М. С. Цветкова

Информационная безопасность

2–11 классы

Методическое пособие для учителя

МОСКВА
«Просвещение»
2021

УДК 372.8
ББК 32.97
Ц27

Ц27 **Цветкова, М. С.** Информационная безопасность. 2–11 классы : методическое пособие для учителя : [издание в pdf-формате] / М. С. Цветкова. — М. : Просвещение, 2021. — 64 с. : ил. — Текст : электронный.

Методическое пособие представляет примерную программу по учебным курсам информационной безопасности, разработанным на основе учебных пособий в серии «Информационная безопасность» для 2–4, 5–6, 7–9 и 10–11 классов. Включает пояснительную записку, планируемые предметные результаты освоения курса, содержание курса с указанием форм организации учебных занятий, основных видов учебной деятельности, календарно-тематическое планирование с указанием количества часов, отводимых на освоение каждой темы. Курс поддержан электронным приложением на сайте издательства http://lbz.ru/metodist/authors/ib/.

Для учителей, методистов и преподавателей профессионального образования.

УДК 372.8
ББК 32.97

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Курс 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 необходимо 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.

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 последствий 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 в Интернете 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: начальных классов, 5–6 классов, 7–9 и 10–11 классов.

Начинать обучение по курсу информационной безопасности крайне актуально для детей начальной школы с дальнейшим развитием в 5–6 классах тем курса по острым проблемным ситуациям при самостоятельной бесконтрольной

работе детей в сети Интернет и при использовании мобильных телефонов, при использовании Интернета для творческого и развивающего досуга, познавательной деятельности и, конечно, для успешной учебы. Такое обучение направлено на решение вопросов массового формирования начальной цифровой грамотности, информационной культуры младших школьников, которые живут в современном информационном обществе, стремительно расширяющем общедоступные коммуникации в Интернете.

Курс для младших школьников включает в себя основные вопросы безопасного поведения в сети Интернет, методов предупреждения и защиты от негативного стороннего воздействия, звонков и сообщений от неизвестных лиц, подробного информирования школьников и их родителей о возможных рисках, которые подстерегают их в сети, сетевой этики, а также информацию о позитивном контенте в Интернете. В содержание курса для младших школьников включена подборка полезных открытых и безопасных электронных ресурсов, видеоматериалов, которые помогут повысить наглядность в проведении тематических уроков по безопасности детей в сети Интернет.

Риски, с которыми дети 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 также 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 популяризации полезных интернет-ресурсов.

«Информационные войны» в глобальном цифровом пространстве породили новые угрозы для общества — кража 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, умения 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, использованию цифровых технологий в быту на основе «умных» технологий, направлениях развития современного киберискусства, использования 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,
- киберугорозы,
- кибератака,
- киберпреступность,
- киберкультура...

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

Курс для учащихся 10–11 классов включает изучение правовой грамоты в сфере информационной безопасности, включая основные виды 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 [1],

на основании которых рекомендуется проектная работа, например составление информационной листовки, буклета по темам:

- персональные данные http://rkn.gov.ru/personal-data/protection-of-the-innocent/
- контроль и надзор в сфере информационных технологий http://rkn.gov.ru/it/control/
- контроль и надзор в сфере связи http://rkn.gov.ru/communication/control/
- контроль и надзор в сфере массовых коммуникаций http://rkn.gov.ru/mass-communications/

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: «Окружающий мир» для 2–4 классов, «Информатика» и ОБЖ для 5–6 и 7–9 классов, «Обществознание» и «Информатика» (раздел «Социальная информатика») для 10–11 классов, например:

– 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 предметах.

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 для устранения 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 работе с информацией по 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 2–4, 5–6, 7–9 и 10–11 классов [2, 3, 4, 5], снабженных открытыми электронными материалами на сайте издательства БИНОМ [6].

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 [7, 8, 9, 10, 11].

В таблице представлены примеры видов деятельности обучающихся по ФГОС, которые можно использовать во время проведения уроков на основе следующих источников: учебные пособия, электронные ресурсы (электронные практикумы и курсы ИТ-компаний), дополнительные материалы (сайты, видеоматериалы).

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	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

Учебная деятельность учащихся	2–4 и 5–6 классы	7–9 классы	10–11 классы
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 учебно-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 антибуллингового поведения • применение правил защиты от мошенников в сети Интернет • самоорганизация сбалансированного использования цифровых устройств для рабочего и досугового времени	Индивидуальная работа: • использование правовых норм информационой безопасности в жизни и сетевой активности • личное участие в проектах по распространению правовых норм в сфере информационой безопасности

Учебная деятельность учащихся по курсу информационной безопасности включает также направления проектной деятельности для 2–11 классов.

