Бюджетное общеобразовательное учреждение г Омска
«Средняя общеобразовательная школа №162»

РАБОЧАЯ ПРОГРАММА

по курсу внеурочной деятельности

«Информационная безопасность»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Курс разработан в соответствии с требованиями Федерального государственного образовательного стандарта основного общего образования. Он направлен на повышение цифровой грамотности школьников: на уроках курса «Информационная безопасность» обучающиеся знакомятся с разными возможностями Интернета, учатся вовремя распознавать онлайн-риски (технические, контентные, коммуникационные, потребительские и риск интернет-зависимости), успешно разрешать проблемные ситуации в Сети, защищать свои персональные данные и управлять ими.

Цели курса ««Информационная безопасность» — формирование цифровой компетентности школьников и расширение возможностей полезного, критичного, ответственного и безопасного использования Интернета.

Данный курс предполагает решение следующих задач:

- расширить у обучающихся 5–9 классов диапазон возможностей, связанных с использованием цифровых технологий;
- способствовать осознанию школьниками влияния, которое цифровые технологии оказывают на их образ жизни;
- расширить представления обучающихся о возможностях Интернета как источника информации, инструмента коммуникации и потребления;
- познакомить обучающихся с возможными онлайн-рисками (техническими, контентными, коммуникационными, потребительскими и риском интернет-зависимости);
- способствовать формированию устойчивых стратегий своевременного распознавания онлайн-рисков и безопасного поведения при столкновении с ними, сформировать навыки успешного разрешения проблемных ситуаций в Сети, защиты своих персональных данных и управления ими;
- способствовать формированию у обучающихся адекватного образа цифровых технологий, предполагающего, с одной стороны, понимание их позитивной роли в развитии человеческой цивилизации, а с другой — критическую оценку влияния цифровых технологий на разные стороны жизнедеятельности человека;
- способствовать формированию критического мышления, творческого мышления и креативности, способности к рефлексии, навыков сотрудничества. Курс внеурочной деятельности ««Информационная безопасность» реализуется за пять лет обучения из расчёта 1 час в неделю (34 часа в год).

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА

Курс позволяет формировать универсальные учебные действия (УУД) в соответствии с требованиями Федерального государственного образовательного стандарта основного общего образования.

К ***регулятивным УУД*** относятся сформированные у обучающихся в результате освоения данного курса умение ставить цели, задачи, планировать их реализацию и выбирать эффективные пути их достижения; умение выбирать оптимальные способы разрешения проблемных ситуаций, возникающих при использовании Интернета, что особенно важно при осуществлении деятельности, направленной на обеспечение личной безопасности в Интернете.

К ***коммуникативным УУД*** в контексте данного курса относятся умение учитывать мнение других пользователей при взаимодействии с ними в онлайн-среде; стремление к кооперации, компромиссу, конструктивному взаимодействию; умение устанавливать контакт в онлайн-общении; умение конструктивно разрешать конфликтные ситуации (выявлять, идентифицировать проблемы, искать и оценивать способы разрешения конфликта, принимать решения и реализовывать их); умение планировать взаимодействие (определять цели, способы взаимодействия) с учётом особенностей онлайн-коммуникации.

В рамках курса формируются такие ***познавательные УУД***, как умение формулировать познавательную цель при пользовании Интернетом и цифровыми технологиями; умение искать информацию; умение анализировать информацию с целью выделения существенных и несущественных признаков; умение синтезировать информацию; умение критически оценивать достоверность информации; умение выбирать основания и критерии для сравнения информации, устанавливать причинно-следственные связи, выстраивать логические цепи рассуждений, выдвигать гипотезы и обосновывать их.

По итогам освоения курса у обучающихся должен появиться ***опыт учебно-исследовательской*** и ***проектной деятельности*** в онлайн-среде. У обучающихся возникнут познавательные интересы в области цифровых технологий.

Курс позволяет решать ряд ***воспитательных задач***. Он обеспечивает наличие у обучающихся знаний основных прав и обязанностей пользователя Интернета в соответствии с законами РФ. Обучающиеся должны научиться ориентироваться в системе моральных норм и ценностей, а также в особенностях взаимоотношений и культуры поведения в онлайн-среде. Обучающиеся осваивают культуру общения в Интернете, учатся способствовать формированию культуры поведения в онлайн-среде среди сверстников. Обучающиеся смогут оценивать поступающую онлайн-информацию, исходя из нравственных и этических норм. Они смогут проводить рефлексию своей деятельности и осознают ответственность за результаты этой деятельности.

