

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Курс «Цифровая гигиена» ориентирован на проведение уроков по информационной безопасности школьников и безопасному поведению в сети Интернет и отражает актуальные вопросы безопасной работы с персональной информацией, сообщениями и звонками по мобильному телефону, электронной почтой, информационными и коммуникационными ресурсами в сети Интернет, доступа к ресурсам для досуга, поиска новостной, познавательной, учебной информации, общения в социальных сетях, получения и передачи файлов, размещения личной информации в коллективных социальных сервисах. В основе курса лежат технические, этические и правовые нормы соблюдения информационной безопасности, установленные контролирующими и правоохранительными органами, а также практические рекомендации ведущих ИТ-компаний и операторов мобильной связи Российской Федерации.

Особенности курса

**по информационной безопасности**

Безопасность в сети Интернет в свете быстрого развития социальных информационных технологий, их глобализации, использования облачных технологий и повсеместного массового распространения среди детей мобильных персональных цифровых устройств доступа к сети Интернет, появления большого количества сетевых сервисов и интернет-коммуникаций, в том числе закрытых сетевых сообществ неизвестного толка, а также общедоступных и зачастую навязчивых интернет-ресурсов (СМИ, реклама, спам), содержащих негативный и агрессивный контент, появление сетевых средств вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, массовое использование детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним, резко повышает потребность в воспитании у учащихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от негативной информации.

При реализации требований безопасности в сети Интернет для любого пользователя, будь это школьник или учитель, образовательное учреждение должно обеспечивать защиту конфиденциальных сведений, представляющих собой в том числе персональные данные школьника. Но включение детей в интернет-взаимодействие наиболее активно осуществляется вне школы без надлежащего надзора со стороны взрослых.

В связи с этим в настоящее время следует особое внимание уделять воспитанию у детей культуры информационной безопасности при работе в сети Интернет вне школы. Для этого необходимо проводить непрерывную образовательно-просветительскую работу с детьми, начиная с младшего школьного возраста, формировать у родителей и учащихся ответственное и критическое отношение к источникам негативной информации, в том числе внимательно относиться к использованию детьми личных устройств мобильной связи, домашнего компьютера с Интернетом, телевизора, подключенного к Интернету, использовать дома программные средства защиты от доступа детей к негативной информации или информации по возрастным признакам (возраст+). Научить школьника правильно ориентироваться в большом количестве ресурсов в сети Интернет является важной задачей для вовлечения детей в современную цифровую образовательную среду, отвлечения их от бесполезного, отвлекающего контента, бесцельной траты времени в социальных сетях и мессенджерах.

Главная цель курса — обеспечить социальные аспекты информационной безопасности в воспитании школьников в условиях цифрового мира, включение цифровой гигиены в контекст воспитания детей на регулярной основе, формирование у выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов обучения и воспитания детей.

Структура и содержание курса

**Задачи курса** по информационной безопасности детей:

* формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как человеческая жизнь, свобода, равноправие и достоинство людей, здоровье, опыт гуманных, уважительных отношений с окружающими;
* создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствия деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;
* формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;
* мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;
* научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, осознавать ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства Интернета как среду созидания, а не разрушения человека и общества.

Структура и содержание курса

Особенностью курса является поэтапное развитие учебного материала для разных возрастных групп учащихся. Курс представлен четырьмя блоками для детей по возрастным группам: 5–6 классов, 7–8,9-10,11 классов.

Риски, c которыми школьники могут встретиться, пользуясь Интернетом, отражены в модуле курса для учащихся начальных классов.

* Дети могут получить доступ к негативной, преступной информации. К ней относятся: порнография, дезинформация, обман, пропаганда ненависти, нетерпимости, насилия, жестокости.
* Дети могут получить доступ к информации в интернет- магазинах или на сайтах объявлений, совершить действия и купить товары, потенциально опасные для них. Существуют сайты, предлагающие инструкции по изготовлению взрывчатых веществ, продающие оружие, алкоголь, отравляющие и ядовитые вещества, наркотики, табачные изделия или никотинсодержащие продукты.
* Дети могут быть подвержены притеснениям со стороны других пользователей сети Интернет, которые грубо ведут себя в Интернете, пишут оскорбления и угрожают.
* Дети могут загрузить себе на компьютеры вирусы или подвергнуть свои устройства нападению хакеров.
* Дети могут выдать важную и личную информацию, заполняя анкеты и принимая участие в онлайн-конкурсах, и в результате стать жертвой безответственных торговцев, использующих нечестные, запрещенные маркетинговые методы.
* Дети могут стать жертвами обмана при покупке товаров через Интернет, а также выдать важную финансовую информацию другим пользователям (например, номер кредитной карточки, пин-коды и пароли).
* Дети могут стать жертвой киберманьяков, ищущих преступной личной встречи с ребенком.
* Дети могут быть вовлечены в неформальные сообщества через мессенджеры и социальные сети, вовлечены в группы на сайтах, предлагающих принять участие в азартных играх, вымогающих денежные средства и внедряющихся в психику ребенка.

Эти риски потребовали расширить темы курса информационной безопасности в сети Интернет для школьников 5–6 классов такими понятиями, как:

* негативный и позитивный Интернет;
* культура организации компьютерного досуга и профилактика игромании;
* мошенники в сети Интернет;
* агрессия в Интернете;
* сетевой этикет;
* навязчивые предложения;
* правила регистрации в электронных ресурсах и защита личных данных.

Курс для школьников 7–9 классов отражает особенности современного цифрового мира как киберпространства, насыщенного сетевыми сервисами и интернет-коммуникациями, доступными детям, в том числе негативной направленности:

* закрытые сетевые сообщества неизвестного толка, опасные группы, негативные контакты;
* навязчивые интернет-ресурсы (спам, реклама, азартные игровые сервисы);
* сайты, содержащие негативный и агрессивный контент, в том числе противоправные материалы, влекущие ответственность по законам Российской Федерации;
* сетевые средства вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете;
* использование детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним.

Все это резко повышает потребность в воспитании у учащихся культуры информационной безопасности, с одной стороны, и профориентации в мире профессий будущего — с другой, а также в популяризации полезных интернет- ресурсов.

«Информационные войны» в глобальном цифровом пространстве породили новые угрозы для общества — кражу персональных данных, призывы к агрессии и террору, склонение к насилию, суициду. С учетом последних тенденций, названных «фейковые новости», в киберпространстве появились: навязчивый ложный контент деструктивного, очерняющего людей и события содержания, пропаганда наркотических средств под видом ложной информации о продукции, в том числе распространяемый автоматически, ложные новости и постановочные репортажи. Навыки обдуманного поведения при поиске информации в сети Интернет, критического анализа полученной информации, умение работать с информацией избирательно и ответственно, знакомство с профессиями в сфере информационной безопасности — это важная часть современной цифровой грамотности школьников 7–9 классов, которая востребована в жизни и учебе при работе в сети Интернет, социальных сетях и мессенджерах.

Проникновение мобильных устройств с доступом к Интернету в быт и досуг детей обострило проблему интернет- зависимости, игромании, зависимости от социальных сетей, необоснованного доверия посторонним людям в Сети и, как следствие, незащищенности детей от атак мошенников, преступников, агрессивно настроенных людей, включая вовлечение детей в теневые, закрытые субкультуры, несущие угрозу здоровью и даже жизни ребенка. При этом в сети Интернет есть много позитивного контента, СМИ, позволяющих получать информацию о профессиях будущего, об использовании цифровых технологий в быту на основе «умных» технологий, о направлениях развития современного киберискусства, использовании Интернета для электронного обучения и др.