Конкурс рисунков «Правила поведения в сети Интернет» по темам информационной безопасности для 2–4 и 5–6 классов.

Конкурс кроссвордов — презентаций «Цифровая гигиена» для детей 5–6 классов.

Клуб «Киберпатруль».

Команда 1 учащихся 7–9 классов разрабатывает материалы и проводит мероприятия по сбору материалов, конструированию и оформлению информационного школьного стенда по информационной безопасности с использованием детских рисунков.

Команда 2 учащихся готовит информационный листок для родителей по информационной безопасности, памятки в классы.

Команда 3 проводит викторину «Цифровая гигиена» по информационной безопасности для 2–4 и 5–6 классов.

Команда 4 готовит видеорепортажи с турниров и конкурсов по информационной безопасности в школе.

Клуб «Кибербудущее».

Команда учащихся 7–9 классов отбирает материалы в СМИ и выпускает медиажурнал «Кибербудущее» в электронной форме в виде страницы сайта или в виде презентации. Медиажурнал выпускается в школе 1 раз в четверть, всего 4 выпуска за год по 4 темам с подборками новинок киберпространства:

1. Киберкультура (киберкниги, киберискусство, киберперформанс)
2. Кибертехника (космос, медицина, промышленность, энергетика, беспилотники)
3. Кибердом (интернет вещей, умный дом)
4. Киберэкономика (киберденьги, биг-дата (большие данные), кибервойны, кибермошенники)

Турнир «Киберобщество».

Команда учащихся 10–11 классов готовит два набора заданий и проводит ежегодный турнир по основам информационной безопасности в два этапа: полуфинал и финал. В работу

команд входит разработка тестов для проведения этапов турнира по возрастным группам в формах:

- Викторина «Цифровая гигиена» (для 2–4 классов)
- Кроссворд-презентация «Цифровая гигиена» — выбор ответа по изображенной ситуации (для 5–6 классов)
- Квест по предложенной траектории на тему угроз с практическими работами на компьютере (для 7–9 классов)
- Правовой тур по информационной безопасности (для 10–11 классов)

Рекомендуется также провести конкурс на разработку логотипа и проекта кубка для кибертурнира.

В рамках проекта обеспечивается выбор оргкомитета турнира, группы разработчиков заданий, жюри турнира. Участниками являются команды от классов.

Команды победители получают кубок в каждой возрастной группе.

Видеорепортажи с турниров готовит команда клуба «Киберпатруль».

Разработка всех проектов проводится в соответствии с планом на основе выбора проблемы в составе работы клуба:

1. Анализ проблемы, разработка плана презентации или подборки плакатов по выявленным актуальным вопросам.
2. Сбор информации по каждому вопросу. Анализ полученной информации. Подготовка текстового сообщения по вопросу.
3. Разработка иллюстрации или схемы к слайду/плакату.
4. Конструирование слайдов или набора электронных плакатов с использованием анимации, роликов.
5. Представление презентации или плакатов для экспертизы и обсуждения в клубе.
6. Использование материалов проекта на школьных мероприятиях.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

Учебно-тематическое планирование учебного курса для 2–4 классов

Курс может быть реализован учебным курсом на 30 часов, а также в рамках занятий по предмету «Информатика» (2–4, 3–4 классы), или включен темами в занятия по предмету «Окружающий мир» (2–4 классы) в форме проведения тематических уроков, а также проведен в рамках школьных мероприятий: уроков-дискуссий, цикла бесед для классных часов с участием родителей в 1–4 классах по модулям учебно-тематического планирования.

Вариант 1. Планирование обучения по модулям со 2 по 4 классы.

2 класс: модуль 1, всего 10 уроков.

3 класс: модули 2 и 3, всего 14 уроков.

4 класс: модуль 4, всего 6 уроков.

Вариант 2. Планирование обучения в 3–4 классах.

3 класс: Модули 1 и 2, всего 17 уроков.

4 класс модули 3 и 4, всего 13 уроков.

Вариант 3. Планирование проведения уроков в 4 классе.

Один урок в неделю. 30 уроков

Курс представлен в учебном пособии «Информационная безопасность. Правила безопасного Интернета. 2–4 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 2–4 классов **http://lbz.ru/metodist/authors/ib/2-4.php**

Курс включает 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.

