

Муниципальное казённое общеобразовательное учреждение
«Основная общеобразовательная школа» с. Перетино Партизанского муниципального района
(МКОУ ООШ с. Перетино)

УТВЕРЖДЕНО
Директор МКОУ "ООШ" с.
Перетино

Жибарь Е. Ю.
приказ № 67
от «31» августа 2023 г.

РАБОЧАЯ ПРОГРАММА

Учебного курса «Информационная безопасность»

для обучающихся 5-6, 7-8 классов

Составитель: Степаненко Лариса Львовна
учитель информатики МКОУ "ООШ" с. Перетино

с. Перетино 2023

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Нормативную правовую основу настоящей примерной образовательной программы по учебному курсу «Информационная безопасность» составляют следующие документы:

- Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- ФГОС основного общего образования;
- ПООП основного общего образования;
- распоряжение Правительства РФ от 2 декабря 2015 г. № 2471-р «Об утверждении Концепции информационной безопасности детей»;
- Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы»;
- Перечень поручений по реализации Послания Президента Федеральному Собранию от 27 февраля 2019 г. Пр-294.

Программа учебного курса «Информационная безопасность» разработана для организаций, реализующих программы общего образования. *В ней учтены приоритеты научно-технологического развития Российской Федерации* (Пр-294, п.2а-16) и обновление программы воспитания и социализации обучающихся в школах Российской Федерации.

Цели изучения учебного курса «Информационная безопасность»

Безопасность в сети Интернет в свете быстрого развития 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, расширения угроз новых сетевых средств вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, а также в связи с массовым использованием детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним, резко повышает потребность в воспитании у обучающихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от агрессивной и противоправной информации.

Программа учебного курса информационной безопасности имеет высокую актуальность и отражает важные вопросы безопасной работы с новыми формами коммуникаций и услуг цифрового мира: потребность в защите персональной информации, угрозы, распространяемые глобальными средствами коммуникаций Интернета и мобильной связи, использующими рассылки сообщений, электронную почту, информационно-коммуникативные ресурсы взаимодействия в сети Интернет через массово доступные услуги электронной коммерции, социальные сервисы, сетевые объединения и сообщества, ресурсы для досуга (компьютерные игры, видео и цифровое телевидение, цифровые средства массовой информации и новостные сервисы), а также повсеместное встраивание дистанционных ресурсов и технологий в учебную деятельность, использующую поиск познавательной и учебной информации, общение в социальных сетях, получение и передачу файлов, размещение личной информации в коллективных сервисах. Помимо профилактики информационных угроз и противоправных действий через ресурсы в сети Интернет и мобильные сети, крайне

актуально использовать коммуникации для привлечения обучающихся к информационно-учебной и познавательно-творческой активности по использованию позитивных интернет-ресурсов: учебных, культурных, научно-популярных, интеллектуальных, читательских, медийных, правовых, познавательных и специализированных социальных сообществ и сервисов для детских объединений и творческих мероприятий для детей и молодежи.

При реализации требований безопасности в сети Интернет для любого пользователя, будь то школьник или учитель, образовательное учреждение должно обеспечивать защиту конфиденциальных сведений, представляющих собой в том числе персональные данные школьника, и предотвращать доступ к противоправной негативной информации. 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 с участием родителей. Для этого следует проводить непрерывную образовательно-просветительскую работу с детьми, формировать у обучающихся ответственное и критическое отношение к источникам информации, правовую культуру в сфере защиты от негативной информации и противоправных действий средствами коммуникаций, 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 — важная задача для вовлечения детей в современную цифровую образовательную среду, отвлечения их от бесполезного контента и игромании, бесцельной траты времени в социальных сетях и сервисах мобильной связи.

Главная цель курса — обеспечить социальные аспекты информационной безопасности в воспитании культуры информационной безопасности у школьников в условиях цифрового мира, включение на регулярной

основе цифровой гигиены в контекст воспитания и обучения детей, формирование у выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов воспитания и обучения детей:

- формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта 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, 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.

Место учебного курса «Информационная безопасность»

в учебном плане

Особенностью программы курса является ее поэтапное развитие для разных возрастных групп обучающихся основного общего образования с учетом их возрастных особенностей. Программа курса ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им. Программа курса представлена двумя разделами по возрастным группам: для 5—6 классов и 7—9 классов.