Все это потребовало расширить тему информационной безопасности в сети Интернет для школьников 7–9 классов такими понятиями, как:

* киберагент;
* кибермир;
* киберискусство;
* киберобщество;
* киберугрозы;
* кибератака;
* киберпреступность;
* киберкультура и др.

Важную часть практического содержания курса составляет выполнение заданий по информационной безопасности с использованием сети Интернет, ознакомление с позитивным контентом познавательного, учебного и развивающего на- значения, выполнение практической работы, предложенной в открытых практикумах ИТ-компаний и операторов мобильной телефонии для разных возрастных групп учащихся (практикумы встроены в содержание модулей курса).

Курс для учащихся 10–11 классов включает изучение правовой грамоты в сфере информационной безопасности, в том числе основных видов юридической ответственности (уголовной, административной и гражданско-правовой) за преступления и проступки в области информационной безопасности. Полученные знания помогут избегать ошибок и опасностей, которые подстерегают нас в информационном мире, а также ответственно работать в информационном пространстве с соблюдением норм права.

Важную часть курса составляет изучение правовой информации об основных законодательных актах в сфере информационной безопасности, а также материалов, размещенных на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, на основании которых рекомендуется проектная работа, например составление информационной листовки, буклета по темам:

* персональные данные [(http://gotourl.ru/15619);](http://gotourl.ru/15619)%3B)
* контроль и надзор в сфере информационных технологий [(http://gotourl.ru/15620);](http://gotourl.ru/15620)%3B)
* контроль и надзор в сфере связи [(http://gotourl.ru/15621);](http://gotourl.ru/15621)%3B)
* контроль и надзор в сфере массовых коммуникаций [(http://gotourl.ru/15622).](http://gotourl.ru/15622))

ПЛАНИРУЕМЫЕ ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА

В соответствии с ФГОС общего образования необходимо сформировать у учащихся такие личностные результаты, которые позволят подростку ориентироваться в информационном мире с учетом имеющихся в нем угроз:

* принимать ценности человеческой жизни, семьи, гражданского общества, многонационального российского народа, человечества;
* быть социально активным, уважающим закон и правопорядок, соизмеряющим свои поступки с нравственными ценностями, осознающим свои обязанности перед семьей, обществом, Отечеством;
* уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания, сотрудничать для достижения общих результатов;
* осознанно выполнять правила здорового и экологически целесообразного образа жизни, безопасного для человека и окружающей его среды.

В результате обучения по модулям курса акцентируется внимание на такие метапредметные результаты освоения основной образовательной программы основного общего образования, как:

* освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах, включая взрослые и социальные сообщества; участие в школьном самоуправлении и общественной жизни в пределах возрастных компетенций с учетом региональных, этнокультурных, социальных и экономических особенностей;
* формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности;
* умение использовать средства информационных и коммуникационных технологий (далее — ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Также планируется достижение некоторых предметных результатов, актуальных для данного курса в интеграции с предметами: «Информатика» и ОБЖ для 5–6 и 7–9 классов, «Обществознание» и «Информатика»:

* формирование основ правосознания для соотнесения собственного поведения и поступков других людей с нравственными ценностями и нормами поведения, установленными законодательством Российской Федерации;
* освоение приемов работы с социально значимой информацией, ее осмысление; развитие способностей обучающихся делать необходимые выводы и давать обоснованные оценки социальным событиям и процессам;
* формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

Планируется достижение некоторых предметных результатов, актуальных для данного курса.

В результате освоения курса учащиеся будут

*знать и понимать:*

* источники угроз, поступающих на мобильный телефон, планшет, компьютер;
* виды угроз;
* проблемные ситуации в сетевом взаимодействии;
* правила поведения для защиты от угроз;
* правила поведения в проблемных ситуациях;
* этикет сетевого взаимодействия;
* роль близких людей, семьи в устранении проблем и угроз в сети Интернет и мобильной телефонной связи;
* телефоны экстренных служб;
* личные данные;
* позитивный Интернет;

*уметь:*

* правильно использовать аватар с учетом защиты личных данных;
* формировать и использовать пароль;
* использовать код защиты телефона;
* регистрироваться на сайтах без распространения личных данных;
* вести общение в социальной сети или в мессенджере сообщений;
* правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.);
* отключиться от нежелательных контактов;
* использовать позитивный Интернет.

ВИДЫ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

ОБУЧАЮЩИХСЯ НА УРОКАХ

Уроки информационной безопасности несут практическую направленность.

Познавательная часть урока основана на постановке учителем проблемы в качестве темы урока; ее рекомендуется проводить в форме беседы-дискуссии, опираясь на видеоматериалы и факты по теме. Рекомендуется на каждом уроке в рамках изучаемой темы:

* рассказать школьникам о возможных негативных последствиях, которые могут наступить при работе в сети Интернет;
* мотивировать школьников использовать ресурсы сети Интернет для определенных целей;
* выстроить беседы в максимально доверительном тоне. Доверие между ребенком и взрослым — залог успеха в таком важном деле;
* использовать компьютерный класс, где установлена аппаратная защита — постоянно обновляемый антивирус, программа защиты (контент-фильтр) для сортировки и отсеивания информации негативного характера;
* активно вовлекать детей в обсуждение проблемы по теме.

Практическая часть урока основана на выполнении заданий по выбранной теме, в том числе практических работ от ведущих ИТ-компаний, специально разработанных для детей и представленных в открытом доступе. Все уроки по темам курса снабжены тестами для промежуточного контроля, которые удобно проводить в форме мини-викторин.

Для достижения планируемых результатов предусмотрены учебно-методические комплекты по информационной безопасности для 5–6, 7–8, 9–10 и 11 классов, снабженные открытыми электронными материалами на сайте издательства «БИНОМ. Лаборатория знаний».

В состав интернет-ресурсов для проведения занятий по информационной безопасности включены открытые курсы и электронные материалы, видеоролики от ведущих ИТ- компаний и операторов мобильных сетей.