№ 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://lbz.ru/metodist/authors/ib/2-4.php**
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 «Вай-Фай» 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	1.1. 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. 1.2. Ознакомься с видеоуроком 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://lbz.ru/metodist/authors/ib/2-4.php**
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://www.safety.mts.ru/ru/deti_v_inete/for_children/rules/)
		Проектное задание 2.3	2.3. Посмотри дома с вместе со взрослыми или на уроке с помощью учителя видеоурок СПАС Экстрим «Безопасный Интернет». Составь личную памятку безопасности в сети Интернет
7 часов	**Модуль 3. Путешествуем в сети Интернет**		**http://lbz.ru/metodist/authors/ib/2-4.php**
18	3.1. Поиск информации в Интернете		Ознакомься с материалами сайта и используй их для разнообразия своего досуга. 3.1. *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. 3.2. *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	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. 3.4. *Электронное учебное пособие «Учимся беречь энергию» «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. 3.5. *Сайт Lingualeo. Покори язык.* Lingualeo — это увлекательный, эффективный и бесплатный сервис для изучения английского языка. 3.6. *Сайт Учи.ру.* Учащиеся из всех регионов России изучают школьные предметы в интерактивной форме. 3.7. *Сайт «Российская электронная школа».* Сайт с материалами об окружающем мире. 3.8. *Сайт Московского планетария.* Сайт коллекций Московского планетария поможет познакомиться с миром космоса. 3.9. *Московский зоопарк. Видео.* Живое видео из вольеров зоопарка поможет проводить наблюдения за жизнью животных в зоопарке, что поможет в изучении окружающего мира.

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/ Электронное приложение
			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	3.11. *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. 3.12. *Аудиохрестоматия.* Выбери произведение, прослушай его. «Аудиохрестоматия» — это уникальный портал аудиозаписей книг, на котором собраны лучшие произведения мировой литературы в исполнении признанных мастеров сцены. 3.13. *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	3.6. Сайты с коллекциями для детей	Задания 3.14–3.17	3.14. *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. 3.15. *Журнал «Мурзилка».* Ознакомься с разделом «Авторы Мурзилки читают свои произведения». 3.16. *Теремок.* Ознакомься с уроками безопасности для детей. 3.17. *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: • союзмультфильм • российская детская библиотека • началка инфо • телеканал карусель • аудиохрестоматия Перейди на нужные сайты и добавь их в систему закладок, используя сочетания клавиш Ctrl+D.

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/ Электронное приложение
			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://lbz.ru/metodist/authors/ib/2-4.php**
25	4.1. Социальные сети для детей 4.2. Что такое Аватар и как его выбрать 4.3. «Друг» в сети, кто за ним прячется	Тест 15 Тест 16 Тест 17	
26	4.4. Ложные сообщения 4.5. Что говорить о себе незнакомцам 4.6. Спроси совета в семье	Тест 18 Тест 19 Тест 20	
27	4.7. Этикет в общении 4.8. Нельзя обижать 4.9. Если тебя обижают	Тест 21 Тест 22 Тест 23	

28	4.10. Защити себя от недоброжелателей 4.11. Если тебе угрожают 4.12. Агрессия и грубость	Тест 24 Тест 25 Тест 26	
29	4.13. Уговоры и предложения 4.14. Отключение от нежелательных контактов	Тест 27 Тест 28	
30	Контрольный урок. Итоговый урок-викторина	Задания 4.1–4.3. Рассказ Смайлика	4.1. Оцени свой этикет в социальных сетях. Ответь на вопрос: какой смайлик выберешь к каждому утверждению в таблице. 4.2. Ответь на вопрос: что ты сделаешь в предложенных ситуациях? Выбери правильный ответ к каждой из предложенных ситуаций. 4.3. 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 5–6 классов

Курс представлен в учебном пособии «Информационная безопасность. Безопасное поведение в сети Интернет. 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://lbz.ru/metodist/authors/ib/5-6.php**

Для школьников 5–6 классов курс включает две части и рассчитан на 30 уроков, 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

1.1. История создания сети Интернет

1.2. Что такое Всемирная паутина?

1.3. Путешествие по сети Интернет: сайты и электронные сервисы

1.4. Как стать пользователем Интернета?

1.5. Опасности для пользователей Интернета

1.6. Что такое кибератака

1.7. Что такое информационная безопасность

1.8. Законы о защите личных данных в Интернете

1.9. Сетевой этикет

1.10. Коллекции сайтов для детей

1.11. Электронные музеи

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

2.1. Правила работы с СМС

2.2. Правила работы с электронной почтой

2.3. Правила работы с видеосервисами

2.4. Правила работы в социальных сетях

2.5. Правила защиты от вирусов, спама, рекламы и рассылок

2.6. Правила защиты от негативных сообщений

2.7. Правила общения в социальной сети

2.8. Правила работы с поисковыми системами и анализ информации

2.9. Правила ответственности за распространение ложной и негативной информации

2.10. Правила защиты от нежелательных сообщений и контактов

2.11. Правила вызова экстренной помощи

2.12. Правила защиты устройств от внешнего вторжения

2.13. Правила выбора полезных ресурсов в Интернете

2.14. 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.