Реализация программы учебного курса возможна в разных формах:

- как дополнительные модули обучения в интеграции с предметами «Информатика» и (или) «ОБЖ» для двух возрастных групп: 5—6 и 7—9 классов (от 30 учебных часов для каждой возрастной группы);
- в рамках отдельного учебного курса «Информационная безопасность» для внеурочной деятельности по выбору из объема часов, формируемых самостоятельно образовательной организацией;
- в рамках часов, предусмотренных по программе воспитания (социализации) в образовательной организации для разных уровней общего образования.

Программа учебного курса поддерживается электронными ресурсами на основе документальных фильмов, анимационных ресурсов и электронных практикумов в открытом доступе от ИТ-компаний Российской Федерации в рамках их участия в проектах по информационной безопасности для детей. 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.

Общая характеристика учебного курса «Информационная безопасность»

Начинать обучение по курсу информационной безопасности крайне актуально по острым проблемным ситуациям в условиях присутствия в жизни детей персональных устройств работы в сети Интернет и мобильных сетях связи, а также для содействия при использовании детьми Интернета для обучения, творческого и развивающего досуга, познавательной деятельности. Программа направлена на решение вопросов массового формирования культуры информационной безопасности школьников, которые живут в современном информационном обществе, стремительно расширяющем общедоступные коммуникации в Интернете.

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.

Раздел программы курса для 5—6 классов отражает практические вопросы и жизненные проблемы:

- негативный и позитивный Интернет, цифровизация профессий;
- 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.

Раздел программы курса для 7—9 классов отражает особенности современного цифрового мира как киберпространства, насыщенного сетевыми сервисами и интернет-коммуникациями, доступными детям, новыми сервисами и устройствами с искусственным интеллектом (умные вещи, Интернет вещей), в том числе несущими в себе угрозы:

- 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 электронных сервисов, социальных/банковских карт, имеющих персональные настройки доступа к ним.

Отражение потребностей цифрового мира в современной цифровой грамотности и новых профессиональных качествах современного человека востребовано в жизни и учебе школьников и несет в себе актуальные запросы для выпускника основного общего образования в его дальнейшей жизни и профессиональном выборе с обязательным использованием требований информационной безопасности:

- профориентация в мире профессий будущего, знакомство с профессиями в сфере информационной безопасности;
- популяризация электронных средств и ресурсов обучения;
- развитие кругозора о полезных интернет-ресурсах;
- получение представлений о цифровых технологиях для улучшения качества жизни;
- навыки обдуманного поведения при поиске информации в сети Интернет, критический анализ полученной информации, умение работать с информацией избирательно и ответственно.

СОДЕРЖАНИЕ

УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Содержание учебного курса «Информационная безопасность» для разных возрастных модулей программы складывается из двух линий:

- 1) Информационное общество и информационная культура.
- 2) Информационное пространство и правила информационной безопасности.

5 – 6 классы

Линия «Информационное общество и информационная культура»

Модуль 1. Информационное общество.

1.1. Информационное общество.

История создания сети Интернет.

Что такое Всемирная паутина?

1.2. Интернет как глобальная компьютерная сеть.

Как стать пользователем Интернета. Опасности для пользователей Интернета.

Сайты, электронные сервисы.

1.3. Угрозы в сети Интернет.

Защита личных данных в сети Интернет.

1.4. Сетевой этикет.

Коллекции сайтов для детей. Электронные музеи.

Линия «Информационное пространство и правила информационной безопасности»

Модуль 2. Правила пользователей сети Интернет.

2.1. Работа с СМС, электронной почтой, видео сервисами, в чатах и социальных сетях. Что такое информационная безопасность.

2.2. Защита от вредоносных программ и нежелательных рассылок, от негативных сообщений, защита своих устройств от внешнего вторжения.

2.3. Общение в социальной сети, работа с поисковыми системами и анализ информации, ответственность за распространение ложной и негативной информации, защита от нежелательных сообщений и контактов, вызов экстренной помощи.

2.4. Использование полезных ресурсов в сети Интернет, работа в сети Интернет для людей с особыми потребностями.

7—9 классы

Линия «Информационное общество и информационная культура»

Модуль 1. Современное информационное пространство и искусственный интеллект. 1.1. Киберпространство. Кибермиры. Киберфизическая система.

1.2. Киберобщество. Киберденьги. Кибермошенничество.

Модуль 2. Современная информационная культура.