Виды учебной деятельности

|  |  |  |  |
| --- | --- | --- | --- |
| **Учебная деятельность учащихся** | **2–4 и 5–6 классы** | **7–9 классы** | **10–11 классы** |
| Получение знаний | Коллективная работа:   * участие в беседе, организованной учителем, на основе материалов параграфа учебного пособия; * поиск и презентация примеров угроз по теме; * анализ правил поведения при угрозах по сценарию: разбор примеров, выявление угрозы, оценка предложенного в тексте или видеоматериале поведения, предложение по корректировке поведения с учетом правил.   Групповая работа:   * анализ видеоматериала по теме занятия в форме обсуждения в группах (угрозы и меры их профилактики); * формулирование выводов — правил по теме занятия.   Индивидуальная работа:  выявление угроз в предложенном сюжете | Коллективная работа:   * анализ учебного материала по теме; * анализ угроз; * формирование сообщения по сценарию: разбор примеров, выявление угрозы, оценка предложенного в тексте или видеоматериале поведения, предложение по корректировке поведения с учетом правил; * анализ современных тенденций развития киберпространства, поиск и презентация примеров.   Групповая работа:   * формулирование выводов — правил по теме занятия; * анализ/поиск/обсуждение информации на сайтах по теме занятия.   Индивидуальная работа:   * формулирование правил, действий для профилактики угроз, отраженных в теме занятия | Коллективная работа:   * анализ учебного материала по теме; * анализ правовых норм и правоприменительной практики по теме занятия; * отбор материала и формирование сообщения по сценарию: разбор примеров, выявление правонарушения и оценка ответственности; * участие в беседе по теме занятия с использованием правовых документов.   Групповая работа:   * формулирование выводов по теме занятия; * анализ/поиск/обсуждение информации в правовых документах по теме занятия.   Индивидуальная работа:   * формулирование действий для профилактики правонарушений по теме занятия |
| Освоение умений  17 | Коллективная работа:   * формирование пошаговых правил, инструкции по проблеме занятия.   Групповая работа:   * участие команд в викторине на основе вопросов теста к параграфу; * работа с сайтом учебно-познавательного назначения; * работа с мессенджером сообщений, организованным учителем; * взаимоконтроль в работе с тестами по теме.   Индивидуальная работа:   * регистрация в детской социальной сети; * формирование ника и пароля; * формирование папки   «Спам» | Коллективная работа:   * формирование памятки, брошюры для школьного стенда; * организация совместно с педагогом беседы/диспута по проблеме занятия с использованием видеоматериалов, сайтов учебно-познавательного назначения.   Групповая работа:   * разработка пошаговых правил, инструкции по проблеме занятия (для дальнейшего проведения инструктажа для учащихся и родителей на школьном мероприятии по информационной безопасности); * антивирусная профилактика компьютера.   Индивидуальная работа:   * выполнение практической работы к блоку занятий; * самоконтроль по тестам к занятию | Коллективная работа:   * формирование памятки, брошюры для школьного стенда по правовым основам информационной безопасности; * организация совместно с педагогом беседы/диспута по проблеме занятия с использованием специализированных сайтов; * разработка рекомендаций по проблеме занятия (для дальнейшего проведения инструктажа для учащихся и родителей на школьном мероприятии по правовым основам информационной безопасности).   Индивидуальная работа:   * выполнение практической работы к блоку занятий; * самоконтроль по тестам к занятию |

|  |  |  |  |
| --- | --- | --- | --- |
| Применение знаний и умений  в учебной ситуации и в жизни | Коллективная работа:   * формирование памятки правил безопасной работы в сети Интернет и с мобильным телефоном.   Групповая работа:   * использование сайтов учеб- но-познавательного назначения; * поиск информации по заданию учителя; * формулировка текста сообщения с использованием правил сетевого этикета; * блокировка нежелательного номера телефона; * включение в адресную книгу телефонов службы спасения; * выполнение заданий к занятию; * разработка викторины для проведения состязания   в классе. | Коллективная работа:   * проектирование материалов для школьного стенда по информационной безопасности.   Групповая работа:   * проведение школьного мероприятия по выбранной теме; * проведение консультаций по киберугрозам для ученических групп при координации педагога; * участие в разработке наборов заданий для школьного конкурса по информационной безопасности; * участие в мероприятии по профориентации в условиях развития новых профессий в киберпространстве. | Коллективная работа:   * проектирование материалов для школьного стенда по правовым основам информационной безопасности.   Групповая работа:   * проведение школьного мероприятия по выбранной теме; * проведение консультаций по правовым основам информационной безопасности для ученических групп при координации педагога; * участие в разработке наборов заданий для школьного конкурса по правовым основам информационной безопасности. |
|  | Индивидуальная работа:   * выполнение творческого задания, представление результата в форме устного сообщения, компьютерной презентации, электронного доклада; * применение правил безопасного поведения при работе с мобильным телефоном и в сети Интернет; * применение правил сетевого этикета | Индивидуальная работа:   * формулирование текстов сообщений с использованием правил сетевого этикета; * профилактика от угроз личного компьютера; * корректировка ника и пароля; * применение правил безопасной работы на мобильном устройстве; * применение правил анти- буллингового поведения * применение правил защиты от мошенников в сети Интернет; * самоорганизация сбалансированного использования цифровых устройств для рабочего и досугового времени | Индивидуальная работа:   * использование правовых норм информационной безопасности в жизни и сетевой активности; * личное участие в проектах по распространению правовых норм в сфере информационной безопасности |

**Виды учебной деятельности**

**обучающихся на уроках**

Учебная деятельность учащихся по курсу информационной безопасности включает также направления проектной деятельности для 5–11 классов.

Конкурс рисунков «Правила поведения в сети Интернет» по темам информационной безопасности для 5–6 и 7–8 классов.

Конкурс кроссвордов-презентаций «Цифровая гигиена» для детей 9–10 классов.

Клуб «Киберпатруль».

Турнир «Киберобщество».

В круг задач входит разработка тестов для проведения этапов турнира по возрастным группам в формах:

* + викторина «Цифровая гигиена» (для 5–6 классов);
  + кроссворд-презентация «Цифровая гигиена» — выбор ответа по изображенной ситуации (для 7-8 классов);
  + квест по предложенной траектории на тему угроз с практическими работами на компьютере (для 9–10 классов);
  + правовой тур по информационной безопасности (для 11 класса).

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

Тематическое планирование учебного курса для 5–6 классов

Курс реализован отдельным учебным предметом на 34 часа, а также в рамках занятий по предмету «Информационная гигиена» в форме проведения тематических уроков, а также включен в рамки школьных мероприятий: уроков-дискуссий, цикла бесед для классных часов с участием родителей в 5–6 классах по модулям учебно-тематического планирования.

Курс представлен в учебном пособии «Информационная безопасность» - Правила безопасного Интернета. 5–6 классы». К учебному пособию на сайте издательства размещено бесплатное электронное приложение. Оно включает ресурсы для выполнения практических заданий к урокам из пособия, а также открытые познавательные ресурсы для 5–6 классов ([**http://gotourl.ru/11557**).](http://gotourl.ru/11557))

Курс включает следующие модули и темы.

Модуль 1. Правила безопасной работы в сети Интернет с мобильным телефоном.

Угрозы из СМС-сообщений. Угрозы от незнакомых лиц. Ложные сообщения и просьбы. Проблемы хулиганства по телефону. Телефоны экстренных служб. Выход в Интернет, беспроводную сеть. Защита устройства от входа, код входа.

Модуль 2. Правила безопасной работы в сети Интернет с планшетом или на компьютере.

Защита входа в устройство. Пароль и логин. Электронная почта. Спам. Вирусы. Регистрация на сайтах. Личные данные.

Модуль 3. Путешествуем в сети Интернет.

Поиск информации в сети Интернет. Позитивный Интернет. Сайты для учебы, досуга, творчества, чтения книг, виртуальных путешествий.

Модуль 4. Правила безопасной работы в социальной сети.

Социальные сети. Детские социальные сети. Аватар и его выбор. «Друзья» в сети. Опасности общения в социальной сети с виртуальными «друзьями». Поддержка семьи для устранения проблем общения в социальных сетях.

Этикет общения. Реакция на негативные сообщения, угрозы, агрессию, уговоры и опасные предложения. Отключение от нежелательных контактов.

