

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство образования и науки Самарской области

**Кинельское управление Министерства образования и науки Самарской
области**

ГБОУ ООШ с. Парфеновка

« Рассмотрено»

Руководитель МО

_____/Зубкова Н.Н./

Протокол № 1

« 24 » августа 2023 г

«Проверено»

и.о. заместителя

директора по УВР

_____/ Орехова Е.И./

« 24 » августа 2023 г

« Утверждено»

Руководитель

ГБОУ ООШ с.Парфеновка

_____/Козлова В.В./

Приказ№ 65-од__от «24»
августа 2023 г

Рабочая программа

курса внеурочной деятельности

«Информационная безопасность»

для обучающихся 7-9 классов

Уровень образования: основной

Направление: Социальное

Форма организации: кружок

Количество часов(сроки реализации): 102часа (общее) , один год

Составитель: Овчинникова О..Н.
учитель истории

с.Парфёновка

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа курса «Информационная безопасность» адресована учащимся 7-9 классов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным, метапредметным и личностным результатам.

Цели:

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 ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Место курса в плане внеурочной деятельности

Программа учебного курса рассчитана на 34 учебных часа, на изучение отводится по 1 часу в неделю в каждом классе. Программа реализуется из части учебного плана внеурочной деятельности.

Режим занятий внеурочной деятельности регламентируется расписанием работы занятий внеурочной деятельности.

Учебно-методическое обеспечение.

- Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы: учеб. пособие для общеобразоват. организаций. - М.: Просвещение,
- Попов В.Б., Основы информационных и телекоммуникационных технологий. Мультимедиа : учеб. пособие / В.Б. Попов. - М. : Финансы и статистика,
- Морозов, Н. П., Чернокнижный, С. Б. Защита деловой информации для всех -СПб. : ИД «ВЕСЬ»,
- Касперский К. Записки исследователя компьютерных вирусов. – СПб.: Питер,

Планируемые результаты

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 ценности безопасного образа жизни;
- интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные результаты

В ходе изучения учебного курса обучающиеся усваивают опыт проектной деятельности и навыки работы с информацией, в том числе в текстовом, табличном виде, виде диаграмм и пр.

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;
- формулировать учебные задачи как шаги достижения поставленной цели деятельности;
- обосновывать целевые ориентиры и приоритеты ссылками на ценности, указывая и обосновывая логическую последовательность шагов;
- определять необходимые действие(я) в соответствии с учебной и познавательной задачей и составлять алгоритм их выполнения;
- обосновывать и осуществлять выбор наиболее эффективных способов решения учебных и познавательных задач;
- определять/находить, в том числе из предложенных вариантов, условия для выполнения учебной и познавательной задачи;
- выстраивать жизненные планы на краткосрочное будущее (заявлять целевые ориентиры, ставить адекватные им задачи и предлагать действия, указывая и обосновывая логическую последовательность шагов);
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- определять потенциальные затруднения при решении учебной и познавательной задачи и находить средства для их устранения;
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- определять совместно с педагогом и сверстниками критерии планируемых результатов и критерии оценки своей учебной деятельности;
- систематизировать (в том числе выбирать приоритетные) критерии планируемых результатов и оценки своей деятельности;
- отбирать инструменты для оценивания своей деятельности, осуществлять самоконтроль своей деятельности в рамках предложенных условий и требований;

- 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;
- устанавливать связь между полученными характеристиками продукта и характеристиками процесса деятельности и по завершении деятельности предлагать изменение характеристик процесса для получения улучшенных характеристик продукта;
- сверять свои действия с целью и, при необходимости, исправлять ошибки самостоятельно;
- определять критерии правильности (корректности) выполнения учебной задачи;
- анализировать и обосновывать применение соответствующего инструментария для выполнения учебной задачи;
- свободно пользоваться выработанными критериями оценки и самооценки, исходя из цели и имеющихся средств, различая результат и способы действий;
- оценивать продукт своей деятельности по заданным и/или самостоятельно определенным критериям в соответствии с целью деятельности;
- обосновывать достижимость цели выбранным способом на основе оценки своих внутренних ресурсов и доступных внешних ресурсов;
- фиксировать и анализировать динамику собственных образовательных результатов;
- наблюдать и анализировать собственную учебную и познавательную деятельность и деятельность других обучающихся в процессе взаимопроверки;
- соотносить реальные и планируемые результаты индивидуальной образовательной деятельности и делать выводы;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия

В результате освоения учебного курса обучающийся сможет:

- выделять общий признак двух или нескольких предметов или явлений, объяснять их сходство;
- объединять предметы и явления в группы по определенным признакам, сравнивать, классифицировать и обобщать факты и явления;
- 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;
- строить рассуждение на основе сравнения предметов и явлений, выделяя при этом общие признаки;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- вербализовать эмоциональное впечатление, оказанное на него источником;
- объяснять явления, процессы, связи и отношения, выявляемые в ходе познавательной и исследовательской деятельности (приводить объяснение с изменением формы представления; объяснять, детализируя или обобщая; объяснять с заданной точки зрения);
- делать вывод на основе критического анализа разных точек зрения, подтверждать вывод собственной аргументацией или самостоятельно полученными данными;
- переводить сложную по составу (многоаспектную) информацию из графического или формализованного (символьного) представления в текстовое, и наоборот;

-анализировать/рефлексировать опыт разработки и реализации учебного проекта, исследования (теоретического, эмпирического) на основе предложенной проблемной ситуации, поставленной цели и/или заданных критериев оценки продукта/результата;

-критически оценивать содержание и форму текста;

-определять необходимые ключевые поисковые слова и запросы;

-осуществлять взаимодействие с электронными поисковыми системами, словарями;

-формировать множественную выборку из поисковых источников для объективизации результатов поиска;

-соотносить полученные результаты поиска со своей деятельностью.

Коммуникативные универсальные учебные действия

В результате освоения учебного курса обучающийся сможет:

-определять возможные роли в совместной деятельности;

-играть определенную роль в совместной деятельности;

-принимать позицию собеседника, понимая позицию другого, различать в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории;

-определять свои действия и действия партнера, которые способствовали или препятствовали продуктивной коммуникации;

-строить позитивные отношения в процессе учебной и познавательной деятельности;

-корректно и аргументированно отстаивать свою точку зрения, в дискуссии уметь выдвигать контраргументы, перефразировать свою мысль (владение механизмом эквивалентных замен);

-критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;

-предлагать альтернативное решение в конфликтной ситуации;

-выделять общую точку зрения в дискуссии;

-договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;

-организовывать учебное взаимодействие в группе (определять общие цели, распределять роли, договариваться друг с другом и т. д.);

-устранять в рамках диалога разрывы в коммуникации, обусловленные непониманием/неприятием со стороны собеседника задачи, формы или содержания диалога;

определять задачу коммуникации и в соответствии с ней отбирать речевые средства;

отбирать и использовать речевые средства в процессе коммуникации с другими людьми (диалог в паре, в малой группе и т. д.);

-представлять в устной или письменной форме развернутый план собственной деятельности;

-соблюдать нормы публичной речи, регламент в монологе и дискуссии в соответствии с коммуникативной задачей;

-высказывать и обосновывать мнение (суждение) и запрашивать мнение партнера в рамках диалога;

-принимать решение в ходе диалога и согласовывать его с собеседником;

-создавать письменные «клишированные» и оригинальные тексты с использованием необходимых речевых средств;

-использовать вербальные средства (средства логической связи) для выделения смысловых блоков своего выступления;

-использовать невербальные средства или наглядные материалы, подготовленные/отобранные под руководством учителя;

-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.

Предметные результаты

Обучающийся научится:

-целеполаганию, включая постановку новых целей, преобразование практической задачи в познавательную;

-самостоятельно анализировать условия достижения цели на основе учета выделенных учителем ориентиров действия в новом учебном материале;

-уметь самостоятельно контролировать свое время и управлять им;

-учитывать разные мнения и стремиться к координации различных позиций в сотрудничестве;

-задавать вопросы, необходимые для организации собственной деятельности и сотрудничества с партнером;

-осуществлять взаимный контроль и оказывать в сотрудничестве необходимую взаимопомощь;

-давать определение понятиям;

-устанавливать причинно-следственные связи;

-осуществлять логическую операцию установления родовидовых отношений, ограничение понятия;

-обобщать понятия — осуществлять логическую операцию перехода от видовых признаков к родовому понятию, от понятия с меньшим объемом к понятию с большим объемом;

-строить логическое рассуждение, включающее установление причинно-следственных связей;