В процессе освоения курса у обучающихся формируется доброжелательное отношение к другим пользователям Интернета, нетерпимость к любым формам агрессивного и противоправного поведения в Интернете и готовность противостоять им, а также уважение к общечеловеческим ценностям, готовность к распространению их в онлайн-среде. У обучающихся развивается потребность в личностном росте, самореализации в соответствии с ценностями и нормами, в том числе в онлайн-среде, чему способствуют разработка, реализация и участие в различных социальных проектах, а также в других видах деятельности, предлагаемых в рамках курса. Обучающиеся осознают смысл овладения цифровыми технологиями.

Формируются также готовность и способность к участию в различных видах онлайн-деятельности, направленных на личностное развитие; осознанное стремление соответствовать социально одобряемым нормам поведения по отношению к взрослым и сверстникам в различных онлайн-контекстах. У школьников появляется потребность участвовать в онлайн-деятельности, способствующей личностному развитию.

Во время изучения внеурочного курса «Кибербезопасность» формируются ***ИКТ-компетенции***: умение строить поисковые запросы в онлайн-источниках и находить релевантную информацию; умение анализировать, сопоставлять, обобщать, интерпретировать и систематизировать информацию, оценивать её достоверность; умение сохранять и передавать информацию, в том числе в форме гипермедиа (текст, изображение, звук, ссылки между разными информационными компонентами), при соблюдении правил кибербезопасности. Приобретённые компетенции позволят более эффективно осваивать программы других учебных курсов.

Курс состоит из семи смысловых модулей, которые представлены в каждом классе. Работа над каждым модулем способствует формированию определённого набора компетенций.

Модуль 1. Цифровой мир и интернет-зависимость. Формируются способность и готовность к ***осознанному, ответственному и безопасному освоению и использованию Интернета и цифровых устройств,*** а именно способность и готовность:

- ответственно выбирать оптимальные и безопасные пути освоения цифровых технологий, Интернета и цифровых устройств;
- понимать и адекватно использовать возможности, предоставляемые Интернетом и цифровыми технологиями, в соответствии с этическими нормами и текущим законодательством РФ;
- понимать и адекватно оценивать риски, возникающие в процессе освоения Интернета и цифровых технологий; находить оптимальные способы решения проблем, возникающих в процессе освоения Интернета и цифровых технологий;

- оценивать количество личного времени, проводимого за использованием Интернета и цифровых устройств, и качество содержательного наполнения этого времени;
- ответственно и сбалансированно распределять личное время, в том числе отводимое на использование цифровых технологий;
- оценивать наличие признаков чрезмерного использования Интернета и цифровых устройств;
- находить адекватные, оптимальные пути решения проблемы чрезмерного использования Интернета и цифровых устройств.

Модуль 2. Техносфера и технические риски. Формируются способность и готовность к ***ответственному и безопасному использованию средств подключения к Интернету и программного обеспечения, связанного с работой в Интернете***, а именно способность и готовность:

- ответственно и безопасно использовать различные способы подключения к Интернету и возможности их настройки в соответствии с текущими задачами, а также осваивать новые средства связи;
- ответственно и безопасно использовать современное программное обеспечение для работы в Интернете и возможности их настройки в соответствии с текущими задачами, а также осваивать новое программное обеспечение;
- ответственно и безопасно относиться к конфиденциальности личных данных в Интернете и уметь защищать их от несанкционированного доступа;
- ответственно и безопасно использовать программные средства для защиты технических устройств от вирусов;
- оценивать основные риски, связанные с различными способами подключения к Сети, использованием локальных и облачных приложений для работы в Интернете, аутентификацией в Интернете, использованием антивирусных средств для защиты технических устройств.

Модуль 3. Информация и контентные риски. Формируются способность и готовность ***ответственно и безопасно обращаться с информацией в Интернете (искать, оценивать, создавать, размещать, потреблять и распространять информационный контент)***, а именно способность и готовность:

- ответственно и безопасно использовать различные поисковые системы и их возможности для поиска в Интернете информации, необходимой для решения различных жизненных задач, в том числе образовательных; оценивать качество информации и информационных ресурсов в Интернете, в том числе их достоверность, надёжность, безопасность, а также потенциальные риски, связанные с их использованием и распространением;
- ответственно и безопасно использовать различные интернет-ресурсы для создания и размещения в Интернете оригинальной позитивной информации (мультимедиа, текстов, сайтов и т. д.);
- ответственно и безопасно потреблять и распространять информацию в соответствии с этическими нормами, текущим законодательством РФ в области авторского права и защиты детей от информации, причиняющей вред их здоровью и развитию;
- оценивать основные риски использования информации в Интернете, связанные с поиском и оценкой достоверности и надёжности информации, созданием и размещением информационного контента, распространением в Сети противозаконной информации, угрожающей здоровью и развитию детей и подростков.