Тематическое планирование уроков информационной гигиены

во 5–6 классах

|  |  |  |  |
| --- | --- | --- | --- |
| **№ урока** | **Тема урока/параграф учебного пособия** | **Практическая работа к уроку (задачи и викторины)** | **Содержание задания/ электронное приложение** |
| **10 часов** | **Модуль 1. Правила безопасной работы в сети Интернет с мобильным телефоном** | | [**http://gotourl.ru/11557**](http://gotourl.ru/11557) |
| 1 | Введение.  Уроки Смайлика | Задание В.1 | Нарисуй смайлик |
| 2 | 1.1. СМС от неизвестных лиц | Тест 1 |  |
| 3 | 1.2. Ложные сообщения | Тест 2 |  |
| 4 | 1.3. Угрозы в СМС | Тест 3 |  |
| 5 | 1.4. Звонки с предложениями | Тест 4 |  |
| 6 | 1.5. Защита от входа в твой телефон | Тест 5 |  |
| 7 | 1.6. Подключение телефона к Wi-Fi-сети | Тест 6 |  |
| 8 | 1.7. Вызов экстренных служб | Тест 7 |  |
| 9 | 1.8. Телефонное хулиганство | Тест 8 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 10 | Контрольный урок | Проектные задания 1.1–1.2 | * 1. Посмотри дома со взрослыми или на уроке с помощью учителя видеоуроки.   Ознакомься с видеоуроком канала БИБИГОН «Уроки хороших манер. Дресс-код/Как пользоваться мобильным телефоном».  Составь свою памятку правил пользования мобильным телефоном.   * 1. Ознакомься с видеоуроком портала СПАС Экстрим   «Мобильные мошенники».  Ответь на вопрос: кто такие мобильные мошенники и чем они опасны? |
| **7 часов** | **Модуль 2. Правила безопасной работы в сети Интернет с планшетом или на компьютере** | | [**http://gotourl.ru/11557**](http://gotourl.ru/11557) |
| 11 | 2.1. Мой планшет или компьютер: защита входа | Тест 9 |  |
| 12 | 2.2. Моя почта, логин и пароль | Задание 2.1  Тест 10 | 2.1. Вместе со взрослыми в семье или с учителем создай свой почтовый ящик |
| 13 | 2.3. Спам | Тест 11 |  |
| 14 | 2.4. Почта от неизвестных лиц | Тест 12 |  |
| 15 | 2.5. Вирусы | Тест 13 |  |
| 16 | 2.6. Регистрация на сайтах: личные данные | Тест 14 |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ урока** | | **Тема урока/параграф учебного пособия** | **Практическая работа к уроку** | | **Содержание задания/ электронное приложение** |
| 17 | | Контрольный урок | Проектное задание 2.2 | | 2.2. Используй пособие компании МТС для младших школьников с сайта «Дети в Интернете». Распечатай, прочитай тексты и раскрась картинки, чтобы получить собственное настольное пособие.  [(http://gotourl.ru/15604)](http://gotourl.ru/15604)) |
|  | |  | Проектное задание 2.3 | | 2.3. Посмотри дома вместе со взрослыми или на уроке с учителем видеоурок портала СПАС Экстрим  «Безопасный Интернет».  Составь личную памятку безопасности в сети Интернет |
| **7 часов** | | **Модуль 3. Путешествуем в сети Интернет** | | | [**http://gotourl.ru/11557**](http://gotourl.ru/11557) |
| 18 | | 3.1. Поиск информации в Интернете |  | | Ознакомься с материалами сайта и используй их для разнообразия своего досуга.   * 1. *Детская игровая комната.*   На сайте представлены тексты детских песен, раскраски, гороскоп, шарады, загадки, логические задачки, перевертыши, пословицы, ребусы, кроссворды, сказки, игры для развития логического мышления и многое другое.   * 1. *Страна Мастеров.*   Страна Мастеров объединяет учителей и учащихся, родителей и детей, состоявшихся мастеров и новичков. Тематика сайта: прикладное творчество, мастерство во всех его проявлениях и окружающая среда |
| 19 | | 3.2. Сайты для детей | Задания 3.1–3.2 | |
| 20  Тематическое планирование во 2–4 классах  27 | | 3.3. Сайты о безопасном поведении | Задание 3.3 | | 3.3. *Сайт детской безопасности Министерства чрезвычайных ситуаций.*  Используй материалы сайта для самостоятельной работы дома |
| 21 | | 3.4. Сайты для учебы | Задания 3.4–3.10 | | Ознакомься с сайтами и используй их для онлайн- обучения.   * 1. *Электронное учебное пособие «Учимся беречь энергию» на сайте «Началка.инфо».*   Это электронное пособие размещено в открытом доступе для младших школьников. Пособие рассказывает об энергии, ее видах и превращениях, о том, что может сделать даже ребенок, чтобы сберечь энергетический запас страны. Ознакомься с ресурсом и используй его для учебы на уроках окружающего мира.   * 1. *Сайт Lingualeo. Покори язык.*   Lingualeo — это увлекательный, эффективный и бесплатный сервис для изучения английского языка.   * 1. *Сайт Учи.ру.*   Учащиеся из всех регионов России изучают школьные предметы в интерактивной форме.   * 1. *Сайт «Российская электронная школа».*   Сайт с материалами об окружающем мире.   * 1. *Сайт Московского планетария.*   Сайт коллекций Московского планетария поможет познакомиться с миром космоса.   * 1. *Московский зоопарк. Видео.*   Живое видео из вольеров зоопарка поможет проводить наблюдения за жизнью животных в зоопарке, что поможет в изучении окружающего мира. |
|  |  | |  | 3.10. *Сайт «Культура России».*  Коллекции творчества народов России, информация о театрах и музеях нашей страны, культурное наследие — все это поможет развивать свои знания и поможет в уроках по искусству и технологии | |
| 22 | 3.5. Сайты с электронными книгами | | Задания 3.11–3.13 | * 1. *Национальная электронная детская библиотека.*   Зарегистрируйся в библиотеке, пользуйся ресурсами.  В коллекции НЭДБ представлены произведения для детей, вошедшие в круг детского чтения, оформленные лучшими отечественными художниками-иллюстраторами, а также материалы, являющиеся ярким отражением исторических, политических, культурологических, художественных и педагогических процессов, происходивших в нашей стране в различные исторические периоды.   * 1. *Аудио хрестоматия.*   Выбери произведение, прослушай его.  «Аудио хрестоматия» — это уникальный портал аудиозаписей книг, на котором собраны лучшие произведения мировой литературы в исполнении признанных мастеров сцены.   * 1. *Детская электронная библиотека*. Выбери и скачай книгу для домашнего чтения.   Библиотека для детей разного возраста. Все книги, находящиеся в библиотеке, доступны для бесплатного скачивания | |