2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.

2.2. Социальная инженерия. Классификация угроз социальной инженерии.

2.3. Новые профессии в киберобществе. Цифровизация профессий.

Линия «Информационное пространство и правила информационной безопасности»

Модуль 3. Угрозы информационной безопасности.

3.1. Киберугрозы. Кибервойны. Киберпреступность.

Уязвимости кибербезопасность.

Запрещенные и нежелательные сайты.

3.2. Защита от вредоносных программ и информационных атак.

3.3. Практика электронного обучения в сфере информационной безопасности.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРОГРАММЕ

Программа учебного курса «Информационная безопасность» отражает в содержании цели поддержки и сопровождения безопасной работы с информацией в учебно-познавательной, творческой и досуговой деятельности (планируемые личностные, метапредметные и предметные результаты освоения курса).

В соответствии с федеральным государственным образовательным стандартом основного общего образования необходимо сформировать у обучающихся с учетом возрастных особенностей на каждом уровне общего образования такие *личностные результаты*, которые позволят им грамотно ориентироваться в информационном мире с учетом имеющихся в нем угроз:

— принимать ценности человеческой жизни, семьи, гражданского общества, многонационального российского народа, человечества;

— быть социально активными, уважающими закон и правопорядок, соизмеряющими свои поступки с нравственными ценностями, осознающими свои обязанности перед семьей, обществом, Отечеством;

— уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания, сотрудничать для достижения общих результатов;

— осознанно выполнять правила здорового образа жизни, безопасного для человека и окружающей его среды.

В рамках достижения этих личностных результатов при реализации программы курса информационной безопасности наиболее актуально в условиях быстро меняющегося и несущего в себе угрозы информационного мира обеспечить:

— развитие морального сознания и компетентности в решении моральных проблем на основе личностного выбора, формирование нравственных чувств и нравственного поведения, осознанного и ответственного отношения к собственным поступкам;

— формирование ценности здорового и безопасного образа жизни; усвоение правил индивидуального и коллективного безопасного поведения в чрезвычайных ситуациях, угрожающих жизни и здоровью людей.

В результате освоения программы курса информационной безопасности акцентируется внимание на *метапредметных результатах* освоения основной образовательной программы:

— 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 информационно-коммуникационных технологий (ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Планируется достижение *предметных результатов*, актуальных для курса информационной безопасности в интеграции с предметами «Информатика» и(или) «ОБЖ» для 5—6 и 7—9 классов.

Линия «Информационное общество и информационная культура»:

— понимание личной и общественной значимости современной культуры безопасности жизнедеятельности;

— знание основных опасных и чрезвычайных ситуаций социального характера, включая экстремизм и терроризм, и их последствий для личности, общества и государства; формирование антиэкстремистской и антитеррористической личностной позиции;

— знание и умение применять меры безопасности и правила поведения в условиях опасных и чрезвычайных ситуаций.

Линия «Информационное пространство и правила информационной безопасности»:

— формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики;

— умение принимать обоснованные решения в конкретной опасной ситуации с учетом реально складывающейся обстановки и индивидуальных возможностей.

В результате освоения программы курса с учетом возрастных групп выпускник освоит жизненно важные практические компетенции.

Выпускник научится понимать:

— источники информационных угроз, вредоносные программы и нежелательные рассылки, поступающие на мобильный телефон, планшет, компьютер;

— роль близких людей, семьи, правоохранительных органов для устранения проблем и угроз в сети Интернет и мобильной телефонной связи, телефоны экстренных служб;

— виды информационных угроз, правила поведения для защиты от угроз, виды правовой ответственности за проступки и преступления в сфере информационной безопасности;

— проблемные ситуации и опасности в сетевом взаимодействии и правила поведения в проблемных ситуациях, ситуациях профилактики и предотвращения опасности;

— этикет сетевого взаимодействия, правовые нормы в сфере информационной безопасности;

— правила защиты персональных данных;

— назначение различных позитивных ресурсов в сети Интернет для образования и в профессиях будущего.