Модуль 4. Общение и коммуникационные риски. Формируются способность и готовность ***использовать ресурсы Интернета для ответственной и безопасной коммуникации***, а именно способность и готовность:

- ответственно и безопасно взаимодействовать с другими пользователями на различных интернет-ресурсах (в социальных сетях) в соответствии с общечеловеческими нормами поведения, текущим законодательством РФ, правилами конкретного интернет-ресурса, а также в зависимости от оценки сложившейся ситуации;

- ответственно и безопасно выбирать стратегии коммуникации, в том числе самопрезентации, на различных интернет-ресурсах (в социальных сетях) в зависимости от вида ресурса, целей коммуникации и целевой аудитории;
- ответственно и безопасно управлять собственной репутацией (формировать, поддерживать, защищать) и социальным капиталом в Интернете;
- адекватно оценивать риски, возникающие в процессе коммуникации в Интернете (в случае встречи с незнакомцами, проявления агрессии и т. д.), а также выбирать безопасные стратегии поведения в ситуациях, связанных с этими рисками;
- ответственно и безопасно выбирать стратегии поведения при столкновении с проявлениями агрессии (с троллингом, кибербуллингом и т. д.) в Интернете.

Модуль 5. Цифровая экономика и потребительские риски. Формируются способность и готовность ***ответственно и безопасно потреблять товары и услуги***, представленные на различных интернет-ресурсах, в соответствии с текущим законодательством РФ и правами потребителей, а именно с пособность и готовность: использовать различные интернет-ресурсы для поиска информации о необходимых товарах и услугах;

- оценивать качество продуктов, предоставляемых на различных интернет-ресурсах, а также потенциальные риски, связанные с их потреблением;
- оценивать достоверность информации, представленной на раз-личных рекламных носителях в Интернете;
- ответственно и безопасно использовать интернет-ресурсы, соблюдая пользовательские соглашения и общие правила безопасности;
- изучать и реализовывать права потребителей в соответствии с текущим законодательством РФ;
- оценивать основные потребительские риски, связанные с приобретением и потреблением товаров и услуг, представленных на различных интернет-ресурсах, распространением рекламы в Интернете, различными видами мошенничества в Интернете (в том числе фишингом), различными видами онлайн-игр (многопользовательских, социальных, каузальных).

Модуль 6. Персональные данные. Формируются способность и готовность ***самостоятельно, в соответствии с актуальными жизненными задачами, защищать персональные данные с помощью технических и программных приёмов и средств, устанавливать границы собственной приватно сти и управлять репутацией в Сети***, а именно способность и готовность:

- различать виды персональных данных и понимать последствия небрежного обращения с ними, способы их попадания в Интернет и дальнейшего распространения в Сети;
- уметь пользоваться различными средствами управления персональными данными и приватностью в Интернете;
- ответственно и безопасно использовать методы защиты конфиденциальных персональных данных от несанкционированного доступа;
- ответственно и безопасно использовать специальные безопасные режимы работы в браузерах;
- ответственно и безопасно использовать приёмы, позволяющие контролировать распространение персональных данных в Интернете, а также удалять следы онлайн-активности с различных устройств и онлайн-ресурсов;
- ответственно и безопасно использовать настройки приватности в социальных сетях и на других онлайн-ресурсах;
- ответственно и безопасно использовать механизмы обращения в службу технической поддержки разработчиков устройств, приложений, онлайн-ресурсов, в общественные и государственные организации; оценивать основные риски, связанные с предоставлением и распространением персональных данных.

Модуль 7. Цифровое будущее. Формируются ***позитивный образ цифровых технологий и цифрового будущего, активная субъектная позиция и ценностное отношение к личному***

будущему, а также способность и готовность к конструктивной социализации в условиях цифрового общества, что выражается в способности и готовности:

- разбираться в изменениях, которые происходят в технологи-ческой и социальной сферах;
- понимать, адекватно и ответственно использовать возможности, которые появляются благодаря новым технологиям;
- понимать и адекватно оценивать риски, возникающие вследствие изменений в технологической и социальной сферах;
- находить личные жизненные ориентиры, соответствующие нравственным и этическим нормам;
- создавать и планировать жизненный план в условиях цифрового общества и с учётом происходящих изменений;
- реализовывать личностный потенциал в условиях цифрового общества;
- выбирать и планировать адекватный и оптимальный путь реализации личностного потенциала и жизненного плана в условиях цифрового общества и с учётом происходящих изменений.

СОДЕРЖАНИЕ КУРСА

5 КЛАСС

- **Тема 1. Зачем нам нужен Интернет**
  - Создание современного Интернета. Тим Бернерс Ли. Всемирная паутина. Новые возможности Интернета в осуществлении традиционных социально-культурных практик. Типы интернет-пользователей. Проблема интернет-зависимости. Сбалансированный распорядок дня.
- **Тема 2. Как устроен Интернет**
  - Компьютерная программа. Первая в мире компьютерная программа. Браузер. Программное обеспечение, софт. Профессия программист. Техносфера. Виды цифровых устройств. Три кита Интернета: «железо», софт, сети. Компьютерные вирусы. Правила защиты цифрового устройства от компьютерных вирусов.
- **Тема 3. Какая бывает информация**
  - Что такое информация. Цифровая информация. Контент. Ценность информации. Каналы восприятия информации. Возможности использования каналов восприятия информации в Интернете. Единицы измерения цифровой информации. Формы представления цифровой информации в Интернете.
- **Тема 4. Как работает поиск в Интернете**
  - Поиск информации. Поисковая система. Полезные ресурсы в Интернете. Контентные риски: столкновение с неприятным онлайн-контентом. Способы защиты от контентных рисков: настройки безопасного поиска и кнопка «пожаловаться на контент».
- **Тема 5. Как люди общаются в Интернете**
  - Сервисы для общения в Интернете. Возможности общения в Интернете. Рэй Томлинсон. Первое в мире электронное сообщение. Плюсы и минусы цифрового общения. Правила онлайн-общения.
- **Тема 6. Как совершать покупки в Интернете**
  - Цифровая экономика. Реальные и виртуальные товары. Первый в мире интернет-магазин. Критерии надёжности интернет-магазина. Плюсы и минусы интернет-магазинов. Баннеры, реклама. Правила безопасности при совершении покупок в Интернете.

- **Тема 7. Что такое персональные данные**
  - Общедоступная и персональная информация. Персональные данные. Виды персональных данных.
- **Тема 8. Какие следы мы оставляем в Интернете**
  - Виды персональных данных, выкладываемых в открытый доступ. Риски размещения персональной информации в открытом доступе. Настройки приватности.
- **Тема 9. Урок в школе будущего**
- Современные технологии, используемые в процессе обучения.

- 6 КЛАСС

- **Тема 1. Мы в цифровом мире**
  - Информационные революции, история средств связи. Функции и роль Интернета в повседневной жизни. Возможности и риски, связанные с Интернетом. Интернет-зависимость. Варианты организации свободного времени без использования гаджетов и Интернета.
- **Тема 2. Почему важны пароли в Интернете**
  - История паролей. Всемирный день пароля. Аккаунт, логин, пароль, аутентификация, авторизация. Способы защиты аккаунта (пароль, отпечаток пальца, одноразовый код, USB-ключ, двухфакторная аутентификация). Правила безопасности при защите аккаунта (создание, использование и хранение надёжных паролей). Алгоритмы создания паролей.
- **Тема 3. Полезные интернет-ресурсы**
  - Виды информационных ресурсов. Что такое контент. Контент в Интернете. Полезные онлайн-ресурсы. Цифровые образовательные ресурсы. Контентные риски. Способы защиты от нежелательного контента в Интернете.
- **Тема 4. Как искать и распознавать правдивую информацию** Потребность в информации. Информационная социализация. Инструменты для быстрого поиска в Интернете. Достоверность информации. Что такое фейк. Пост и репост в социальной сети. Способы определения достоверности информации.
- **Тема 5. Как общаться в Интернете**
  - Самопрезентация. Особенности самопрезентации в Интернете. Общение в Интернете. История смайлика. Преимущества и недостатки общения в Интернете. Вербальное и невербальное общение. Эмодзи. Особенности передачи и восприятия информации, выраженной при помощи смайликов и эмодзи и при помощи текста. Уместное и неуместное использование смайликов и эмодзи в онлайн-общении.
- **Тема 6. Как избежать конфликтов в Интернете**
  - Агрессивное и неагрессивное общение. Причины агрессии в Интернете. Правила безопасности при общении в Интернете. Троллинг. Стратегии поведения при столкновении с троллингом. Пути решения проблемы агрессии в Интернете. Возможности бесконфликтного общения в Интернете. Способы поддержки человека, столкнувшегося с агрессией в Интернете. Флешмобы. Правила бесконфликтного общения в Интернете.
- **Тема 7. Как не попасться на удочку онлайн-мошенникам**
  - Цифровая экономика. Преимущества и риски покупок онлайн. Интернет-мошенничество. Фишинг. Виды интернет-мошенничества и их последствия. Спам. Способы защиты от спама. СМС-мошенничество. Способы защиты от интернет- и СМС-мошенничества.
- **Тема 8. Что такое персональные данные**
  - Персональные данные. Публичная и персональная информация. Идентификатор личности. Виды персональных данных.