|  |  |  |  |
| --- | --- | --- | --- |
| 23  29 | 3.6. Сайты с коллекциями для детей | Задания 3.14–3.17 | * 1. *Лукошко.*   Детская электронная библиотека — народные и авторские сказки, стихи и рассказы для детей, а также словарь устаревших слов, встречающихся в текстах.  Ознакомься со страницей «Открытки через Интернет». Используя правила поведения в сети Интернет, оформи поздравительную открытку другу.   * 1. *Журнал «Мурзилка».*   Ознакомься с разделом «Авторы Мурзилки читают свои произведения».   * 1. *Теремок.*   Ознакомься с уроками безопасности для детей.   * 1. *Уроки оригами.*   Сайт с алгоритмами сборки конструкций из бумаги на основе традиций оригами. Выбери фигуру оригами и сложи ее по алгоритму |
| 24 | Контрольный урок | Задания 3.18–3.19 | 3.18. Войди на сайт популярной информационно-поисковой системы Яндекс.  Введи в графу для поиска ключевые слова:   * союз мультфильм; * российская детская библиотека; * началка инфо; * телеканал карусель; * аудио хрестоматия.   Перейди на нужные сайты и добавь их в систему закладок, используя сочетания клавиш Ctrl+D. |
|  |  |  | 3.19. Вместе со своими близкими или учителем найди при помощи информационно-поисковой системы Яндекс сайты олимпиад или конкурсов для начальной школы по любимому тобой предмету.  Выбери интересный для тебя конкурс.  Перейди на нужные сайты и добавь их в систему закладок, используя сочетания клавиш Ctrl+D |
| **6 часов** | **Модуль 4. Правила безопасной работы в социальной сети** | | [**http://gotourl.ru/11557**](http://gotourl.ru/11557) |
| 25 | * 1. Социальные сети для детей.   2. Что такое аватар и как его выбрать.   3. «Друг» в сети, кто за ним прячется | Тест 15  Тест 16  Тест 17 |  |
| 26 | * 1. Ложные сообщения.   2. Что говорить о себе незнакомцам.   3. Спроси совета в семье | Тест 18  Тест 19  Тест 20 |  |
| 27 | * 1. Этикет в общении.   2. Нельзя обижать.   3. Если тебя обижают | Тест 21  Тест 22  Тест 23 |  |
| 28  31 | * 1. Защити себя от недоброжелателей.   2. Если тебе угрожают.   3. Агрессия и грубость | Тест 24  Тест 25  Тест 26 |  |
| 29 | * 1. Уговоры и предложения   2. Отключение от нежелательных контактов | Тест 27  Тест 28 |  |
| 30 | Контрольный урок. Итоговый урок- викторина | Задания 4.1–4.3.  Рассказ Смайлика | * 1. Оцени свой этикет в социальных сетях. Ответь на вопрос: какой смайлик выберешь к каждому утверждению в таблице.   2. Ответь на вопрос: что ты сделаешь в предложенных ситуациях?   Выбери правильный ответ к каждой из предложенных ситуаций.   * 1. На рисунке «Я в Интернете» представлены сайты из пособия. Расскажи, какие из них использовались на уроках и дома.   Прочти рассказ Смайлика и скажи, правильно или неправильно он действовал, пользуясь мобильным  телефоном |

Тематическое планирование учебного курса для 7–8 кл.

Курс представлен в учебном пособии «Информационная безопасность - Безопасное поведение в сети Интернет. 7–8 классы». К учебному пособию на сайте издательства размещено бесплатное электронное приложение. Оно включает ресурсы для выполнения практических заданий к урокам из пособия, а также открытые познавательные ресурсы для 7–8 классов ([**http://gotourl.ru/11581**).](http://gotourl.ru/11581))

Для школьников 7–8 классов курс включает две части и рассчитан на 34 урока, которые может реализовать учитель информатики и ОБЖ.

Информационная часть урока организована с использованием материала для анализа учебной информации с демонстрацией работы в сети Интернет на примере использования различных устройств доступа к Сети. Практическая часть каждого урока предлагается в форме теста, компьютерного задания, и по итогам курса можно выявить наиболее активных учащихся и поощрить их грамотой за курс.

Курс открывается уроком об информационном обществе. Содержание курса включает темы, сформулированные в форме проблем для их решения: что нужно знать о сети Интернет (часть 1) и как использовать ее ресурсы при самостоятельной работе (часть 2).

Введение. Что такое информационное общество?

Часть 1. Что нужно знать? Пространство Интернета на планете Земля.

* 1. История создания сети Интернет.
  2. Что такое Всемирная паутина?
  3. Путешествие по сети Интернет: сайты и электронные сервисы.
  4. Как стать пользователем Интернета?
  5. Опасности для пользователей Интернета.
  6. Что такое кибератака.
  7. Что такое информационная безопасность?
  8. Законы о защите личных данных в Интернете.
  9. Сетевой этикет.
  10. Коллекции сайтов для детей.
  11. Электронные музеи.

**Тематическое планирование в 7–8 классах**

Часть 2. Что нужно уметь? Правила для пользователей сети Интернет.

* 1. Правила работы с СМС.
  2. Правила работы с электронной почтой.
  3. Правила работы с видеосервисами.
  4. Правила работы в социальных сетях.
  5. Правила защиты от вирусов, спама, рекламы и рассылок.
  6. Правила защиты от негативных сообщений.
  7. Правила общения в социальной сети.
  8. Правила работы с поисковыми системами и анализ информации.
  9. Правила ответственности за распространение ложной и негативной информации.
  10. Правила защиты от нежелательных сообщений и контактов.
  11. Правила вызова экстренной помощи.
  12. Правила защиты устройств от внешнего вторжения.
  13. Правила выбора полезных ресурсов в Интернете.
  14. Средства работы в Интернете для людей с особыми потребностями.

Курс в 5–6 классах реализуется в рамках образовательной Программы формирования ИКТ-компетентности обучающихся согласно ФГОС основного общего образования, а также в рамках изучения предмета ОБЖ.

Курс проводится как одногодичный в 7-8 классах. Рассчитан на 1 урок в неделю. 34 урока за учебный год.