Выпускник научится применять на практике:

— правила цифровой гигиены для использования средств защиты персональных данных (формировать и использовать пароль, использовать код защиты персонального устройства, регистрироваться на сайтах без распространения личных данных);

— компетенции медиа информационной грамотности при работе с информацией в сети Интернет, критическое и избирательное отношение к источникам информации;

— компетенции компьютерной грамотности по защите персональных устройств от вредоносных программ, использованию антивирусных программных средств, лицензионного программного обеспечения;

— информационно-коммуникативные компетенции по соблюдению этических и правовых норм взаимодействия в социальной сети или в мессенджере, умение правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.), отключаться от нежелательных контактов, действовать согласно правовым нормам в сфере информационной безопасности (защиты информации).

Выпускник освоит нормы культуры информационной безопасности в системе универсальных учебных действий для самостоятельного использования в учебно-познавательной и досуговой деятельности позитивного Интернета и средств электронного обучения с соблюдением правил информационной безопасности.

Для выявления достижения планируемых результатов обучения рекомендуется использовать диагностические тесты и опросы, проектные работы и конкурсы по информационной безопасности в образовательных организациях.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

5—6 классы

Программа учебного курса для 5—6 классов основного общего образования рассчитана на объем не менее 30 часов. Программа курса может быть реализована по выбору образовательной организации как самостоятельный учебный курс во внеурочной деятельности детей за один год обучения или отдельными модулями в программах освоения учебных предметов «Информатика» и (или) «ОБЖ» (в 5—6 классах), а также в рамках школьных мероприятий с участием родителей интегрирована модулями в календарное планирование программы воспитания.

Варианты учебного планирования:

Вариант 1. Планирование обучения за один год обучения. Один урок в неделю. 30 уроков.

Вариант 2. Планирование обучения по модулям в 5—6 классах.

Модуль 1, всего 15 уроков.

Модуль 2, всего 15 уроков.

Модуль/тема	Всего часов	Теоретические занятия	Практическая работа с ресурсами и программами на компьютере
<i>Линия «Информационное общество и информационная культура»</i>	15	7	8
Модуль 1. Информационное общество	15	7	8
1.1. Информационное общество	3	2	1
1.2. Интернет как глобальная компьютерная сеть. Сайты, электронные сервисы. Коллекции сайтов для учебной и познавательной деятельности	4	1	3
1.3. Угрозы в сети Интернет. Защита личных данных в сети Интернет	6	3	3
1.4. Сетевой этикет. Коллекции сайтов для детей. Электронные музеи	2	1	1
<i>Линия «Информационное пространство и правила информационной безопасности»</i>	15	7	8
Модуль 2. Правила пользователей сети Интернет	15	7	8
2.1.Работа с СМС, электронной почтой, видеосервисами, в чатах и социальных сетях	3	2	1
2.2. Защита от вредоносных программ и нежелательных рассылок, от негативных сообщений,	3	1	2

защита своих устройств от внешнего вторжения			
2.3.Общение в социальной сети, работа с поисковыми системами и анализ информации, ответственность за распространение ложной и негативной информации, защита от нежелательных сообщений и контактов, вызов экстренной помощи	6	3	3
2.4.Использование полезных ресурсов в сети Интернет, работа в сети Интернет для людей с особыми потребностями	3	1	2
Всего:	30	14	16

7—9 классы

Программа учебного курса для 7—9 классов основного общего образования рассчитана на объем не менее 30 часов. Программа курса может быть реализована по выбору образовательной организации как самостоятельный учебный курс во внеурочной деятельности детей за один год обучения или отдельными модулями в программах освоения учебных предметов «Информатика» и (или) «ОБЖ» (в 7—9 классах), а также в рамках школьных мероприятий с участием родителей интегрирована модулями в календарное планирование программы воспитания.

Варианты учебного планирования:

Вариант 1. Планирование обучения за один год обучения. Один урок в неделю. 30 уроков.

Вариант 2. Планирование обучения по модулям в 7—9 классах.

Модуль 1, всего 10 уроков.

Модуль 2, всего 10уроков.

Модуль 3, всего 10 уроков.