Варианты учебного планирования:

Вариант 1. Курс проводится как одногодичный в 5 или в 6 классе по выбору образовательной организации. Курс рассчитан на 1 урок в неделю. 30 уроков за учебный год.

Вариант 2. Курс проводится по полугодиям в 5 и 6 классах, по 15 уроков в каждом классе.

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php
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 информационной 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. Сайт «Безопасный Интернет для детей»: http://i-deti.org/video/ • Видеоролик «Угрозы Интернета для детей» • Видеоролик «Мировой опыт защиты детей в Интернете»

3	1.1. История создания сети Интернет	Тест 1. Задания 1.2–1.3	1.2. Ознакомьтесь с видеоматериалами. Обсудите их в группе и ответьте на вопрос: где находится Интернет? Сайт телеканала «Карусель»: https://www.karusel-tv.ru/ Видеоролик «Почемучка. Где находится Интернет?». 1.3. Придумайте кроссворд на базе слова «Интернет»
4	1.2. Что такое Всемирная паутина	Задания 1.4–1.5. Тест 2	1.4. На сайте телеканала «Карусель» посмотрите разделы сайта, используя слова-меню. 1.5. Ознакомьтесь с видеоуроком телеканала «Карусель»: : https://www.karusel-tv.ru/ «Почемучка. Что такое веб-браузер»? 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	1.6. Выполните поиск сайта телеканала «Карусель» с помощью поисковой системы Яндекс. Выберите нужную ссылку и перейдите на этот сайт. 1.7. Ознакомьтесь с видеоуроком телеканала «Карусель»: «Почемучка. Поисковая система». Ответьте на вопрос: что такое поисковые системы и для чего они предназначены? 1.8. Познакомьтесь с сайтом «Культура.РФ». Обсудите в группе, какие разделы вы находите наиболее интересными для себя, что понравилось больше всего. 1.9. Ознакомьтесь с детской социальной сетью «Лунтик»: www.luntik.ru, представляющей российские и зарубежные мультфильмы для детей

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php
6	1.4. Как стать пользователем Интернета	Задание 1.10. Тест 4	1.10. Ознакомьтесь с видеоуроком телеканала «Карусель»: «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	1.11. На сайте Большой Российской Энциклопедии: https://bigenc.ru/ перейдите в раздел «Россия» и ознакомьтесь с рубриками раздела. 1.12. 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	1.13. Ознакомьтесь с видеоматериалами. Ответьте на вопросы: что такое компьютерный вирус? Чем он опасен для компьютера? Сайт телеканала «Карусель»: https://www.karusel-tv.ru/, видеоурок «Почемучка. Вирусы» 1.14. Ознакомьтесь с видеоматериалами. Обсудите действия героя в ситуации кибербуллинга и фишинга. Сайт «Защита детей. Лаборатория Касперского». • Мультфильм «Приключения робота Каспера — Кибербуллинг»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-kiberbulling/; • Мультфильм «Приключения робота Каспера — Фишинг»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-fishing/

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»: https://www.karusel-tv.ru/. Видеоурок «Почемучка. Безопасность при работе в Интернете»
10	1.8. Законы о защите личных данных в Интернете	Задания 1.16–1.18 Тест 8	1.16. Портал «Лига безопасного Интернета». Ознакомьтесь с видеоуроком «Защита персональных данных детей». 1.17. Сайт «Персональныеданные.Дети». Пройдите электронный тест «Что ты знаешь о персональных данных». 1.18. 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: https://kids.kaspersky.ru/entertainment/ficksics/fiksi-sovety-ostorozhnej-v-internete-konfidentsialnost/ • Мультфильм «Приключения робота Каспера — Общение в игре»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-privatnost-akkauntov-2/