- **Тема 9. Что нужно знать о цифровых следах**
  - Цифровой след. Понятие приватности. Настройки приватности в цифровых устройствах. Виды кодов (линейный штрихкод и QR-код). Источники приватных сведений о человеке. Рекомендации по управлению приватностью в Интернете.
- **Тема 10. Дома будущего**
  - Новшества в архитектуре и строительстве, связанные с цифровыми технологиями. Применение цифровых технологий в быту.

- 7 КЛАСС

- **Тема 1. Как не заблудиться в Интернете**
  - Место Интернета в жизни современного человека. Домен и доменное имя. Виды доменов. Требования к доменным именам. Проблема интернет-зависимости. Всплывающие уведомления. Профилактика чрезмерной увлечённости Интернетом.
- **Тема 2. Как безопасно подключаться к Интернету**
  - Способы подключения к Интернету. Проводное и беспроводное соединение. Правила безопасности при беспроводном подключении к Интернету. Правила и алгоритмы составления надёжного пароля.
- **Тема 3. Как искать полезную информацию в Интернете**
  - Потребность в информации как одна из базовых потребностей человека. Контент сайта. Механизм работы поисковых систем. Возможности и правила поиска в поисковых системах Google и Яндекс. Функция «поиск по картинке». Информационная перегрузка.
- **Тема 4. Почему нужно проверять информацию в Интернете**
- Достоверная и недостоверная информация. Фейковые новости.
- Признаки недостоверной, фейковой информации.
- **Тема 5. Человек в Интернете: реальный или виртуальный?**
  - Способы общения в Интернете. Форумы, чаты, мессенджеры. «Друзья» в социальных сетях и Интернете. Аватар — «лицо» человека в Интернете. Механизм формирования образа человека в Интернете. Риски общения с незнакомцами в Интернете. Правила безопасного общения с интернет-друзьями.
- **Тема 6. Как противостоять агрессии в Интернете**
  - Агрессия и конфликты в Интернете. Троллинг. Действия по профилактике агрессивного поведения в Интернете. Действия при столкновении с агрессией в Интернете.
- **Тема 7. Как безопасно совершать покупки в Интернете**
  - Цифровая экономика. Покупки в Интернете. Риски онлайншопинга. Правила безопасности при совершении покупок онлайн.
- **Тема 8. Как персональные данные оказываются в Сети**
  - Персональные данные. Конфиденциальность. Цифровые следы. Способы попадания персональных данных в Сеть. Куки-файлы. Правила защиты персональных данных. Режим инкогнито. Три кита защиты персональных данных: надёжные пароли, настройки приватности, управление персональными данными.
- **Тема 9. Для чего нужно управлять персональными данными**
  - Значимость персональных данных. Способы управления персональными данными в Интернете. Рекомендации по предотвращению кражи персональных данных.
- **Тема 10. Цифровой мир будущего**
  - Интернет вещей. Цифровые технологии и предметы повседневного пользования.