Модуль/тема	Всего часов	Теоретические занятия	Практическая работа с ресурсами и программами на компьютере
<i>Линия «Информационное общество и информационная культура»</i>	20	9	11
Модуль 1. Современное информационное пространство и искусственный интеллект	10	5	5
1.1. Киберпространство. Кибермиры. Киберфизическая система	5	2	3
1.2.Киберобщество. Киберденьги. Кибермошенничество	5	3	2
Модуль 2. Современная информационная культура	10	4	6
2.1.Киберкультура.От книги к гипертексту. Киберкнига. Киберискусство.	4	2	2
2.2.Социальная инженерия. Классификация угроз социальной инженерии	4	2	2
2.3.Новые профессии в киберобществе. Цифровизация профессий	2		2
<i>Линия «Информационное пространство и правила информационной безопасности»</i>	10	4	6
Модуль 3. Угрозы информационной безопасности	10	4	6

3.1.Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты	4	2	2
3.2.Защита от вредоносных программ и информационных атак	3	1	2
3.3. Практика электронного обучения в сфере информационной безопасности	3	1	2
Всего:	30	13	17

Поурочное планирование

5-6 классы

№ урока / Дата	Тема урока/ параграф учебного пособия	Практическая работа к уроку	Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php
1	Введение. Что такое «информационное общество»?	Задание В1.Задание В2.	В.2. Ознакомьтесь с видеоматериалом. Обсудите в группе, какую опасность здоровью может нанести неразумное увлечение общением в сети Интернет — лайкомания. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Лайкомания»:
Модуль 1. Пространство Интернета на планете Земля 14 часов			
3	1.1.История создания сети Интернет	Тест 1. Задание 1.2 Задание 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?»

4	1.2.Что такое всемирная паутина?	Задание 1.4. Задание 1.5 Тест 2.	<i>На сайте Телеканала Карусель https://www.karusel-tv.ru/ посмотри разделы сайта, используя слова-меню</i> <i>Ознакомься с видеоуроком Телеканала Карусель: «Почемучка. Что такое веб-браузер»? Ответ на вопрос: каким веб-браузером ты пользуешься?</i>
5	1.3.Путешествие по сети Интернет: сайты и электронные сервисы	Задание 1.6 Задание 1.7 Задание 1.8 Задание 1.9 Тест 3	1.6.Выполните поиск сайта телеканала «Карусель» с помощью поисковой системыЯндекс. <i>Выбери нужную ссылку, и перейди на этот сайт.</i> 1.7.Ознакомься с видеоуроком Телеканала Карусель:Почемучка. Поисковая система. <i>Ответ на вопрос: «что такое поисковые системы и для чего они предназначены»?</i> 1.8.Познакомься с сайтомКультура.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.
6	1.4. Как стать пользователем сети Интернет?	Задание 1.10 Тест 4	1.10. Ознакомьтесь с видеоуроком Телеканала Карусель: «Почемучка. Способы выхода в Интернет» Ответ на вопрос: какие различные способы выхода в Интернет ты можешь применять?
7	1.5 Какие опасности подстерегают пользователей сети Интернет?	Задание 1.11. Задание 1.12. Тест 5	На сайте Большой Российской Энциклопедии https://bigenc.ru/ перейди в раздел «Россия» и ознакомься с разделами энциклопедии Ознакомься с видеоуроком Телеканала Карусель: «Почемучка. Информация» Ответ на вопрос: Что такое информация?

8	1.6 Что такое кибератака?	Задание 1.13. Задание 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/
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 Каковы законы защиты личных данных в сети Интернет?	Задание 1.16 Задание 1.17 Задание 1.18 Тест 8	Сайт «Лига безопасного Интернета» <i>Ознакомься с видеоуроком «Защита персональных данных детей»</i> <i>Сайт «Персональные данные. Дети» Пройди тест «Что ты знаешь о персональных данных»</i> 1.18 Ознакомьтесь с видеоматериалами. Обсудите в группе, что такое «конфиденциальность» и зачем её 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-robot-a-kaspera-privatnost-akkauntov-2/
----	---	--	---

11	1.9 Что такое сетевой этикет?	Задание 1.19. Задание 1.20 Тест 9	1.19. Ознакомьтесь с видеоуроком из архива канала Бибигон: «Правила поведения в коллективе / Сетевой этикет» <i>Ответ на вопрос: какие правила поведения в коллективе нужно использовать в сообщениях на мобильном телефоне или по электронной почте?</i> 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/mult filmy/priklyucheniya robota-kaspera-overshering-vred-reputatsii
12	1.10. Коллекции сайтов для детей	Задание 1.21	Задание 1.21 Ознакомьтесь с видеоматериалами. Обсудите в группе, что такое «пози- тивный 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 «Гоголь: Играй, Гуляй, Общайся, Учись». 1.23

			Проведите путешествие по ресурсам сайта «Веб-Ландия». Обсудите в группе, какие из них помогут вам в развитии творчества.
13	1.10. Электронные музеи	Задание 1.24 Задание 1.25 Задание 1.26 Задание 1.27 Задание 1.28	Русский музей в Санкт-Петербурге Виртуальный филиал: http://www.virtualrm.spb.ru/ru/resources/galleries Ознакомьтесь с виртуальными экскурсиями. 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 Музей изобразительных искусств имени А. С. Пушкина в Москве Электронная коллекция: http://www.arts-museum.ru/collections/index.php Выберите тематику и посетите электронную экспозицию Музея изобразительных искусств имени А. С. Пушкина. Эрмитаж Виртуальное путешествие: https://www.hermitagemuseum.org/wps/portal/hermitage/panorama?lng=ru Выберите виртуальное путешествие по Эрмитажу. 1.28. Политехнический музей в Москве Раздел на сайте «Панорамные туры»: https://polymus.ru/ru/museum/fonds/panoramic/ Выберите тур на сайте Политехнического музея и ознакомьтесь с его экспозицией на своём компьютере.

14-15	Контрольный урок	Контрольные задания к части 1	Скачайте на свой компьютер файл пособием, представленным «Лабораторией Касперского» в открытом доступе. Распечатайте пособие и выполните в нём задания. Сайт «Лига безопасного интернета» Практикум «Азбука информационной безопасности» (Лаборатория Касперского): http://ligainternet.ru/upload/docs/docs-for-dowloud/Azbuka_informatsionnoy_bezopasnosti.pdf
Модуль 2. Правила пользователей сети Интернет 15 часов			
16	2.1. Правила работы с СМС и мессенджерами сообщений	Задание 2.1. Тест 10	Задание 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-robot-kaspera-drug-vovka/ • Мультфильм «Приключения робота Каспера — Приватность аккаунтов»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robot-kaspera-privatnost-akkauntov/
17	2.2. Правила работы с электронной почтой	Задание 2.2. Задание 2.3 Тест 11	2.2 Ознакомьтесь с видеоматериалами. Составьте свою памятку 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 рассылки на ваш адрес. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Сообщения со взломанных аккаунтов»: https://kids.kaspersky.ru/entertainment/mult filmy/priklyucheniyarobota-kaspera-soobshheniya-so-vzlomannyh-akkauntov/
18	2.3. Правила работы с видеосервисами	Задание 2.4 Задание 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/mult filmy/priklyucheniyarobota-kaspera-pokupki-v-igrah/
19	2.4. Правила работы в социальных сетях	Задание 2.6. Задание 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/fiksi- sovetyostorozhnej-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 иметоды 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	Задание 2.9. Задание 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 — Мошенничеств в интернете»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robot-kaspera-moshennichestvo-v-internete/ 2.10 Ознакомьтесь с видеоматериалами.Обсудите в группе, какая опасность может скрываться на сайтах, какиетраты денег могут незаметно, но на-стойчиво предлагаться. Сайт «Защита детей. Лаборатория Касперского». • Мультфильм «Приключения робота Каспера — Опасности на надёжных 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	Задание 2.11. Задание 2.12. Задание 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-profil/2.12 Вместе с учителем или родителями внимательно прочитайте текст в социальной сети на страницах системы 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 анализа информации	Задание 2.14 Задание 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/multifilm/priklyucheniya-robot-kasperi-piratskie-sajty/Задание 2.15 Ознакомьтесь с видеоматериалами. Обсудите в группе, что такое ложная информация и как её распознать. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Ложная информация»: https://kids.kaspersky.ru/entertainment/multifilm/priklyucheniya-robot-kasperi-lozhnaya-informatsiya/
24	2.9. Правила ответственности за распространения ложной и негативной информации	Задание 2.16. Задание 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/ • 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 своих 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-robotakaspara-paroli/
27	2.13. Правила использования полезных ресурсов в сети Интернет	Задание 2.21 Задание 2.22 Задание 2.23	2.21. Российская государственная детская библиотека: https://rgdb.ru/ Раздел «Национальная электронная детская библиотека»:

			http://arch.rgdb.ru/xmlui/2.22 Аудиохрестоматия: http://audiohrestomatiya.ru/ «Аудиохрестоматия» — это медиапортал, на котором собраны произведения мировой литературы в исполнении известных артистов. 2.23 Детская электронная библиотека: http://www.deti-book.info/
28	2.14. Средства работы в сети Интернет для людей с особыми потребностями	Задания 2.24 Задание 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 познанию спе- циально создан социально- информационный проект Nvda.ru. Бесплатная программа экранного доступа Nvda: https://nvda.ru/ Ознакомьтесь с разделом Web- радио на сайте проекта Nvda.

29-30	Контрольный урок	Контрольные задания 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?»
31-34	Обобщение знаний полученных за год		

7 – 8 классы

№ урока	Тема урока/ параграф учебного пособия	Кол-во часов/Дата	Видеоматериалы и интернет ресурсы
1	Введение.	1	https://urokцифры.рф/lessons/cybersecurity https://fcprc.ru/wpcontent/uploads/2021/12/MR-po- bezopasnomu-ispolzovaniyu-seti-Internet-.pdf http://персональныеданные.дети/multimedia/videorolik_o_zawite_det_skih_personalnyh_dannyh1/ http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachersdetail.php?ID=3652 https://stepic.org/course/Безопасность-в-интернете-191
Модуль 1. Киберпространство 9 часов			
2	Киберпространство	1	https://urokцифры.рф/lessons/cybersecurity https://fcprc.ru/wpcontent/uploads/2021/12/MR-po- bezopasnomu-ispolzovaniyu-seti-Internet-.pdf http://персональныеданные.дети/multimedia/videorolik_o_zawite_det_skih_personalnyh_dannyh1/ http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachersdetail.php?ID=3652 https://stepic.org/course/Безопасность-в-интернете-191

3-4	Кибермиры	2	
5	Киберфизическая система	1	
6	Киберобщество	1	
7	Киберденьги	1	
8	Кибермошейничество	1	
9-10	Практическая работа по разделу 1	2	
Модуль 2. Киберкультура 10 часов			
11	Киберкультура	1	https://урокицифры.рф/lessons/cybersecurity https://fcprc.ru/wpcontent/uploads/2021/12/MR-po-bezopasnomu-ispolzovaniyu-seti-Internet-.pdf http://персональныеданные.дети/multimedia/videorolik_o_zawite_det_skih_personalnyh_dannyh1/ http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachersdetail.php?ID=3652 https://stepic.org/course/Безопасность-в-интернете-191
12	От книги к гипертексту	1	
13	Кибекнига	1	

14-15	Киберискусство	2	
16	Социальная инженерия	1	
17	Классификация угроз социальной инженерии	1	
18-20	Практическая работа по разделу 2	3	
Раздел III Киберугрозы 10 часов			
21	Кибервойны	1	https://урокицифры.pdf/lessons/cybersecurity https://fcprc.ru/wpcontent/uploads/2021/12/MR-po-bezopasnomu-ispolzovaniyu-seti-Internet-.pdf http://персональныеданные.дети/multimedia/videorolik_o_zawite_det_skih_personalnyh_dannyh1/ http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachersdetail.php?ID=3652 https://stepic.org/course/Безопасность-в-интернете-191
22	Киберпреступность	1	
23	Примеры киберпреступлений	1	
24	Уязвимости кибербезопасности	1	
25	Угрозы информационной безопасности	1	

26	Запрещённые и нежелательные сайты	1	
27	Новые профессии в киберобществе	1	
28- 30	Практическая работа по разделу 3	3	
31-34	Обобщение изученного	2	

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ МАТЕРИАЛЫ ДЛЯ УЧЕНИКА

Учебник для 5-6 классов Информационная безопасность. Авторы: Цветкова М.С., Якушина Е.В, Хлобыстова И. Ю и др.
Учебник для 7-9 классов Информационная безопасность. Авторы: Цветкова М.С., Якушина Е.В, Хлобыстова И. Ю и др.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УЧИТЕЛЯ

Цветкова, М. С. Информационная безопасность. 2–11 классы: методическое пособие для учителя

ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ И РЕСУРСЫ СЕТИ ИНТЕРНЕТ

<https://урокицифры.рф/lessons/cybersecurity>

<https://fcprc.ru/wpcontent/uploads/2021/12/MR-po-bezopasnomu-ispolzovaniyu-seti-Internet-.pdf>

http://персональныеданные.дети/multimedia/videorolik_o_zawite_det_skih_personalnyh_dannyh1/

<http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachersdetail.php?ID=3652>

<https://stepic.org/course/Безопасность-в-интернете-191>