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php
11	1.9. Сетевой этикет	Задания 1.19–1.20. Тест 9	1.19. 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? 1.20. 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 — Овершеринг. Вред репутации»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-overshering-vred-reputatsii/
12	1.10. Коллекции сайтов для детей	Задания 1.21–1.23	1.21. Ознакомьтесь с видеоматериалами. Обсудите в группе, что такое «позитивный контент». Сайт «Безопасный Интернет для детей»: http://i-deti.org/ Знакомимся с Интернетом: http://i-deti.org/video/ 1.22. Ознакомьтесь с разделами интернет-браузера «Гогуль: Играй, Гуляй, Общайся, Учись». 1.23. 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	1.24. Русский музей в Санкт-Петербурге. Виртуальный филиал: http://www.virtualrm.spb.ru/ru/resources/galleries. Ознакомьтесь с виртуальными экскурсиями. 1.25. Третьяковская галерея в Москве. Электронные коллекции: https://www.tretyakovgallery.ru/collection/ Ознакомьтесь с залами Музея с помощью онлайн-панорамы: https://artsandculture.google.com/partner/the-state-tretyakovgallery 1.26. Музей изобразительных искусств имени А. С. Пушкина в Москве. Электронная коллекция: http://www.artsmuseum.ru/collections/index.php Выберите тематику и посетите электронную экспозицию Музея изобразительных искусств имени А. С. Пушкина. 1.27. Эрмитаж. Виртуальное путешествие: https://www.hermitagemuseum.org/wps/portal/hermitage/panorama?lng=ru Выберите виртуальное путешествие по Эрмитажу. Раздел на сайте «Панорамные туры»: https://polymus.ru/ru/museum/fonds/panoramic/ 1.28. Политехнический музей в Москве. Раздел на сайте «Панорамные туры». Выберите тур на сайте Политехнического музея и ознакомьтесь с его экспозицией на своем компьютере

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php
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. Сайт «Лига безопасного Интернета» Практикум «Азбука информационной безопасности» (Лаборатория Касперского): http://ligainternet.ru/upload/docs/docs-for-dowloud/Azbuka_informatsionnoy_bezopasnosti.pdf
	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»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-drug-vovka/ • Мультфильм «Приключения робота Каспера — Приватность аккаунтов»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-privatnost-akkauntov/

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»: https://www.karusel-tv.ru/, 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»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-soobshheniya-so-zlomannyh-akkauntov/
18	2.3. Правила работы с видеосервисами	Задания 2.4–2.5. Тест 12	2.4. Ознакомьтесь с системой помощи по работе с видеозаписями в социальной сети ВКонтакте: https://vk.com/support. 2.5. 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»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-pokupki-v-igrah/

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php
19	2.4. Правила работы в социальных сетях	Задания 2.6–2.7. Тест 13	2.6. Ознакомьтесь с кнопкой «Пожаловаться» в социальной сети ВКонтакте. **2.7.** 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: https://kids.kaspersky.ru/entertainment/ficksics/fiksisovetyostorozhnej-v-internete-trolli/
20	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: Фиксики — Вирус: https://kids.kaspersky.ru/entertainment/ficksics/fiksiki-virus-fixiki/
21	2.6. Правила защиты от негативных сообщений	Задания 2.9–2.10. Тест 15	2.9. Ознакомьтесь с видеоматериалами. Обсудите в группе, какие бывают виды сетевого мошенничества. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Мошенничество в Интернете»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-moshennichestvo-v-internete/

			2.10. 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»: https://kids.kaspersky.ru/entertainment/opasnosti_na-saitah/ • Фиксики: Фикси-советы: Осторожней в Интернете! — Встроенные покупки: https://kids.kaspersky.ru/entertainment/ficksics/fiksi-sovetyostorozhnej-v-internete-vstroennye-pokupki/
22	2.7. Правила общения в социальной сети	Задания 2.11–2.13. Тест 16	2.11. 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». Фиксики: Фикси-советы: Осторожней в Интернете! — Профили: https://kids.kaspersky.ru/entertainment/ficksics/fiksi-sovetyostorozhnej-v-internete-profili/

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php
			2.12. Вместе с учителем или родителями внимательно прочитайте текст в социальной сети на страницах о системе помощи. • Система помощи в социальной сети ВКонтакте: https://vk.com/support • Система помощи в социальной сети Facebook: https://www.facebook.com/help/ • Система помощи в социальной сети Одноклассники: https://www.ok.ru/help 2.13. Ознакомьтесь с видеоматериалами. Составьте памятку поведения в социальных сетях на тему информационной безопасности. Сайт телеканала «Карусель»: https://www.karusel-tv.ru/ 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	2.14. 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»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-piratskie-sajty/

			2.15. 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»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-lozhnaya-informatsiya/
24	2.9. Правила ответственности за распространение ложной и негативной информации	Задания 2.16–2.17	2.16. Ознакомьтесь с законами, представленными на сайте «Безопасный Интернет для детей»: http://i-deti.org/ в разделе «Законодательство». 2.17. Ознакомьтесь с видеоматериалами. Обсудите в группе, как общество защищает детей в Интернете. Сайт «Безопасный Интернет для детей»: http://i-deti.org/ Как обнаружить ложь и остаться правдивым в Интернете: http://i-deti.org/video/ • Защита персональных данных. Детская безопасность в Интернете: http://i-deti.org/video/
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»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-opasnost-vstrechi-v-reale/

