
Тема 7. Кибербуллинг.			
19	Определение кибербуллинга.	1	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
20	Возможные причины кибербуллинга и как его избежать?	1	
21	Как не стать жертвой кибербуллинга.	1	
22	Как помочь жертве кибербуллинга.	1	
23	Настройки приватности публичных страниц.	1	
24	Правила ведения публичных страниц.	1	
25	Овершеринг.	1	
Тема 9. Фишинг.			
26	Фишинг как мошеннический прием.	1	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни.
27	Популярные варианты распространения фишинга.	1	
28	Отличие настоящих и фишинговых сайтов.	1	
29	Как защититься от фишеров в социальных сетях и мессенджерах.	1	
Выполнение и защита индивидуальных и групповых проектов.			
30-34	Выполнение проектной работы	5	Самостоятельная работа

8 класс

Раздел 2. «Безопасность устройств»

№	Тема	Кол-во часов	Формы проведения
Тема 1. Что такое вредоносный код.			
1	Виды вредоносных кодов.	1	Соблюдает технику безопасности при эксплуатации компьютерных систем.
2-3	Возможности и деструктивные функции вредоносных кодов.	2	
Тема 2. Распространение вредоносного кода			
4	Способы доставки вредоносных кодов.	1	Выявляет и анализирует возможные угрозы информационной безопасности объектов.
5-6	Исполняемые файлы и расширения вредоносных кодов.	2	
7-9	Вредоносная рассылка. Вредоносные скрипты.	3	
10-11	Способы выявления наличия вредоносных кодов на устройствах.	2	
12-14	Действия при обнаружении вредоносных кодов на устройствах.	3	
Тема 3. Методы защиты от вредоносных программ.			
15-17	Способы защиты устройств от вредоносного кода.	3	Изучает виды антивирусных программ и правила их установки.
18-20	Антивирусные программы и их характеристики.	3	
21-23	Правила защиты от вредоносных кодов.	3	
Тема 4. Распространение вредоносного кода для мобильных устройств.			
24-26	Расширение вредоносных кодов для мобильных устройств.	3	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.
27-29	Правила безопасности при установке приложений на мобильные устройства.	3	
Выполнение и защита индивидуальных и групповых проектов.			
30-34	Выполнение и защита индивидуальных и групповых проектов.	5	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

9 класс

Раздел 3. Безопасность информации

№	Тема	Кол-во часов	Формы проведения
Тема 1. Социальная инженерия: распознать и избежать			
1	Приемы социальной инженерии.	1	Находит нужную информацию в базах данных, составляя запросы на поиск.
2	**Правила безопасности при виртуальных контактах.**	1	
Тема 2. Ложная информация в Интернете. 1 час.			
3-4	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей.	2	Определяет возможные источники необходимых сведений, осуществляет поиск информации.
5-6	Фейковые новости.	2	
7-8	Поддельные страницы.	2	
Тема 3. Безопасность при использовании платежных карт в Интернете.			
9-10	Транзакции и связанные с ними риски.	2	Приводит примеры рисков, связанных с совершением онлайн, покупок.
11-12	Правила совершения онлайн покупок.	2	
13-14	Безопасность банковских сервисов.	2	
Тема 4. Беспроводная технология связи.			
15-16	Уязвимость Wi-Fi-соединений.	2	Используя различную информацию, определяет понятия.
17-18	Публичные и непубличные сети	2	
19-20	Правила работы в публичных сетях	2	
Тема 5. Резервное копирование данных.			
21-22	Безопасность личной информации.	2	Изучает особенности и стиль ведения личных и публичных аккаунтов. Создает резервные копии.
23-24	Создание резервных копий на различных устройствах.	2	
Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.			
25	Доктрина национальной информационной безопасности.	1	Умеет привести выдержки из законодательства РФ: обеспечивающего конституционное право на поиск, получение и распространение информации.
26	Обеспечение свободы и равенства доступа к информации и знаниям.	1	
27	Основные направления государственной политики в области формирования культуры информационной безопасности	1	

			Отражающего правовые аспекты защиты киберпространств
Выполнение и защита индивидуальных и групповых проектов.			
28-30	Выполнение и защита индивидуальных и групповых проектов.	3	**Самостоятельная работа**
31-32	Повторение	2	
33-34	Волонтерская практика.	2	

2 ВАРИАНТ

На изучение модуля 1 «Информационная безопасность» отводится по 1 часу в неделю в 8 и 9 классе

Учебные занятия по программе реализованы

8 класс - раздел «Безопасность общения» и «Безопасность устройств».
9 класс – раздел «Безопасность информации».
Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

8 класс

Раздел 1 «Безопасность общения»