- 8 КЛАСС

- **Тема 1. Другая реальность — дополненная и виртуальная**
  - Виртуальная реальность. Дополненная реальность. История развития технологий виртуальной и дополненной реальности. Применение виртуальной и дополненной реальности в разных сферах жизни. Видеоигры. Зависимость от видеоигр. Профилактика зависимости от видеоигр.
- **Тема 2. Защита от вредоносных программ**
  - Вредоносные программы: мифы и реальность. Компьютерный вирус. Виды вредоносных программ. Троянская программа. Способы защиты от технических рисков.
- **Тема 3. Как стать мастером поиска в Интернете**
  - Команды быстрого поиска в Интернете. Возможности строки поиска для решения математических задач. Нежелательный контент.
- Способы борьбы с нежелательным контентом.
- **Тема 4. Фейки в Интернете: как их распознать**
  - Фейковые новости. Фактчекинг. Признаки фейковых новостей. Способы определения фейковых видео и фотографий. База знаний Wolfram Alpha. Критерии оценки достоверности информации.
- **Тема 5. Репутация в Интернете: как её сохранить**
  - Репутация и самопрезентация в Интернете и офлайн. Риски, сопряжённые с самопрезентацией в Интернете. Негативное и положительное влияние поведения в Интернете на репутацию в жизни офлайн. Управление репутацией.
- **Тема 6. Агрессия в Сети: способы предотвращения**
  - Проявление агрессии в Интернете. Влияние столкновения с агрессией в Сети на пользователей. Профилактика агрессии в Сети. Технические средства защиты от агрессии в Сети. Социальная реклама. Правила безопасного общения в Интернете.
- **Тема 7. Электронные платежи: правила безопасности**
  - История денег. Банковские онлайн-операции. Интернет-платежи. Цифровая экономика. Платёжные карты. Виртуальные деньги. Криптовалюты. Риски при осуществлении интернет-платежей. Правила безопасности при осуществлении покупок в Интернете.
- **Тема 8. Персональные данные в Сети: как их защитить**
  - Государственный контроль над защитой персональных данных, Роскомнадзор. Сайт «Персональныеданные.дети». Федеральный закон «О персональных данных», персональные данные, оператор персональных данных, обработка персональных данных. Виды персональных данных. Признаки надёжного пароля. Способы создания надёжного пароля. Как пароли попадают к мошенникам. Правила хранения и защиты паролей.
- **Тема 9. Оберегаем личное пространство в Интернете**
  - Приватность. Личное пространство. Личные границы. Зоны общения. Распределение персональных данных по зонам общения. Шкала «открытости-закрытости». Тест на степень открытости в Интернете. Настройки приватности в социальных сетях. Рекомендации по настройкам приватности в социальных сетях.
- **Тема 10. Профессии будущего**
  - Цифровые технологии и профессии. Изменения в мире профессий. Новые профессии, связанные с цифровыми технологиями.

- 9 КЛАСС

- **Тема 1. Искусственный интеллект: что нас ждёт в будущем?**

- Искусственный интеллект, машинное обучение, нейросети, глубокое обучение. Применение искусственного интеллекта в различных сферах жизни. Тест Тьюринга. Чат-боты. Положительные и отрицательные последствия внедрения технологий искусственного интеллекта.

- **Тема 2. Как безопасно искать и хранить информацию в Интернете**

- Браузер. Возможности и недостатки разных браузеров. Функции браузеров: сохранение паролей, сохранение истории посещений, запоминание введённых данных, функция защиты от фишинга и вредоносного программного обеспечения, управление всплывающими окнами, управление информацией о местоположении пользователя, управление доступом к камере и микрофону, управление загрузкой файлов. Облачные программы, облачные сервисы, облачные приложения для учёбы. Минусы и плюсы облачных и локальных сервисов.

- **Тема 3. Как увидеть правду в море лжи**

- Постправда. Фейковые новости. Советы по определению фейковых новостей. Борьба с распространением фейковых новостей на уровне российского законодательства. Ответственное отношение к репостам. Значимость критического мышления.

- **Тема 4. Как соблюдать авторское право в Интернете**

- Авторское право. Виды лицензий авторского права. Копирайт. Проприетарная лицензия. Копилефт. Лицензия Creative Commons. Пиратство, плагиат. Тест на отношение к сетевому пиратству. Статьи Гражданского кодекса Российской Федерации, связанные с вопросами авторского права.

- **Тема 5. Всегда ли нужно оставаться на связи?**

- Социальные сети, мессенджеры. Общение в мессенджерах и социальных сетях. Чрезмерное увлечение общением в Интернете. Фабинг. FOMO. Прокрастинация. Способы самоконтроля и борьбы с прокрастинацией.