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php
			• Мультфильм «Приключения робота Каспера — Никогда не разговаривайте с неизвестными»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-nikogda-ne-razgovarivajte-sneizvestnymi/
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://allsafety.ru/first_aid/telefon.htm 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»: https://kids.kaspersky.ru/entertainment/priklyucheniya-robota-kaspera-paroli/
27	2.13. Правила выбора полезных ресурсов в Интернете	Задания 2.21–2.23	2.21. Российская государственная детская библиотека: https://rgdb.ru/ Раздел «Национальная электронная детская библиотека»: http://arch.rgdb.ru/xmlui/ Ознакомьтесь с каталогом книг, коллекцией диафильмов, архивом детских журналов.

			2.22. Аудиохрестоматия: http://audiohrestomatiya.ru/ «Аудиохрестоматия» — это медиапортал, на котором собраны произведения мировой литературы в исполнении известных артистов, а также биографии писателей. Выберите писателя, ознакомьтесь с его биографией. 2.23. Детская электронная библиотека: http://www.deti-book.info/ 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	2.24. Ознакомьтесь с сайтом Всероссийского общества слепых. Сайт Всероссийского общества слепых: http://www.vos.org.ru/ 2.25. Для поддержки людей с ограниченными возможностями по зрению специально создан социально-информационный проект Nvda.ru. Бесплатная программа экранного доступа Nvda: https://nvda.ru/ Ознакомьтесь с разделом Web-радио на сайте проекта Nvda.

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php
29–30	Контрольный урок	Контрольное задание к части 2	Выполните задания: • Сайт «Защита детей. Лаборатория Касперского»: https://kids.kaspersky.ru/entertainment/kak-vesti-sebya-v-internete/ Тест-викторина • Сайт «Единый урок безопасности в сети Интернет»: http://xn--d1abkefqip0a2f.xn--d1acj3b/?view=quiz&quiz_id=28 Контрольная работа для младшей группы. • Сайт «Лига безопасного интернета»: http://www.ligainternet.ru/encyclopedia-of-security/parents-andteachers/parents-and-teachers-detail.php?ID=3652 Тест «Безопасный Интернет» • Портал «Персональные данные — дети»: http://xn-80aalcbc2bocdadlpp9nfk.xn--d1acj3b/zadaniya/personalnye_dannye/ Тест «Что ты знаешь о персональных данных?»

Тематическое планирование учебного курса для 7–9 классов

Курс «Кибербезопасность» разработан для учащихся 7–9 классов и предлагается к изучению как курс по выбору образовательной организации в рамках рамках предметов «Информатика» или ОБЖ. Курс рассчитан на 33 часа и может реализоваться по 11 часов в качестве внеурочного модуля в 7, 8 и 9 классах, или как одногодичный курс в 8 или в 9 классах.

К курсу разработано учебное пособие «Кибербезопасность. 7–9 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 электронные документы и ресурсы для 7–9 классов **http://lbz.ru/metodist/authors/ib/7-9.php**

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

К каждому модулю предлагается практическая работа на компьютерах. По итогам изучения модуля учащимся предлагается 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 видео материалов и документов в электронном приложении, дискуссию по вопросам к параграфу, выполнение практической части в задании к параграфу на компьютере.

В курсе используется ряд новых терминов, которые сформировались недавно. Киберне́тика (от др.-греч. Κυβερνητική) — это «искусство управления». Теперь можно говорить не только о безопасности в интернете, но и о возможности управления информационным пространством в преступных или негативных целях. Достижения науки и техники, создание всемирной сети Интернет позволили преступности выйти на новый уровень и захватить *киберпространство*. Теперь преступнику 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 преступлений данного вида*.

Пособие включает четыре раздела.

Введение.

Раздел 1. Киберпространство. (11 часов)

Киберпространство. Кибермиры. Киберфизическая система. Кибероблество. Киберденьги. Кибермошенничество.

Практикум к разделу 1. Практическая работа на основе онлайн-курса Академии Яндекс «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 кибероблестве.

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.