Тематическое планирование уроков информационной безопасности

в 7–8 классах

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ урока** | **Тема урока/параграф учебного пособия** | **Практическая работа к уроку** | **Содержание задания/видеоматериалы** [**http://gotourl.ru/11581**](http://gotourl.ru/11581) | |
| 1 | Введение. Что такое информационное общество? | Задания В.1–В.2 | В.1. Проведите самооценку и выясните для себя, не вредите ли вы своему здоровью. Не забираете ли для ин формационной работы слишком много времени в ущерб учебе, творчеству, живому общению со сверстниками? Не появилась ли у вас интернет-зависимость?  В.2. Ознакомьтесь с видеоматериалами. Обсудите в группе, какую опасность здоровью может нанести неразумное увлечением общением в сети Интернет — лайкомания.  Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера: Лайкомания» | |
| 2 | **Часть 1. Что нужно знать? Пространство Интернета на планете Земля (15 часов)** | Задание 1.1 | 1.1. Ознакомьтесь с видеоматериалами. Обсудите в группе, какие угрозы таит в себе Интернет.   * Видеоролик «Угрозы Интернета для детей»: [http://gotourl.ru/11613.](http://gotourl.ru/11613) * Видеоролик «Мировой опыт защиты детей в Интернете»: <http://gotourl.ru/11585> | |
| 3 | 1.1. История создания сети Интернет | Тест 1. Задания 1.2–1.3 | * 1. Ознакомьтесь с видеоматериалами. Обсудите их в группе и ответьте на вопрос: где находится Интернет? Сайт телеканала «Карусель»: [http://gotourl.ru/11579.](http://gotourl.ru/11579)   Видеоролик «Почемучка. Где находится Интернет?».   * 1. Придумайте кроссворд на базе слова «Интернет» | |
| 4  35 | 1.2. Что такое Всемирная паутина? | Задания 1.4–1.5.  Тест 2 | * 1. На сайте телеканала «Карусель» посмотрите разделы сайта, используя слова-меню.   2. Ознакомьтесь с видеоуроком «Почемучка. Что такое веб-браузер?» телеканала «Карусель»: <http://gotourl.ru/11657>   Ответьте на вопрос: каким веб-браузером вы пользуетесь? | |
| 5 | 1.3. Путешествие по сети Интернет: сайты и электронные сервисы | Задания 1.6–1.9.  Тест 3 | * 1. Выполните поиск сайта телеканала «Карусель» с помощью поисковой системы Яндекс.   Выберите нужную ссылку и перейдите на этот сайт.   * 1. Ознакомьтесь с видеоуроком телеканала   «Карусель»: «Почемучка. Поисковая система». Ответьте на вопрос: что такое поисковые системы и для чего они предназначены?   * 1. Познакомьтесь с сайтом «Культура. РФ». Обсудите в группе, какие разделы вы находите наиболее интересными для себя, что понравилось больше всего.   2. Ознакомьтесь с детской социальной сетью   «Лунтик»: [http://gotourl.ru/11586,](http://gotourl.ru/11586) представляющей российские и зарубежные мультфильмы для детей. | |
| 6 | 1.4. Как стать пользователем Интернета? | Задание 1.10.  Тест 4 | 1.10. Ознакомьтесь с видеоуроком телеканала «Кару- сель»: «Почемучка. Способы выхода в Интернет». Ответьте на вопрос: какие различные способы выхода в Интернет вы можете применять? | |
| 7 | 1.5. Опасности для пользователей Интернета | Задания 1.11–1.12.  Тест 5 | * 1. На сайте «Большой российской энциклопедии»: [(http://gotourl.ru/11587)](http://gotourl.ru/11587)) перейдите в раздел «Россия» и ознакомьтесь с рубриками раздела.   2. Ознакомьтесь с видеоуроком телеканала   «Карусель»: «Почемучка. Информация». Ответьте на вопрос: что такое информация? | |
| 8 | 1.6. Что такое кибератака? | Задания 1.13–1.14.  Тест 6 | * 1. Ознакомьтесь с видеоматериалами. Ответьте на вопросы: что такое компьютерный вирус? чем он опасен для компьютера?   Сайт телеканала «Карусель»: [http://gotourl.ru/15450,](http://gotourl.ru/15450) видеоурок «Почемучка. Вирусы».   * 1. Ознакомьтесь с видеоматериалами. Обсудите действия героя в ситуации кибербуллинга и фишинга. Сайт «Защита детей. Лаборатория Касперского». * Мультфильм «Приключения робота Каспера: Кибербуллинг»: <http://gotourl.ru/11608> * Мультфильм «Приключения робота Каспера: Фишинг»: <http://gotourl.ru/11609> | |
| 9 | 1.7. Что такое информационная безопасность? | Задание 1.15.  Тест 7 | 1.15. Ознакомьтесь с видеоматериалами. Составьте личную памятку безопасности при работе в Интернете. Сайт телеканала «Карусель»: [http://gotourl.ru/10979.](http://gotourl.ru/10979)  Видеоурок «Почемучка. Безопасность при работе в Интернете» | |
| 10  37 | 1.8. Законы о защите личных данных в Интернете | Задания 1.16–1.18.  Тест 8 | * 1. Портал «Лига безопасного Интернета». Ознакомьтесь с видеоуроком «Защита персональных данных детей»: [http://gotourl.ru/15605.](http://gotourl.ru/15605)   2. Сайт «Персональные данные. Дети».   Пройдите электронный тест «Что ты знаешь о персональных данных»: [http://gotourl.ru/15606.](http://gotourl.ru/15606)   * 1. Ознакомьтесь с видеоматериалами. Обсудите в группе, что такое конфиденциальность и зачем ее соблюдать в Интернете. Какие угрозы подстерегают в сетевых играх?   Сайт «Защита детей. Лаборатория Касперского».   * «Фиксики: Фикси-советы: Осторожней в Интернете! Конфиденциальность»: [http://gotourl.ru/11610.](http://gotourl.ru/11610) * Мультфильм «Приключения робота Каспера — Общение в игре»: <http://gotourl.ru/11611> | |
| 11 | 1.9. Сетевой этикет | Задания 1.19–1.20.  Тест 9 | * 1. Ознакомьтесь с видеоуроком из архива канала   «Бибигон»: «Правила поведения в коллективе/ Сетевой этикет».  Ответьте на вопрос: какие правила поведения в коллективе нужно использовать в сообщениях на мобильном телефоне или по электронной почте?   * 1. Ознакомьтесь с видеоматериалами. Обсудите в группе, какие правила нужно соблюдать при общении в Интернете, чтобы не навредить себе.   Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера: Овер- шеринг. Вред репутации»: <http://gotourl.ru/11612> | |
| 12 | 1.10. Коллекции сайтов для детей | Задания 1.21–1.23 | * 1. Ознакомьтесь с видеоматериалом «Знакомимся с Интернетом»: [http://gotourl.ru/11584.](http://gotourl.ru/11584) Обсудите   в группе, что такое «позитивный контент».   * 1. Ознакомьтесь с разделами интернет-браузера   «Гогуль: Играй. Гуляй. Общайся. Учись».   * 1. Проведите путешествие по ресурсам сайта   «ВебЛандия». Обсудите в группе, какие из них помогут вам в развитии творчества | |
| 13 | 1.11. Электронные музеи | Задания 1.24–1.28 | * 1. Русский музей в Санкт-Петербурге. Виртуальный филиал: [http://gotourl.ru/11591.](http://gotourl.ru/11591) Ознакомьтесь с виртуальными экскурсиями.   2. Третьяковская галерея в Москве. Электронные коллекции: [http://gotourl.ru/11592.](http://gotourl.ru/11592)   Ознакомьтесь с залами музея с помощью онлайн- панорамы: [http://gotourl.ru/11593.](http://gotourl.ru/11593)   * 1. Музей изобразительных искусств имени   А. С. Пушкина в Москве. Электронная коллекция: [http://gotourl.ru/11594.](http://gotourl.ru/11594)  Выберите тематику и посетите электронную экспозицию Музея изобразительных искусств имени  А. С. Пушкина.   * 1. Эрмитаж. Виртуальное путешествие. Выберите виртуальное путешествие по Эрмитажу: <http://gotourl.ru/11595> | |
|  |  |  | 1.28. Политехнический музей в Москве. Раздел на сайте «Панорамные туры»: [http://gotourl.ru/11596.](http://gotourl.ru/11596) Выберите тур на сайте Политехнического музея и ознакомьтесь с его экспозицией на своем компьютере | |
| 14–15 | Контрольный урок | Контрольное задание к части 1 | Скачайте на свой компьютер файл с пособием, представленным «Лабораторией Касперского» в открытом доступе. Распечатайте пособие и выполните в нем задания.  Практикум «Азбука защиты информации» («Лаборатория Касперского»): <http://gotourl.ru/11588> | |
|  | **Часть 2. Что нужно уметь? Правила для пользователей сети Интернет (15 часов)** | |  | |
| 16 | 2.1. Правила работы с СМС | Задание 2.1.  Тест 10 | 2.1. Ознакомьтесь с видеоматериалами. Обсудите в группе действия героя, который столкнулся с вымогательством денег через сообщения мнимого друга. Сайт «Защита детей. Лаборатория Касперского».   * Мультфильм «Приключения робота Каспера: Друг Вовка»: [http://gotourl.ru/11614.](http://gotourl.ru/11614) * Мультфильм «Приключения робота Каспера: приватность аккаунтов»: <http://gotourl.ru/11616> | |