№	Тема	Кол-во часов	Характеристика основных видов деятельности
Тема 1. Общение в социальных сетях и мессенджерах.			
1.	Социальная сеть. История социальных сетей.	1	Выполняет базовые операции при использовании месседжеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2.	Мессенджеры. Назначение социальных сетей и мессенджеров.	1	
3.	Пользовательский контент.	1	
Тема 2. С кем безопасно общаться в интернете.			
4	Персональные данные как основной капитал личного пространства в цифровом мире.	1	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
5	Правила добавления друзей в социальных сетях. **Профиль пользователя. Анонимные социальные сети.**	1	
Тема 3. Пароли для аккаунтов социальных сетей.			
6	Сложные пароли. Онлайн генераторы паролей.	1	Изучает основные понятия регистрационной информации и шифрования. Умеет их применять.
7	Правила хранения паролей. **Использованиефункции браузера по запоминанию паролей.**	1	
Тема 4. Безопасный вход в аккаунты.			
8	Виды аутентификации. Настройки безопасности аккаунта	1	Объясняет причины безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.
9	**Работа на чужом компьютере с точки зрения безопасности личного аккаунта.**	1	
Тема 5. Настройки конфиденциальности в социальных сетях.			
10	Персональные данные. Настройки приватности и конфиденциальности в разных	1	Раскрывает причины установки

	социальных сетях.		закрытого профиля. Меняет основные настройки приватности в личном профиле.
11	Приватностьи конфиденциальность в мессенджерах.	1	
Тема 6. Публикация информации в социальных сетях.			
12	Публикация личной информации.	1	Осуществляет поиск и использует сетях. личной информации. информацию, необходимую для выполнения поставленных задач.
Тема 7. Кибербуллинг.			
13	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать?	1	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
14	Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	1	
15	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	1	
Тема 9. Фишинг.			
16	Фишинг как мошеннический прием. Популярные варианты распространения фишинга.	1	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни.
17	Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	1	

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код.			
18	Виды вредоносных кодов. **Возможности и деструктивные функции вредоносных кодов.**	1	Соблюдает технику безопасности при эксплуатации компьютерных систем.
Тема 2. Распространение вредоносного кода			
19	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов.	1	Выявляет и анализирует возможные угрозы информационной безопасности объектов.
20	Вредоносная рассылка. Вредоносные скрипты.	1	
21	Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.	1	
Тема 3. Методы защиты от вредоносных программ.			
22-23	Способы защиты устройств от вредоносного кода.	2	Изучает виды антивирусных программ и правила их установки.
24-25	Антивирусные программы и их характеристики.	2	
26-27	Правила защиты от вредоносных кодов.	2	
Тема 4. Распространение вредоносного кода для мобильных устройств.			
28-29	Расширение вредоносных кодов для мобильных устройств.	2	Разрабатывает презентацию, инструкцию по обнаружению,
30	Правила безопасности при установке приложений на мобильные устройства.	1	

			алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.
Выполнение и защита индивидуальных и групповых проектов.			
30-34	Выполнение и защита индивидуальных и групповых проектов.	5	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

9 класс

Раздел 3. Безопасность информации

№	Тема	Кол-во часов	Формы проведения
Тема 1. Социальная инженерия: распознать и избежать			
1	Приемы социальной инженерии.	1	Находит нужную информацию в базах данных, составляя запросы на поиск.
2	**Правила безопасности при виртуальных контактах.**	1	
Тема 2. Ложная информация в Интернете. 1 час.			
3-4	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей.	2	Определяет возможные источники необходимых сведений, осуществляет поиск информации.
5-6	Фейковые новости.	2	
7-8	Поддельные страницы.	2	
Тема 3. Безопасность при использовании платежных карт в Интернете.			
9-10	Транзакции и связанные с ними риски.	2	Приводит примеры рисков, связанных с совершением онлайн, покупок.
11-12	Правила совершения онлайн покупок.	2	
13-14	Безопасность банковских сервисов.	2	
Тема 4. Беспроводная технология связи.			
15-16	Уязвимость Wi-Fi-соединений.	2	Используя различную информацию, определяет понятия.
17-18	Публичные и непубличные сети	2	
19-20	Правила работы в публичных сетях	2	

Тема 5. Резервное копирование данных.			
21-22	Безопасность личной информации.	2	Изучает особенности и стиль ведения личных и публичных аккаунтов. Создает резервные копии.
23-24	Создание резервных копий на различных устройствах.	2	
Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.			
25	Доктрина национальной информационной безопасности.	1	Умеет привести выдержки из законодательства РФ: обеспечивающего конституционное право на поиск, получение и распространение информации. Отражающего правовые аспекты защиты киберпространств
26	Обеспечение свободы и равенства доступа к информации и знаниям.	1	
27	Основные направления государственной политики в области формирования культуры информационной безопасности	1	
Выполнение и защита индивидуальных и групповых проектов.			
28-30	Выполнение и защита индивидуальных и групповых проектов.	3	Самостоятельная работа
31-32	Повторение	2	
33-34	Волонтерская практика.	2	

3 ВАРИАНТ

На изучение модуля 1 «Информационная безопасность» отводится по 1 часу в неделю в 9 классе

№	Тема	Основное содержание	Кол-во часов	Характеристика основных видов учебной деятельности обучающихся
Раздел 1. «Безопасность общения»				
1	Тема 1. Общение в социальных сетях и мессенджерах.	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	1	Выполняет базовые операции при использовании месседжеров и социальных сетей. Создает свой образ всети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2	Тема 2. С кем безопасно общаться в интернете.	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальныесети.	1	Руководствуется в общении социальными ценностями иустановками коллектива и общества в целом. Изучает правила сетевогообщения.
3	Тема 3. Пароли для аккаунтов социальных сетей.	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	1	Изучает основные понятия регистрационной информации и шифрования. Умеет их применять.
4	Тема 4. Безопасный вход в аккаунты.	Виды аутентификации. Настройки безопасности аккаунта. Работа начужом компьютере с точки зрения безопасности личного аккаунта.	1	Объясняет причины безопасного входа при работе на чужом устройстве.Демонстрирует устойчивый навык безопасного входа.
5	Тема 5.Настройки конфиденциальности в социальных сетях.	Настройки приватности и конфиденциальности в разныхсоциальных сетях. Приватность и конфиденциальность в мессенджерах.	1	Раскрывает причины установкизакрытого профиля. Меняет основныенастройки приватности в личномпрофиле.
6	Тема 6. Публикация информации в социальных сетях.	Персональныеданные. Публикация личной информации.	1	Осуществляет поиск и использует информацию, необходимую длявыполнения поставленных задач

7	Тема 7. Кибербуллинг.	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	1	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Тема 8. Публичные аккаунты.	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	1	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9-10	Тема 9. Фишинг.	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	2	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни.
11- 13	Выполнение и защита индивидуальных игрупповых проектов		3	Самостоятельная работа.
Раздел 2. «Безопасность устройств»				
14	Тема 1. Что такое вредоносный код	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	1	Соблюдает технику безопасности при эксплуатации компьютерных систем.
15	Тема 2. Распространение вредоносного кода.	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия	1	Выявляет и анализирует возможные угрозы информационной безопасности объектов.

		вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.		
16-17	Тема 3. Методы защиты от вредоносных программ.	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	2	Изучает виды антивирусных программ и правила их установки.
18	Тема 4. Распространение вредоносного кода для мобильных устройств.	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	1	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.
19-21	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
Раздел 3 «Безопасность информации»				
22	Тема 1. Социальная инженерия: распознать и избежать.	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	1	Находит нужную информацию в базах данных, составляя запросы на поиск.
23	Тема 2. Ложная информация в Интернете.	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	1	Определяет возможные источники необходимых сведений, осуществляет поиск информации.

24	Тема 3. Безопасность при использованииплатежных карт в Интернете.	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	1	Приводит примеры рисков, связанных с совершением онлайн, покупок.
25	Тема 4. Беспроводная технология связи.	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	1	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
26	Тема 5. Резервное копирование данных.	Безопасность личной информации. Создание резервных копий на различных устройствах.	1	Создает резервные копии.
27- 28	Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	2	Умеет привести выдержки из законодательства РФ: обеспечивающего конституционное право на поиск, получение и распространение информации. Отражающего правовые аспектызащиты киберпространства
29 - 31	Выполнение и защита индивидуальных игрупповых проектов		3	Самостоятельная работа
32 - 34	Повторение		3	
	Итого		34	

Модуль 2.

Формы проведения мероприятий для родителей: лектории, выступления на родительских собраниях, микрообучение на основе технологий онлайн-обучения, геймификация, создание чек-листов, совместное обучение, совместные родительско-детские проекты.

Тематическое планирование учебного курса (Модуль 2).

Тема 1. История возникновения Интернета. Понятия Интернетугроз. Изменения границ допустимого в контексте цифрового образа жизни

Тема 2. Изменения нормативных моделей развития и здоровья детей и подростков.

Тема 3. Цифровая гигиена: зачем это нужно? Понятие периметра безопасности. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка. Баланс ценностей развития и ценностей безопасности.

Тема 4. Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 5. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребѐнка дляпрофилактики насилия в Сети?

Тема 6. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта:быть или не быть?

Тема 7. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.

Тема 8. Пособия и обучающие программы по формированию навыков цифровой гигиены.

Список литературы

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш,Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019 – 432 с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б.Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 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 by Kaspersky // https://kids.kaspersky.ru/
8. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017 – 64 с.
9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение,2019 – 80 с.
10. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xnp1ai/index.php/glava-1- osnovy-kiberbezopasnosti-tseli-i-zadachi-kurs
11. 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.