Модуль	Параграфы в учебном пособии	Всего часов	Теоретические занятия	Практическая работа с ресурсами и программами на компьютере
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 Яндекс «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

Модуль	Параграфы в учебном пособии	Всего часов	Теоретические занятия	Практическая работа с ресурсами и программами на компьютере
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***

Тематическое планирование учебного курса для 10–11 классов

Курс рассчитан на 66 часов обучения, поддержан электронными ресурсами по каждой теме, ориентирован на работу обучающихся с документами в области законодательства Российской Федерации в сфере информационной безопасности. Курс может быть реализован в рамках раздела «Социальная информатика» предмета «Информатика» или предмета «Обществознание». Курс может проводиться также как учебный курс по выбору образовательной организации.

К курсу разработано учебное пособие «Правовые основы информационной безопасности. 10–11 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 электронные документы и ресурсы для 10–11 классов **http://lbz.ru/metodist/authors/ib/10-11.php**

Учебно-тематическое планирование разработано на основе учебного пособия по курсу для 10–11 классов. Пособие включает в себя практические работы по уровням «знать» и «применять», а также набор проектных заданий для выполнения в группах учащихся на компьютерах. К пособию для каждой темы на сайте издательства размещено электронное приложение с набором ссылок на материалы (документы, федеральные законы и ссылки к проектным работам) для использования на занятиях, возможно в демонстрационном режиме для использования педагогом при объяснении материала и организации обсуждений и дискуссий на занятиях. Все электронные ресурсы выложены на основе наличия открытого доступа к ним.

УТП включает обязательный для изучения курса теоретический раздел 1 (Модули 1–4). По каждому модулю предусмотрен индивидуальный зачет по предложенным в пособии вопросам.

В рамках изучения курса обучающимся предложен дополнительный практический раздел 2 (Модуль 5), где представлены проектные работы, которые включают набор учебных практических работ и изучение открытого онлайн-курса НОУ

Интуит «Основы информационной безопасности» с прохождением тестирования по итогам изучения курса. Раздел 2 курса учащиеся осваивают в компьютерном классе или в дистанционной форме.

Курс может изучаться разделами в 10 и 11 по 1 часу в неделю, или за один год в 10 или 11 классах по 2 часа в неделю.

Тематическое планирование уроков информационной безопасности в 10–11 классах

Модуль	Параграфы в учебном пособии	Всего часов	Теоретические занятия	Практическая работа на компьютере
Раздел 1				
Модуль 1. Правовые основы информационной безопасности	Глава 1. Понятия юридической ответственности за правонарушения в области информационной безопасности	***5***	***2***	***3***
1.1. Понятия юридической ответственности за правонарушения в области информационной безопасности	2. Основные документы в области информационной безопасности Российской Федерации 3. Информация как объект правовых отношений 4. Функции, принципы и виды юридической ответственности. 5. Субъективная и объективная стороны юридической ответственности	3	2	1
1.2. Контрольное занятие	Подготовка презентации по теме в группах учащихся	2		2
Модуль 2. Законодательство Российской Федерации о гражданско-правовой ответственности в сфере инфобезопасности	Глава 2. Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации)	***7***	***3***	***4***

Модуль	Параграфы в учебном пособии	Всего часов	Теоретические занятия	Практическая работа на компьютере
2.1. Законодательство Российской Федерации о гражданско-правовой ответственности	1. Общие положения законодательства Российской Федерации о гражданско-правовой ответственности. 2. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности (защиты информации)	3	2	1
2.2. Гражданско-правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации)	1. Ответственность за проступок в области присвоение авторства (плагиат) 2. Ответственность за проступок за оскорбления, в том числе в социальных сетях	3	1	2
2.3. Контрольное занятие	Индивидуальный зачет	1		1
Модуль 3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности	Глава 3. Административная ответственность за проступки в области информационной безопасности (защиты информации)	***12***	***6***	***6***
3.1. Понятие административной ответственности	1. Административное правонарушение. Основные понятия административного правонарушения. 2. Особенности административной ответственности несовершеннолетних.	2	1	1

3.2. Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации).	1. Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение 2. Ответственность за проступок — за оскорбления, в том числе в социальных сетях 3. Ответственность за проступок — ложный вызов экстренных служб 4. Ответственность за проступок — пропаганду в Интернете наркотических и психотропных веществ 5. Ответственность за проступок — нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные) 6. Ответственность за проступок — нарушение правил защиты информации 7. Ответственность за проступок — представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство 8. Ответственность за проступок — за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт	9	5	4

Модуль	Параграфы в учебном пособии	Всего часов	Теоретические занятия	Практическая работа на компьютере
	9. Ответственность за проступок — нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации			
3.3. Контрольное занятие	Индивидуальный зачет	1		1
Модуль 4. Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности	Глава 4. Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)	***14***	***7***	***7***
4.1. Понятие уголовной ответственности	1. Уголовный кодекс Российской Федерации 2. Виды наказаний в области уголовной ответственности	2	1	1
4.2. Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации)	1. Ответственность за преступления в области компьютерной информации и применения компьютеров 2. Ответственность за преступления в области присвоения авторства (плагиат)	11	6	5