- **Тема 6. Комфорт и безопасность в социальных сетях**

- Общение в Интернете и социальных сетях. Риски общения в социальных сетях. Помощь другим пользователям, столкнувшимся с трудностями. Создание комфортной и безопасной атмосферы при общении в Интернете. Нетикет. Службы поддержки в социальных сетях.

- **Тема 7. Цифровая экономика: не только покупки**

- Цифровая экономика. Государственная программа «Цифровая экономика Российской Федерации». Цифровая экономика в повседневной жизни. Экономические отношения без посредников. Шеринг-экономика. Меры предосторожности при покупке товаров и услуг без посредников. Краудфандинг, краудсорсинг. Государственные и муниципальные услуги в Интернете.

- **Тема 8. Что знают обо мне цифровые устройства**

- Виды персональных данных. Какая информация хранится на смартфонах. Примущества и недостатки хранения информации в смартфонах. «Умные» вещи. «Интернет вещей». Какие персональные данные собирают «умные» вещи. Правила безопасности при установке приложений. Шифрование в мессенджерах.

- **Тема 9. Как управлять репутацией и удалять персональные данные в Интернете**

- Цифровые следы. Репутация в Сети. Право на забвение. Рекомендации по удалению персональных данных из Сети. Статья 13.11 Кодекса РФ об административных нарушениях (Нарушение законодательства Российской Федерации в области персональных данных).

- **Тема 10. «Умный» город**

- «Умные» города. Цифровые технологии в городских инфраструктурах. Беспилотники. Технология Big Data. Фермы-небоскрёбы.

ПОУРОЧНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

5 КЛАСС

Тема	Общее количество часов	Теория	Практическая работа
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)			
1. Зачем нам нужен Интернет	3	2	1
Модуль 2. Техносфера и технические риски (4 часа)			
2. Как устроен Интернет	4	2	2
Модуль 3. Информация и контентные риски (8 часов)			
3. Какая бывает информация	4	2	2
4. Как работает поиск в Интернете	4	2	2
Модуль 4. Общение и коммуникационные риски (4 часа)			
5.Как люди общаются в Интернете	4	2	2
Модуль 5. Цифровая экономика и потребительские риски (4 часа)			
6. Как совершать покупки в Интернете	4	2	2
Модуль 6. Персональные данные (8 часов)			
7. Что такое персональные данные	4	2	2
8. Какие следы мы оставляем в Интернете	4	2	2
Модуль 7. Цифровое будущее (3 часа)			
9. Урок в школе будущего	3	1	2
Итого	**34**	**17**	**17**

6 КЛАСС

Тема	Общее количество часов	Теория	Практическая работа
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)			
1. Мы в цифровом мире	3	1	2
Модуль 2. Техносфера и технические риски (4 часа)			
2. Почему важны пароли в Интернете	4	2	2
Модуль 3. Информация и контентные риски (8 часов)			
3. Полезные интернет-ресурсы	4	2	2
4. Как искать и распознавать правдивую информацию	4	2	2
Модуль 4. Общение и коммуникационные риски (6 часов)			
5. Как общаться в Интернете	3	2	1
6. Как избежать конфликтов в Интернете	3		
Модуль 5. Цифровая экономика и потребительские риски (4 часа)			
7. Как не попасться на удочку онлайн-мошенникам	4	2	2
Модуль 6. Персональные данные (6 часов)			
8. Что такое персональные данные	2	1	1
9. Что нужно знать о цифровых следах	4	2	2
Модуль 7. Цифровое будущее (3 часа)			
10. Дома будущего	3	1	2
Итого	**34**	**17**	**17**

7 КЛАСС

Тема	Общее количество часов	Теория	Практическая работа
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)			
1. Как не заблудиться в Интернете	3	1	2
Модуль 2. Техносфера и технические риски (3 часа)			
2. Как безопасно подключаться к Интернету	3	2	1
Модуль 3. Информация и контентные риски (8 часов)			
3. Как искать полезную информацию в Интернете	4	2	2
4. Почему нужно проверять информацию в Интернете	4	2	2
Модуль 4. Общение и коммуникационные риски (8 часов)			
5. Человек в Интернете: реальный или виртуальный?	4	2	2
6. Как противостоять агрессии в Интернете	4	2	2
Модуль 5. Цифровая экономика и потребительские риски (3 часа)			
7. Как безопасно совершать покупки в Интернете	3	1	2
Модуль 6. Персональные данные (6 часов)			
8. Как персональные данные оказываются в Сети	3	1	2
9. Для чего нужно управлять персональными данными	3	1	2
Модуль 7. Цифровое будущее (3 часа)			
10. Цифровой мир будущего	3	1	2
Итого	**34**	**15**	**19**

8 КЛАСС

Тема	Общее количество часов	Теория	Практическая работа
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)			
1. Другая реальность — дополненная и виртуальная	3	1	2
Модуль 2. Техносфера и технические риски (4 часа)			
2. Защита от вредоносных программ	4	2	2
Модуль 3. Информация и контентные риски (6 часов)			
3. Как стать мастером поиска в Интернете	3	1	2
4. Фейки в Интернете: как их распознать	3	1	2

Модуль 4. Общение и коммуникационные риски (8 часов)			
5. Репутация в Интернете: как её сохранить	4	2	2
6. Агрессия в Сети: способы предотвращения	4	2	2
Модуль 5. Цифровая экономика и потребительские риски (4 часа)			
7. Электронные платежи: правила безопасности	4	2	2
Модуль 6. Персональные данные (6 часов)			
8. Персональные данные в Сети: как их защитить	3	1	2
9. Оберегаем личное пространство в Интернете	3	1	2
Модуль 7. Цифровое будущее (3 часа)			
10. Профессии будущего	3	1	2
Итого	**34**	**14**	**20**

9 КЛАСС

.

Тема	Общее количество часов	Теория	Практическая работа
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)			
1. Искусственный интеллект: что нас ждёт в будущем?	3	1	2
Модуль 2. Техносфера и технические риски (3 часа)			
2. Как искать и хранить информацию в Интернете	3	2	1
Модуль 3. Информация и контентные риски (7 часов)			
3. Как увидеть правду в море лжи	3	1	2
4. Как соблюдать авторское право в Интернете	4	2	2
Модуль 4. Общение и коммуникационные риски (8 часов)			
5. Всегда ли нужно оставаться на связи?	4	2	2
6. Комфорт и безопасность в социальных сетях	4	2	2
Модуль 5. Цифровая экономика и потребительские риски (4 часа)			
7. Цифровая экономика: не только покупки	4	2	2
Модуль 6. Персональные данные (6 часов)			
8. Что знают обо мне цифровые устройства	3	1	2
9. Как управлять репутацией и удалять персональные данные	3	1	2
Модуль 7. Цифровое будущее (3 часа)			
10. «Умный» город	3	1	1
Итого	**34**	**16**	**18**

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УЧИТЕЛЯ

Солдатова Г.У. Программа курса «Кибербезопасность». 5–9 классы / Г.У. Солдатова, С.В. Чигарькова, И.Д. Пермякова. — М.: ООО «Русское слово — учебник», 2022. — 32 с. — (ФГОС).
Солдатова Г.У. Учебник «Кибербезопасность». 5 класс / Г.У. Солдатова, С.В. Чигарькова, И.Д. Пермякова. — М.: ООО «Русское слово — учебник», 2022.
Солдатова Г.У. Учебник «Кибербезопасность». 6 класс / Г.У. Солдатова, С.В. Чигарькова, И.Д. Пермякова. — М.: ООО «Русское слово — учебник», 2022
Солдатова Г.У. Учебник «Кибербезопасность». 7 класс / Г.У. Солдатова, С.В. Чигарькова, И.Д. Пермякова. — М.: ООО «Русское слово — учебник», 2022
Солдатова Г.У. Учебник «Кибербезопасность». 8 класс / Г.У. Солдатова, С.В. Чигарькова, И.Д. Пермякова. — М.: ООО «Русское слово — учебник», 2022
Солдатова Г.У. Учебник «Кибербезопасность». 9 класс / Г.У. Солдатова, С.В. Чигарькова, И.Д. Пермякова. — М.: ООО «Русское слово — учебник», 2022

ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ И РЕСУРСЫ СЕТИ ИНТЕРНЕТ

1. Дети России онлайн — с айт проектов Фонда Развития Интернет [Электронный ресурс]: [сайт]. [2020]. URL: http://detionline. com (дата обращения: 18.06.2022).
2. Образовательный портал для родителей от Лаборатории Касперского [Электронный ресурс]: [сайт]. [2017]. URL: https://kids. kaspersky.ru (дата обращения: 18.06.2022).
3. Электронные версии выпусков журнала «Дети в информационном обществе» [Электронный ресурс]: [сайт]. [2017]. URL: http:// detionline.com/journal/numbers (дата обращения: 18.06.2022).