| 17 | 2.2. Правила работы с электронной почтой | Задания 2.2–2.3.  Тест 11 | 2.2. Ознакомьтесь с видеоматериалами. Составьте свою памятку с основными правилами использования электронной почты.  Сайт телеканала «Карусель»: [http://gotourl.ru/11666,](http://gotourl.ru/11666) видеоурок «Почемучка. Электронная почта». | |
|  |  |  | 2.3. Ознакомьтесь с видеоматериалами. Обсудите  в группе, какие методы вымогательства денег могут использовать злоумышленники для рассылок на ваш адрес.  Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера: Сообщения со взломанных аккаунтов»: <http://gotourl.ru/11617> | | |
| 18 | 2.3. Правила работы с видеосервисами | Задания 2.4–2.5.  Тест 12 | * 1. Ознакомьтесь с системой помощи по работе   с видеозаписями в социальной сети «ВКонтакте»: [http://gotourl.ru/11597.](http://gotourl.ru/11597)   * 1. Ознакомьтесь с видеоматериалами. Обсудите в группе, как в компьютерных видеоиграх может быть встроено вымогательство денег.   Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера: Покупки в играх»: <http://gotourl.ru/11618> | | |
| 19 | 2.4. Правила работы в социальных сетях | Задания 2.6–2.7.  Тест 13 | * 1. Ознакомьтесь с кнопкой «Пожаловаться» в социальной сети «ВКонтакте».   2. Ознакомьтесь с видеоматериалами. Обсудите в группе, кто такие тролли в Интернете и как с ними бороться, как защититься от нежелательных обращений. Сайт «Защита детей. Лаборатория Касперского».   «Фиксики: Фикси-советы: Осторожней в Интернете! Тролли»: <http://gotourl.ru/11619> | | |
| 20  Тематическое планирование в 5–6 классах  41 | 2.5. Правила защиты от вирусов, спама, рекламы и рассылок | Задание 2.8.  Тест 14 | 2.8. Ознакомьтесь с видеоматериалами.  Обсудите в группе пути распространения вирусов в Интернете и методы борьбы с ними.  Сайт «Защита детей. Лаборатория Касперского».  «Фиксики — Вирус»: <http://gotourl.ru/11620> | | |
| 21 | 2.6. Правила защиты от негативных сообщений | Задания 2.9–2.10.  Тест 15 | * 1. Ознакомьтесь с видеоматериалами. Обсудите в группе, какие бывают виды сетевого мошенничества.   Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера: Мошенничество в Интернете»: <http://gotourl.ru/11621>   * 1. Ознакомьтесь с видеоматериалами.   Обсудите в группе, какая опасность может скрываться на сайтах, какие траты денег могут незаметно,  но настойчиво предлагаться.  Сайт «Защита детей. Лаборатория Касперского.   * Мультфильм «Приключения робота Каспера: Опасности на надежных сайтах»: [http://gotourl.ru/11622.](http://gotourl.ru/11622) * «Фикси-советы: Осторожней в Интернете! Встроенные покупки»: <http://gotourl.ru/11623> | | |
| 22 | 2.7. Правила общения в социальной сети | Задания 2.11–2.13.  Тест 16 | * 1. Ознакомьтесь с видеоматериалами. Обсудите в группе следующие вопросы.   Что недопустимо при общении в социальной сети с незнакомцами?  Можно ли полностью доверять информации, которую размещают на своих страничках участники социальной сети?  Можно ли соглашаться на встречу в реальном мире с незнакомцами из социальной сети?  Сайт «Защита детей. Лаборатория Касперского».  «Фикси-советы: Осторожней в Интернете! Профили»: <http://gotourl.ru/11624>   * 1. Вместе с учителем или родителями внимательно прочитайте текст в социальной сети на страницах   о системе помощи.   * Система помощи в социальной сети «ВКонтакте»: [http://gotourl.ru/11597.](http://gotourl.ru/11597) * Система помощи в социальной сети YouTube: [http://gotourl.ru/15601.](http://gotourl.ru/15601) * Система помощи в социальной сети «Одноклассники»: [http://gotourl.ru/15607.](http://gotourl.ru/15607)   2.13. Ознакомьтесь с видеоматериалами. Составьте памятку поведения в социальных сетях на тему информационной безопасности. | | |
| 43 |  |  | Сайт телеканала «Карусель»: [http://gotourl.ru/15446.](http://gotourl.ru/15446) Видеоурок «Почемучка. Как вести себя в социальных сетях?» | |
| 23 | 2.8. Правила работы  с поисковыми системами и анализ информации | Задания 2.14–2.15.  Тест 17 | * 1. Ознакомьтесь с видеоматериалами. Обсудите   в группе, что такое пиратские сайты и почему они так называются.  Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера: Пиратские сайты»: [http://gotourl.ru/11630.](http://gotourl.ru/11630)   * 1. Ознакомьтесь с видеоматериалами. Обсудите в группе, что такое ложная информация и как ее распознать.   Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера: Ложная информация»: <http://gotourl.ru/11632> | |
| 24 | 2.9. Правила ответственности за распространение ложной и негативной информации | Задания 2.16–2.17 | 2.16. Вместе с родителями или учителем найдите в сети Интернет Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Ознакомьтесь с его содержанием. | |
|  |  |  | 2.17. Ознакомьтесь с видеоматериалами. Обсудите  в группе, как общество защищает детей в Интернете.   * Как обнаружить ложь и остаться правдивым в Интернете: [http://gotourl.ru/11639.](http://gotourl.ru/11639) * Защита персональных данных. Детская безопасность в Интернете: <http://gotourl.ru/11642> | |
| 25 | 2.10. Правила защиты от нежелательных сообщений и контактов | Задание 2.18 | 2.18. Ознакомьтесь с видеоматериалами. Обсудите в группе, какие угрозы подстерегают вас при общении с незнакомцами.  Сайт «Защита детей. Лаборатория Касперского».   * Мультфильм «Приключения робота Каспера: Опасность встречи в реале»: [http://gotourl.ru/11652.](http://gotourl.ru/11652) * Мультфильм «Приключения робота Каспера: Никогда не разговаривайте с неизвестными»: <http://gotourl.ru/11653> | |
| 26 | 2.11. Правила вызова экстренной помощи | Задание 2.19 | 2.19. Ознакомьтесь с сайтом «Пространство безопасности. Школа первой помощи». Раздел «Телефоны первой помощи»: [http://gotourl.ru/11654.](http://gotourl.ru/11654)  Составьте памятку по основным сведениям, которые вы должны сообщить при вызове экстренных служб | |
| 2.12. Правила защиты устройств от внешнего вторжения | Задание 2.20.  Тест 18 | 2.20. Ознакомьтесь с видеоматериалами. Обсудите в группе правила подборки паролей. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера: Пароли»: <http://gotourl.ru/11655> | |
| 27 | 2.13. Правила выбора полезных ресурсов  в Интернете | Задания 2.21–2.23 | 2.21. Российская государственная детская библиотека: <http://gotourl.ru/11601> | |
|  |  |  | Раздел «Национальная электронная детская библиотека»: <http://gotourl.ru/11602.>  Ознакомьтесь с каталогом книг, коллекцией диафильмов, архивом детских журналов.   * 1. Аудиохрестоматия: [http://gotourl.ru/11603.](http://gotourl.ru/11603)   «Аудиохрестоматия» — это медиапортал, на котором собраны произведения мировой литературы в исполнении известных артистов, а также биографии писателей.  Выберите писателя, ознакомьтесь с его биографией.   * 1. Детская электронная библиотека: [http://gotourl.ru/11604.](http://gotourl.ru/11604)   Прочитайте инструкцию о регистрации в электронной библиотеке. Пройдите регистрацию с помощью учителя или родителей |
| 28 | 2.14. Средства работы в Интернете для людей с особыми потребностями | Задания 2.24–2.25 | * 1. Ознакомьтесь с сайтом Всероссийского общества слепых.   Сайт Всероссийского общества слепых: [http://gotourl.ru/11605.](http://gotourl.ru/11605)   * 1. Для поддержки людей с ограниченными возможностями по зрению специально создан социально-информационный проект Nvda.ru.   Бесплатная программа экранного доступа Nvda: [http://gotourl.ru/11606.](http://gotourl.ru/11606)  Ознакомьтесь с разделом Web-радио на сайте проекта Nvda |
| 29–30 | Контрольный урок | Контрольное задание  к части 2 | Выполните задания:   * сайт «Защита детей. Лаборатория Касперского»: [http://gotourl.ru/11607.](http://gotourl.ru/11607)   Тест-викторина:   * сайт «Единый урок безопасности в сети Интернет»: [http://gotourl.ru/15609.](http://gotourl.ru/15609)   Контрольная работа для младшей группы:   * сайт «Лига безопасного интернета»: [http://gotourl.ru/15610.](http://gotourl.ru/15610)   Тест «Безопасный Интернет»:   * портал «Персональные данные. Дети»: [http://gotourl.ru/15611.](http://gotourl.ru/15611)   Тест «Что ты знаешь о персональных данных?»: <http://gotourl.ru/15612> |