-осуществлять информационное подключение к локальной сети и глобальной сети Интернет;

входить в информационную среду ОО, в том числе через Интернет, размещать в информационной среде различные информационные объекты;

-выводить информацию на бумагу, правильно обращаться с расходными материалами; соблюдать требования техники безопасности, гигиены, эргономики и ресурсосбережения при работе с устройствами ИКТ, в частности учитывающие специфику работы с различными экранами;

-находить в тексте требуемую информацию (пробежать текст глазами, определять его основные элементы, сопоставлять формы выражения информации в запросе и в самом тексте, устанавливать, являются ли они тождественными или синонимическими, находить необходимую единицу информации в тексте).

Форма промежуточной аттестации: тестирование.

**Содержание курса внеурочной деятельности
«Информационная безопасность»
с указанием форм организации и видов деятельности**

5 класс

«Сеть интернет»

Тема 1. Введение

Что такое информационное общество?

Тема 2. Пространство Интернета на планете Земля

История создания сети Интернет. Что такое Всемирная паутина? Путешествие по сети Интернет: сайты и электронные сервисы. Как стать пользователем Интернета? Опасности для пользователей Интернета. Что такое кибератака. Что такое информационная безопасность. Законы о защите личных данных в Интернете. Сетевой этикет. Коллекции сайтов для детей. Электронные музеи

Тема 3. Правила для пользователей сети Интернет

Правила работы с СМС. Правила работы с электронной почтой. Правила работы с видеосервисами. Правила работы в социальных сетях. Правила защиты от вирусов, спама, рекламы и рассылок. Правила защиты от негативных сообщений. Правила общения в социальной сети. Правила работы с поисковыми системами и анализ информации. Правила ответственности за распространение ложной и негативной информации. Правила защиты от нежелательных сообщений и контактов. Правила вызова экстренной помощи. Правила защиты устройств от внешнего вторжения. Правила выбора полезных ресурсов в Интернете. Средства работы в Интернете для людей с особыми потребностями.

Тема 4. Выполнение и защита индивидуальных и групповых проектов

Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи, SMART. Защита проекта.

Формы-виды проведения занятий:

Беседа. Игра

Урок – путешествие

Практические занятия

Викторины

Путешествия

Проекты (индивидуальные и групповые)

6 класс

**«Безопасность
общения»**

1. Общение в социальных сетях и мессенджерах

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

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 социальные сети.

3. Пароли для аккаунтов социальных сетей

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

4. Безопасный вход в аккаунты

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

5. Настройки конфиденциальности в социальных сетях

Настройки приватности и конфиденциальности в разных социальных сетях.

Приватность и конфиденциальность в мессенджерах.

6. Публикация информации в социальных сетях

Персональные данные. Публикация личной информации.

7. Кибербуллинг

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать?

Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

8. Публичные аккаунты

Настройки приватности публичных страниц. Правила ведения публичных страниц.

Овершеринг.

9. Фишинг

Фишинг как мошеннический прием. Популярные варианты распространения фишинга.

Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

10. Выполнение и защита индивидуальных и групповых проектов

Формы-виды проведения занятий:

Беседа. Игра

Урок – путешествие

Практические занятия

Викторины

Путешествия

Проекты (индивидуальные и групповые)

7 класс

«Безопасность устройств»

1. Что такое вредоносный код

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

2. Распространение вредоносного кода

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.

3. Методы защиты от вредоносных программ

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

4. Распространение вредоносного кода для мобильных устройств

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

5. Выполнение и защита индивидуальных и групповых проектов

6. Повторение.

Формы-виды проведения занятий:

Беседа. Игра

Урок – путешествие

Практические занятия

Викторины

Путешествия

Проекты (индивидуальные и групповые)

8 класс

«Безопасность информации»

1. Социальная инженерия: распознать и избежать

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

2. Ложная информация в Интернете

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

3. Безопасность при использовании платежных карт в Интернете

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

4. Беспроводная технология связи

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

5. Резервное копирование данных

Безопасность личной информации. Создание резервных копий на различных устройствах.

6. Выполнение и защита индивидуальных и групповых проектов

7. Повторение.

Формы-виды проведения занятий:

Беседа. Игра

Урок – путешествие

Практические занятия

Викторины

Путешествия

Проекты (индивидуальные и групповые)

9 класс

«Информационная безопасность. Цифровая гигиена»

1. Безопасность общения.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Настройки приватности и конфиденциальности в разных социальных сетях.

Приватность и конфиденциальность в мессенджерах.

Персональные данные. Публикация личной информации.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

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

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.

2. Безопасность устройств.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

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.

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

Правила безопасности при установке приложений на мобильные устройства.

3. Безопасность информации.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей.

Фейковые новости. Поддельные страницы.

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

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

Безопасность личной информации. Создание резервных копий на различных устройствах.

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

Формы организации и виды деятельности: работа с Интернет- ресурсами,презентации, проекты.

Тематическое планирование

5 класс (34 часа)

№ занятия	Тема	Кол-во часов
1	Введение	1
2	Пространство Интернета на планете Земля	14
3	Правила для пользователей сети Интернет	15
4	Выполнение и защита индивидуальных и групповых проектов	4
Итого		34

6 класс (34 часа)

№ занятия	Тема	Кол-во часов
1	Общение в социальных сетях и мессенджерах	4
2	С кем безопасно общаться в интернете	3
3	Пароли для аккаунтов социальных сетей	4
4	Безопасный вход в аккаунты	3
5	Настройки конфиденциальности в социальных сетях	4
6	Публикация информации в социальных сетях	3
7	Кибербуллинг	3
8	Публичные аккаунты	2
9	Фишинг	3
10	Выполнение теста.	1
11	Обсуждение тем индивидуальных и групповых проектов	1
12	Выполнение и защита индивидуальных и групповых проектов	3
Итого		34

7 класс (34 часа)

№ занятия	Тема	Кол-во часов
1	Что такое вредоносный код	5
2	Распространение вредоносного кода	5
3	Методы защиты от вредоносных программ	5
4	Распространение вредоносного кода для мобильных устройств	5
5	Подготовка к итоговому тесту	1
6	Выполнение теста	1
7	Работа над ошибками	1
8	Обсуждение тем индивидуальных и групповых проектов	2
9	Выполнение и защита индивидуальных и групповых проектов	5
10	Повторение	4
Итого		34

8 класс (34 часа)

№ занятия	Тема	Кол-во часов
1	Социальная инженерия: распознать и избежать	4
2	Ложная информация в Интернете	6
3	Безопасность при использовании платежных карт в Интернете	4
4	Беспроводная технология связи	4
5	Резервное копирование данных	4
6	Подготовка к итоговому тесту	1
7	Выполнение теста	1
8	Обсуждение тем индивидуальных и групповых проектов	2
9	Выполнение и защита индивидуальных и групповых проектов	4
10	Повторение	4
Итого		34

9 класс (34 часа)

№ занятия	Тема	Кол-во часов
1	Безопасность общения	12
2	Безопасность устройств	8
3	Безопасность информации	10
4	Выполнение и защита индивидуальных и групповых проектов	4
Итого		34

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

5	Настройки Конфиденциальност и в социальных сетях	1	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.
---	--	---	--	---

6	Публикация информации в социальных сетях	2	Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
7	Кибербуллинг	1	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	2	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9	Фишинг	2	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.

Тема 2. «Безопасность устройств»

1	Что такое вредоносный код	1	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
---	---------------------------	---	--	---

2	Распространение вредоносного кода	1	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.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
3	Методы защиты от вредоносных программ	2	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов	Изучает виды антивирусных программ и правила их установки.
4	Распространение вредоносного кода для мобильных устройств	1	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.

5	Выполнение и защита индивидуальных и групповых проектов	3		Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.
---	---	---	--	---

Тема 3 «Безопасность информации»

1	Социальная инженерия: распознать и избежать	2	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
---	---	---	--	--

2	Ложная информация в Интернете	2	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам.
3	Безопасность при использовании платежных карт в Интернете	1	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.

4	Беспроводная технология связи	1	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
5	Резервное копирование данных	2	Безопасность личной информации. Создание резервных копий на различных устройствах.	Создает резервные копии.
6	Основы государственной политики в области формирования культуры информационной Безопасности	2	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации;

			Формирования культуры информационной безопасности.	- отражающего правовые аспекты защиты киберпространства.
7	Выполнение и защита индивидуальных и групповых проектов	4	Темы проектов Безопасность общения Безопасность устройств Безопасность общения	Уметь выполнять проекты Защита проектов
	Итого	34		