	3. Ответственность за преступления в области нарушения авторских прав на лицензионное программное обеспечение 4. Ответственность за преступления в области мошенничества (обмана) 5. Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений 6. Ответственность за преступления — за проведение скрытой (негласной) аудиозаписи 7. Ответственность за преступления — за заведомо ложное сообщение о теракте 8. Ответственность за преступления — за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг) 9. Ответственность за преступления — за мошенничество в сфере компьютерной информации 10. Ответственность за преступления — за незаконное распространение порнографических материалов 11. Ответственность за преступления — за заведомо ложный донос			
4.3. Контрольное занятие	Индивидуальный зачет	1		1
Всего по разделу 1	***Модули 1–4***	***33***	***18***	***15***

				Практическая работа на компьютере
Часы самостоятельной работы	Самостоятельная работа для индивидуальных зачетов и подготовки презентаций (предоставляется в компьютерной форме)	5		5
Итого	***Раздел 1***	***38***	***18***	***20***
	Раздел 2			
Модуль 5. Практика применения правил и норм информационной безопасности	Глава 5. Проектные задания	***28***	***6***	***22***
5.1. Проектная работа. Нормативные основы лицензионных соглашений	1. Лицензионное соглашение свободного ПО Линукс. 2. Как купить лицензию на платную антивирусную программу. 3. Что такое CC лицензия. 4. Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию	3	2	2
5.2. Проектная работа. Практика соблюдения норм инфобезопасности в личном информационном пространстве	1. Как задавать безопасный пароль. Настройки телефона, планшета для защиты от несанкционированного доступа. 2. Защита персональных данных. Обзор. Личный контент в облаке и система его защиты	3	2	2

5.3. Самостоятельная дистанционная работа	Онлайн-курс «Основы информационной безопасности»	15		15
5.4 Контрольное занятие	Тест по онлайн курсу	1		1
Всего по разделу 2	***Модуль 5***	***24***	***4***	***20***
Резерв к разделу 2		***4***	***2***	***2***
Итого	***Раздел 2***	***28***	***6***	***22***
Всего часов по курсу (разделы 1 и 2)	За два года обучения (1 час в неделю) За один год обучения (2 часа в неделю)	***66***	***24***	***42***

СПИСОК ИСТОЧНИКОВ

1. Роскомнадзор, официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, URL: http://rkn.gov.ru/
2. Цветкова М. С., Якушина Е. В. Информационная безопасность. Правила безопасного Интернета. 2–4 классы : учебное пособие.— М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.
3. Цветкова М. С., Якушина Е. В. Информационная безопасность. Безопасное поведение в сети Интернет. 5–6 классы : учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 96 с.
4. Цветкова М. С., Хлобыстова И. Ю. Информационная безопасность. Кибербезопасность. 7–9 классы : учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 64 с.
5. Цветкова М. С., Голубчиков С. В., Новиков В. К., Семибратов А. М., Якушина Е. В. Информационная безопасность: Правовые основы информационной безопасности. 10–11 классы : учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.
6. Сайт электронного приложения к пособиям по информационной безопасности, URL: http://lbz.ru/metodist/authors/ib/
7. «Безопасный Билайн», компания Билайн, URL: http://moskva.beeline.ru/customers/help/safe-beeline/
8. «Безопасность», компания МТС, URL: http://www.safety.mts.ru/ru/
9. «Безопасное общение», компания Мегафон, URL: http://moscow.megafon.ru/bezopasnoe_obschenie/
10. «Памятка по безопасному общению», компания Мегафон, URL: http://moscow.megafon.ru/download/~msk/~moscow/stopfraud/brochure.pdf
11. Открытый онлайн-курс «Безопасность в Интернете», «Академия Яндекс», компания Яндекс, URL: https://academy.yandex.ru/events/online-courses/internet_security/

СОДЕРЖАНИЕ

Цветкова Марина Серафимовна

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

2–11 классы

Методическое пособие

Технический редактор *Е. В. Денюкова*
Корректор *Е. Н. Клитина*
Компьютерная верстка: *С. А. Янковая*

Формат 60x90/16. Усл. печ. л. 4,0.

Акционерное общество «Издательство «Просвещение»
Российская Федерация, 127473, г. Москва, ул. Краснопролетарская, д. 16,
стр. 3, этаж 4, помещение I.

Адрес электронной почты «Горячей линии» — **vopros@prosv.ru.**