**Тематическое планирование в 9–11 классах**

Тематическое планирование учебного курса для 9-11 кл.

Курс «Кибербезопасность» разработан для учащихся 9-11 классов и предлагается к изучению как курс по выбору образовательной организации в рамках предметов «Цифровая гигиена». Курс рассчитан на 34 часа.

К учебному пособию на сайте издательства размещено бесплатное электронное приложение. Оно включает ресурсы для выполнения практических заданий к урокам из пособия, а также открытые электронные документы и ресурсы для 7–9 классов: [**http://gotourl.ru/15613**.](http://gotourl.ru/15613)

Все электронные ресурсы выложены на основе наличия открытого доступа к ним.

К каждому модулю предлагается практическая работа на компьютерах. По итогам изучения модуля учащимся проводится тест.

К каждому параграфу предусмотрен набор заданий по теме для обсуждения и выполнения на уроке, в том числе с использованием электронного приложения.

Организация учебной деятельности на уроке включает теоретическую, понятийную часть с использованием видеоматериалов и документов в электронном приложении, дискуссию по вопросам к параграфу, выполнение практической части задания к параграфу на компьютере.

В курсе используется ряд новых терминов, которые сформировались недавно.

Достижения науки и техники, создание всемирной сети Интернет позволили преступности выйти на новый уровень и захватить *киберпространство*. Теперь злоумышленнику не нужен прямой контакт с жертвой и всего несколько человек могут стать угрозой для каждого пользователя глобальной паутины, крупных корпораций и целых государств.

*Кибертерроризм* и использование виртуального пространства для совершения актов насилия, а также другие деяния,

посягающие на общественную безопасность, включаются в **пятую группу** киберпреступлений.

Количество киберпреступлений, совершаемых в мире, неуклонно растет. Меняется и их качественный состав, и размер причиненного ущерба. Такое торжество преступности в виртуальном пространстве не может обойтись безнаказанно. Законодательство большинство стран мира предполагает *уголовную ответственность за совершение правонарушений данного вида*.

Пособие включает четыре раздела.

Введение.

Раздел 1. Киберпространство (11 часов). Киберпространство. Кибермиры. Киберфизическая система. Киберобщество. Киберденьги. Кибермошенничество.

Практикум к разделу 1. Практическая работа на основе онлайн-курса Академии Яндекса «Безопасность в Интернете» по теме «Безопасные онлайн-платежи».

Тест к разделу 1.

Раздел 2. Киберкультура (11 часов).

Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии.

Практикум к разделу 2. Практическая работа от компаний мобильной связи «Билайн», МТС и «Мегафон» (по выбору учащихся).

Тест к разделу 2.

Раздел 3. Киберугрозы (11 часов).

Кибервойны. Киберпреступность. Примеры киберпреступлений. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты. Новые профессии в киберобществе.

Практикум к разделу 3. Практическая работа на основе онлайн-курса Академии Яндекса «Безопасность в Интернете» (продолжение) по темам:

* защита от вредоносных программ;
* безопасность аккаунтов. Логины и пароли от электронной почты, социальных сетей и других сервисов.

Тест к разделу 3.

Раздел 4. Проверь себя.

Содержит тесты к трем тематическим разделам.

Тематическое планирование уроков информационной безопасности

в 9–11 классах

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Модуль** | **Параграфы в учебном пособии** | **Всего часов** | | **Теория** | | **Практическая работа** | |
| ***Модуль 1*** | Раздел 1. Киберпространство | ***11*** | | ***5*** | | ***6*** | |
| Киберпространство | Киберпространство. Кибермиры. Киберфизическая система.  Киберобщество. Киберденьги. Кибермошенничество | 8 | | 4 | | 4 | |
| Практикум | Практическая работа на основе онлайн- курса Академии Яндекса «Безопасность в Интернете» по теме «Безопасные онлайн-платежи» | 2 | |  | | 2 | |
| Контрольное занятие | Тест к разделу 1 | 1 | | 1 | |  | |
| ***Модуль 2*** | Раздел 2. Киберкультура | ***11*** | | ***5*** | | ***6*** | |
| Киберкультура | Киберкультура.  От книги к гипертексту. Киберкнига. Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии | 8 | | 4 | | 4 | |
| Практикум | Практическая работа от компаний мобильной связи «Билайн», МТС и  «Мегафон» (по выбору учащихся) | 2 |  | | 2 | |
| Контрольное занятие | Тест к разделу 2 | 1 | 1 | |  | |
| ***Модуль 3*** | Раздел 3. Киберугрозы | ***11*** | ***5*** | | ***6*** | |
| Киберугрозы | Кибервойны. Киберпреступность. Примеры киберпреступлений.  Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты. Новые профессии в киберобществе | 8 | 4 | | 4 | |
| Практикум | Практическая работа на основе онлайн- курса Академии Яндекса «Безопасность в Интернете» (продолжение) по темам: защита от вредоносных программ; безопасность аккаунтов | 2 |  | | 2 | |
| Контрольное занятие | Тест к разделу 3 | 1 | 1 | |  | |
| ***Всего по курсу*** | ***Модули 1–3*** | ***33*** | ***15*** | | ***18*** | |

СПИСОК ИСТОЧНИКОВ

1. Роскомнадзор: официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. — URL: [http://rkn.gov.ru/.](http://rkn.gov.ru/)
2. Цветкова М. С. Информационная безопасность. Правила безопасного Интернета: 2–4 классы: учебное пособие / М. С. Цветкова, Е. В. Якушина. — М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.
3. Цветкова М. С. Информационная безопасность. Безопасное поведение в сети Интернет: 5–6 классы: учебное пособие/ М. С. Цветкова, Е. В. Якушина. — М.: БИНОМ. Лаборатория знаний, 2020. — 96 с.
4. Цветкова М. С. Информационная безопасность. Кибер- безопасность. 7–9 классы: учебное пособие / М. С. Цветкова, И. Ю. Хлобыстова. — М.: БИНОМ. Лаборатория знаний, 2020. — 64 с.
5. Цветкова М. С. Информационная безопасность. Правовые основы информационной безопасности: 10–11 классы: учебное пособие / М. С. Цветкова, С. В. Голубчиков, В. К. Новиков [и др.]. — М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.
6. Сайт электронного приложения к пособиям по информационной безопасности. — URL: [http://gotourl.ru/15614.](http://gotourl.ru/15614)
7. Безопасный Билайн / компания «Билайн», URL: [http://gotourl.ru/15615.](http://gotourl.ru/15615)
8. Безопасность / компания МТС. — URL: <http://gotourl.ru/15616>
9. Безопасное общение / компания «Мегафон». — URL: <http://gotourl.ru/15617>
10. Памятка по безопасному общению / компания «Мегафон» — URL: