

Муниципальное автономное общеобразовательное учреждение  
«Средняя общеобразовательная школа № 22» г. Сыктывкара  
(МАОУ «СОШ №22» г. Сыктывкара)  
«22 №-а шӧр школа»  
Сыктывкарса муниципальной асьюралана велӧдан учреждение  
(«22 №-а ШШ МАВУ»)

ПРИНЯТО  
Педагогическим советом  
Протокол № 23  
от «07» августа 2023 г.

Утверждаю  
Директор \_\_\_\_\_ В.А. Елагина  
Приказ от 31.08.2021г. № 499-ОД

## РАБОЧАЯ ПРОГРАММА УЧЕБНОГО ПРЕДМЕТА

«ЦИФРОВАЯ ГРАМОТНОСТЬ»

ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

(Срок реализации 5 лет)

(Разработана в соответствии с Федеральным государственным  
образовательным стандартом основного общего образования)

Составитель:  
Педагог-библиотекарь Бондаренко М.А.

## **ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

Данная рабочая программа составлена на основе Федерального государственного образовательного стандарта основного общего образования, утвержденного приказом Министерства образования и науки РФ от 17 декабря 2010 № 1897 (в ред. Приказа Минобрнауки России от 31.12.2015 № 1577), с изменениями и дополнениями, в соответствии с Основной образовательной программой основного общего образования МАОУ «СОШ №22» г.Сыктывкара, Рабочей программой воспитания МАОУ «СОШ №22» г.Сыктывкара (модуль «Школьный урок»), с Положением о рабочей программе учебного предмета, курса, дисциплины (модуля), с учебным планом МАОУ «СОШ №22» г.Сыктывкара. Для реализации рабочей программы учебного предмета выбран учебно-методический комплект «Информационная безопасность» Цветковой М.С. для 5-9 классов издательства ООО «Бином. Лаборатория знаний». УМК включает программу, учебники, учебные пособия, электронные пособия, методические пособия. Данная линия учебников соответствует Федеральному государственному образовательному стандарту основного общего образования и включена в Федеральный перечень учебников .

*В программе учтены приоритеты научно-технологического развития Российской Федерации (Пр-294, п. 2а-16).*

### **ОБЩАЯ ХАРАКТЕРИСТИКА УЧЕБНОГО ПРЕДМЕТА**

Начинать обучение по предмету цифровая грамотность 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 цифровой грамотности 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 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 для 7 класса 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.

Раздел программы для 8-9 классов включает изучение правовой грамоты в сфере информационной безопасности, в том числе основных видов юридической ответственности (уголовной, административной и гражданско-правовой) за преступления и проступки в области информационной безопасности (защиты информации). Полученные знания помогут избегать ошибок и правонарушений в информационном мире, а также ответственно работать в информационном пространстве, соблюдая нормы права. Важную часть программы 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. В программе для старшеклассников предусмотрена практика применения культуры информационной безопасности в

электронном обучении, которое уже повсеместно встроено в профессиональную подготовку и дальнейшую активность в труде.

Отражение потребностей цифрового мира в современной цифровой грамотности и новых профессиональных качествах современного человека востребовано в жизни и учебе 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 соблюдения правовых норм защиты информации;

- навыки обдуманного поведения при поиске информации в сети Интернет, критический анализ полученной информации, умение работать с информацией избирательно и ответственно.

**Форма организации образовательного процесса: классно-урочная, дистанционная.**

*На уроках в соответствии с Программой формирования/развития УУД и РПВ используются следующие формы совместной деятельности учащихся:*

интеллектуальные игры, стимулирующие познавательную мотивацию учащихся;

дискуссии, дающие учащимся возможность приобрести опыт ведения конструктивного диалога;

групповая работа или работа в парах, обучающая командной работе и взаимодействию с другими учащимися;

игровая деятельность, помогающая поддержать мотивацию детей к получению знаний, налаживанию позитивных межличностных отношений в классе, установлению доброжелательной атмосферы во время урока.

**Технологии, используемые в обучении:**

- развивающего обучения,

- обучения в сотрудничестве,

- проблемного обучения,

- развития исследовательских навыков, \_\_\_

информационно-коммуникационные,

- здоровьесбережения и т. д.

Описание приёмов представлено на <https://drive.google.com/drive/folders/1S4oF-h3mvUuTQfRyvr3IT76VAVWdeP2n?usp=sharing>.

Ресурс для игрофикации <https://www.classcraft.com/ru/>

Международный проект «Школа реальных дел» <https://sites.google.com/>

Тексты для чтения <https://kot.sh/category/geroi> (рубрика- Герои)

Кейсы для организации проектной и исследовательской деятельности:

- ФГБНУ «Институт стратегии развития образования Российской академии образования» ЕДИНОЕ СОДЕРЖАНИЕ ОБЩЕГО ОБРАЗОВАНИЯ <https://edsoo.ru/pages/researches.html> <http://skiv.instrao.ru/content/board1/rabochie-materialy/>
- Портал Функциональная грамотность. Учимся для жизни [https://uchitel.club/pedsovet\\_2020/pisaregion/](https://uchitel.club/pedsovet_2020/pisaregion/)
- Открытый банк заданий ФГБНУ «Федеральный институт педагогических измерений» <https://fipi.ru/otkrytyy-bank-zadaniy-dlya-otsenki-yestestvennonauchnoy-gramotnosti>

## **ЦЕЛЬ ИЗУЧЕНИЯ УЧЕБНОГО ПРЕДМЕТА**

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 предмета цифровая грамотность 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 предмета — обеспечить социальные аспекты цифровой грамотности 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 ПРЕДМЕТА В УЧЕБНОМ ПЛАНЕ**

Особенностью данной программы является включение в контекст не только обучения, но и воспитания в условиях быстро нарастающих новых видов информационных угроз и развития средств противодействия им, отраженных в законодательстве Российской Федерации, а также поэтапное ее развитие для разных возрастных групп обучающихся основного общего образования с учетом их возрастных особенностей. Программа представлена тремя разделами по возрастным группам: для 5—6 классов, 7 класса и 8—9 классов.

Учебный план предусматривает обязательное изучение цифровой грамотности на этапе основного общего образования в объеме 175 часов. Изучение учебного предмета цифровая грамотность рассчитано на пять лет обучения, один час в неделю.

Класс	Количество часов	Практическая часть	Виды контроля
			Промежуточная аттестация
5	35	10	1
6	35	10	1
7	35	10	1
8	36	10	1
9	34	10	1
Итого	175	50	5

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.

### ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРОГРАММЕ

Программа учебного предмета «Цифровая грамотность» 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 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 личного 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 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;

— готовность и способность к самостоятельной информационно-познавательной деятельности, включая умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников.

Планируется достижение *предметных результатов*:

— 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.

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

— формирование основ правосознания для соотнесения собственного поведения и поступков других людей с нравственными ценностями и нормами поведения, установленными законодательством Российской Федерации;

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

— освоение приемов работы с социально значимой информацией, ее осмысление; развитие способностей обучающихся делать необходимые выводы и давать обоснованные оценки социальным событиям и процессам;

— принятие этических аспектов информационных технологий; осознание ответственности людей, вовлеченных в создание и использование информационных систем, распространение информации;

— понимание основ правовых аспектов использования компьютерных программ и работы в Интернете;

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

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

***Учащийся научится выполнять:***

— определять источники информационных угроз, вредоносных программ и нежелательных рассылок, поступающие на мобильный телефон, планшет, компьютер;

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

— распознавать виды информационных угроз, применять правила поведения для защиты от угроз, ориентироваться в видах правовой ответственности за проступки и

преступления в сфере информационной безопасности;

— ориентироваться в проблемных ситуациях и опасностях в сетевом взаимодействии и правилах поведения в проблемных ситуациях, ситуациях профилактики и предотвращения опасности;

— владеть этикетом сетевого взаимодействия, правовыми нормами в сфере информационной безопасности;

— владеть правилами защиты персональных данных;

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

***По завершении учебного года учащиеся получит возможность научиться:***

— использовать 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);

— владеть компетенцией медиаинформационной грамотности при работе с информацией в сети Интернет, применять критическое и избирательное отношение к источникам информации;

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

— пользоваться 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.*

## **СОДЕРЖАНИЕ УЧЕБНОГО ПРЕДМЕТА**

### **5 класс**

Часть 1. Правила работы с мобильным телефоном.

Введение. Привет, я Смайлик. СМС от неизвестных лиц. Ложные сообщения. Угрозы в СМС. Звонки с предложениями. Защита от входа в твой телефон. Подключение телефона к «Вай-Фай» сети. Вызов экстренных служб. Телефонное хулиганство.

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

Мой планшет или компьютер: защита входа. Регистрация на сайтах. Личные данные. Моя почта, логин и пароль. Спам. Почта от неизвестных лиц. Вирусы. Microsoft Word. Microsoft Office Excel. Microsoft Power Point.

Часть 3. Путешествуем в сети Интернет.

Поиск информации в Интернете. Сайты для детей. Сайты о безопасном поведении. Сайты для учебы. Сайты с электронными книгами. Сайты с коллекциями для детей

Часть 4. Правила безопасной работы в социальной сети.

Социальные сети для детей. Что такое Аватар и как его выбрать. «Друг» в сети, кто за ним прячется. Ложные сообщения. Что говорить о себе незнакомцам. Спроси совета в семье. Этикет в общении. Нельзя обижать. Если тебя обижают. Защити себя от недоброжелателей. Если тебе угрожают. Уговоры и предложения. Отключение от нежелательных контактов.

## **6 класс**

Часть 1. Пространство Интернета на планете Земля.

Введение. Что такое «информационное общество»? История создания сети Интернет. Что такое всемирная паутина? Путешествие по сети Интернет: сайты и электронные сервисы. Как стать пользователем сети Интернет? Какие опасности подстерегают пользователей сети Интернет? Что такое кибератака? Что такое «информационная безопасность»? Каковы законы защиты личных данных в сети Интернет? Что такое сетевой этикет? Коллекции сайтов для детей. Электронные музеи

Часть 2. Правила для пользователей сети Интернет.

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

## **7 класс**

Часть 1. Современное информационное пространство и искусственный интеллект. Киберпространство. Кибермиры. Киберфизическая система. Киберобщество. Киберденьги. Кибермошенничество.

Часть 2. Современная информационная культура. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии. Новые профессии в киберобществе. Цифровизация профессий.

Часть 3. Угрозы информационной безопасности. Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасность. Запрещенные и нежелательные сайты. Защита от вредоносных программ и информационных атак. Практика электронного обучения в сфере информационной безопасности.

## **8 класс**

Часть 1. Понятие юридической ответственности за правонарушение в области информационной безопасности.

Введение. Основные документы в области информационной безопасности Российской Федерации. Информация как объект правовых отношений. Функции, принципы и виды юридической ответственности. Субъективная и объективная стороны юридической ответственности.

Часть 2. Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации).

Общие положения законодательства Российской Федерации о гражданско-правовой ответственности. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности (защиты информации). Ответственность за проступок в области присвоение авторства (плагиат). Ответственность за проступок за оскорбления, в том числе в социальных сетях.

Часть 3. Административная ответственность за проступки в области информационной безопасности (защиты информации).

Административное правонарушение. Основные понятия административного правонарушения. Особенности административной ответственности несовершеннолетних. Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение. Ответственность за проступок – за оскорбления, в том числе в социальных сетях. Ответственность за проступок – ложный вызов экстренных служб.

Ответственность за проступок - пропаганду в Интернете наркотических и психотропных веществ. Ответственность за проступок –нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные). Ответственность за проступок – нарушение правил защиты информации. Ответственность за проступок – представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство. Ответственность за проступок – за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт. Ответственность за проступок –нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации.

### 9 класс

Часть 1. Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации).

Введение. Основные документы в области информационной безопасности Российской Федерации. Информация как объект правовых отношений. Функции, принципы и виды юридической ответственности. Уголовный кодекс Российской Федерации. Виды наказаний в области уголовной ответственности. Ответственность за преступления в области компьютерной информации и применения компьютеров. Ответственность за преступления в области присвоения авторства (плагиат). Ответственность за преступления в области нарушения авторских прав на лицензионное программное обеспечение. Ответственность за преступления в области мошенничества (обмана). Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений. Ответственность за преступления – за проведение скрытой (негласной) аудиозаписи. Ответственность за преступления – за заведомо ложное сообщение о теракте. Ответственность за преступления – за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг). Ответственность за преступления – за мошенничество в сфере компьютерной информации. Ответственность за преступления – за незаконное распространение порнографических материалов. Ответственность за преступления – за заведомо ложный донос.

Часть 2. Проектные задания.

Лицензионное соглашение свободного ПО Линукс. Как купить лицензию на платную антивирусную программу. Что такое СС лицензия. Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию. Как задавать безопасный пароль. Настройки телефона, планшета для защиты от несанкционированного

доступа. Защита персональных данных. Обзор. Личный контент в облаке и система его защиты.

## ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

### 5 класс

Наименование разделов	Кол-во
Правила работы с мобильным телефоном	5
Правила безопасной работы в сети Интернет с планшетом или на компьютере	17
Путешествуем в сети Интернет	6
Правила безопасной работы в социальной сети	8

### 6 класс

Наименование разделов	Кол-во
Пространство Интернета на планете Земля	18
Правила для пользователей сети Интернет	17

### 7 класс

Наименование разделов	Кол-во
Киберпространство	10
Киберкультура	12
Киберугрозы	13

### 8 класс

Наименование разделов	Кол-во
Понятие юридической ответственности за правонарушение в области информационной безопасности	7
Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации)	7
Административная ответственность за проступки в области информационной безопасности (защиты информации)	21

### 9 класс

Наименование разделов	Кол-во
-----------------------	--------

Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)	28
Проектные задания	7

## УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

### 5 класс

№ урока	Тема урока/ параграф учебного пособия	Общее количество часов	Содержание
Часть 1. Правила работы с мобильным телефоном.			
1	Введение. Привет, я Смайлик	1	Часть 1. Правила работы с мобильным телефоном.  Введение. Привет, я Смайлик. СМС от неизвестных лиц. Ложные сообщения. Угрозы в СМС. Звонки с предложениями. Защита от входа в твой телефон. Подключение телефона к «Вай-Фай» сети. Вызов экстренных служб. Телефонное хулиганство.
2	1.1 СМС от неизвестных лиц 1.2. Ложные сообщения 1.3. Угрозы в СМС	1	
3	1.4. Звонки с предложениями 1.5. Защита от входа в твой телефон 1.6. Подключение телефона к «Вай-Фай» сети	1	
4	1.7. Вызов экстренных служб 1.8. Телефонное хулиганство	1	
5	Контрольный урок	1	
Часть 2. Правила безопасной работы в сети Интернет с планшетом или на компьютере			
6	2.1 Мой планшет или компьютер: защита входа 2.2. Регистрация на сайтах.	1	Часть 2. Правила безопасной работы в сети Интернет с планшетом или на



	Личные данные		компьютере.
7	2.3. Моя почта, логин и пароль 2.4. Спам	2	Мой планшет или компьютер: защита входа. Регистрация на сайтах.
8	2.5. Почта от неизвестных лиц 2.6. Вирусы	1	Личные данные. Моя почта, логин и пароль. Спам. Почта от неизвестных лиц. Вирусы.
9-11	2.8. Microsoft Word	3	Microsoft Word. Microsoft
12-14	2.9. Microsoft Office Excel	3	Office Excel. Microsoft Power
15-18	2.10. Microsoft Power Point	4	Point
19	Контрольный урок	1	
<p>Часть 3.</p> <p>Путешествуем в сети Интернет</p>			
20	3.1. Поиск информации в Интернете 3.2. Сайты для детей	1	Часть 3. Путешествуем в сети Интернет.
21	3.3. Сайты о безопасном поведении	1	Поиск информации в Интернете.
22	3.4 Сайты для учебы	1	Сайты для детей. Сайты о безопасном поведении.
23	3.5 Сайты с электронными книгами	1	Сайты для учебы. Сайты с электронными книгами.
24	3.6 Сайты с коллекциями для детей	1	Сайты с коллекциями для детей
25	Контрольный урок	1	
<p>Часть 4.</p> <p>Правила безопасной работы в социальной сети</p>			
26	4.1. Социальные сети для детей 4.2. Что такое Аватар и как его выбрать 4.3. «Друг» в сети, кто за ним прячется	1	Часть 4. Правила безопасной работы в социальной сети.
27	4.4. Ложные сообщения 4.5. Что говорить о себе незнакомцам	1	Социальные сети для детей. Что такое Аватар и как его выбрать. «Друг» в сети, кто за ним прячется. Ложные сообщения. Что говорить о

28	4.6. Спроси совета в семье 4.7. Этикет в общении	1	себе незнакомцам. Спроси совета в семье. Этикет в общении. Нельзя обижать. Если тебя обижают. Защити себя от недоброжелателей. Если тебе угрожают. Уговоры и предложения. Отключение от нежелательных контактов
29	4.8. Нельзя обижать 4.9. Если тебя обижают	1	
30	4.10. Защити себя от недоброжелателей 4.11. Если тебе угрожают 4.12. Агрессия и грубость	1	
31	4.13. Уговоры и предложения 4.14. Отключение от нежелательных контактов	1	
32-33	Защита творческих проектов	2	
34	Промежуточная аттестация	1	
35	Контрольный урок	1	

**6 класс**

<b>№ урока</b>	<b>Тема урока/ параграф учебного пособия</b>	<b>Общее количество часов</b>	<b>Содержание</b>
Часть 1. Пространство Интернета на планете Земля			
1	Введение. Что такое «информационное общество»?	1	Часть 1. Пространство Интернета на планете Земля.  Введение. Что такое «информационное общество»? История создания сети Интернет. Что такое всемирная паутина?  Путешествие по сети Интернет: сайты и электронные сервисы. Как
2	1.1.История создания сети Интернет	1	
3	1.2.Что такое всемирная паутина?	1	
4-5	1.3.Путешествие по сети Интернет: сайты и электронные сервисы	2	
6	1.4.Как стать пользователем сети Интернет?	1	

7-8	1.5 Какие опасности подстерегают пользователей сети Интернет?	2	<p>стать пользователем сети Интернет? Какие опасности подстерегают пользователей сети Интернет? Что такое кибератака? Что такое «информационная безопасность»? Каковы законы защиты личных данных в сети Интернет? Что такое сетевой этикет? Коллекции сайтов для детей. Электронные музеи</p>
9	1.6 Что такое кибератака?	1	
10	1.7 Что такое «информационная безопасность»?	1	
11-12	1.8 Каковы законы защиты личных данных в сети Интернет?	2	
13-14	1.9 Что такое сетевой этикет?	2	
15-16	1.10. Коллекции сайтов для детей	2	
17	1.10. Электронные музеи	1	
18	Контрольный урок	1	
<p>Часть 2. Правила для пользователей сети Интернет</p>			
19	2.1.Правила работы с СМС и мессенджерами сообщений 2.2.Правила работы с электронной почтой	1	<p>Часть 2. Правила для пользователей сети Интернет.</p> <p>Правила работы с СМС и мессенджерами сообщений. Правила работы с электронной почтой. Правила работы с видеосервисами. Правила работы в социальных сетях. Правила защиты от вирусов, спама, рекламы и рассылок. Правила защиты от</p>
20	2.3.Правила работы с видеосервисами 2.4. Правила работы в социальных сетях	1	
21	2.5.Правила защиты от вирусов, спама, рекламы и рассылок	1	
22	2.6. Правила защиты от негативных сообщений	1	
23	2.7. Правила общения в	1	

	социальной сети		<p>негативных сообщений.</p> <p>Правила общения в социальной сети. Правила работы с поисковыми системами и анализа информации.</p> <p>Правила ответственности за распространения ложной и негативной информации.</p> <p>Правила защиты от нежелательных сообщений и контактов.</p> <p>Правила вызова экстренной помощи.</p> <p>Правила защиты своих устройств от внешнего вторжения.</p> <p>Правила использования полезных ресурсов в сети Интернет.</p> <p>Средства работы в сети Интернет для людей с особыми потребностями.</p>
24	2.8. Правила работы с поисковыми системами и анализа информации	1	
25-26	2.9.Правила ответственности за распространения ложной и негативной информации	2	
27	2.10.Правила защиты от нежелательных сообщений и контактов	1	
28	2.11. Правила вызова экстренной помощи	1	
29	2.12. Правила защиты своих устройств от внешнего вторжения	1	
30	2.13. Правила использования полезных ресурсов в сети Интернет	1	
31	2.14. Средства работы в сети Интернет для людей с особыми потребностями	1	
32-33	Защита творческих проектов	2	
34	Промежуточная аттестация	1	
35	Контрольный урок	1	
<b>7 класс</b>			
<b>№ урока</b>	<b>Тема урока/ параграф учебного пособия</b>	<b>Общее количество часов</b>	<b>Содержание</b>
1	Введение.	1	
Часть 1. Киберпространство			

2-3	1.1 Киберпространство	2	Часть 1. Современное информационное пространство и искусственный интеллект.  Киберпространство. Кибермиры. Киберфизическая система. Киберобщество. Киберденьги. Кибермошенничество.
4	1.2 Кибермиры	1	
5	1.3 Киберфизическая система	1	
6	1.4 Киберобщество	1	
7	1.5 Киберденьги	1	
8-9	1.6. Кибермошенничество	2	
10	Контрольный урок	1	
Часть 2. Киберкультура			
11-12	2.1. Введение. Киберкультура	2	Часть 2. Современная информационная культура.  Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии. Новые профессии в киберобществе. Цифровизация профессий.
13	2.2. От книги к гипертексту	1	
14-15	2.3. Киберкнига	2	
16-17	2.4. Киберискусство	2	
18-19	2.5. Социальная инженерия	2	
20-21	2.6. Угрозы социальной инженерии	2	
21	Контрольный урок	1	
Часть 3. Киберугрозы			
22	3.1 Введение. Кибервойны	1	Часть 3. Угрозы информационной безопасности.  Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасность.
23-24	3.2 Киберпреступность	2	
25	3.3 Примеры киберпреступлений	1	
26-27	3.4 Уязвимости кибербезопасности	2	
28-29	3.5. Угрозы информационной	2	

	безопасности		Запрещенные и нежелательные сайты. Защита от вредоносных программ и информационных атак. Практика электронного обучения в сфере информационной безопасности.
30	3.6 Запрещенные и нежелательные сайты	1	
31	3.7 Новые профессии в киберобществе	1	
32-33	Защита творческих проектов	2	
34	Промежуточная аттестация	1	
35	Контрольный урок	1	
<b>8 класс</b>			
<b>№ урока</b>	<b>Тема урока/ параграф учебного пособия</b>	<b>Общее количество часов</b>	<b>Содержание</b>
Часть 1. Понятие юридической ответственности за правонарушение в области информационной безопасности			
1-2	Введение. 1.1. Основные документы в области информационной безопасности Российской Федерации	2	Часть 1. Понятие юридической ответственности за правонарушение в области информационной безопасности.  Введение. Основные документы в области информационной безопасности Российской Федерации. Информация как объект правовых отношений. Функции, принципы и виды юридической ответственности. Субъективная и объективная
3	1.2 Информация как объект правовых отношений	1	
4-5	1.3 Функции, принципы и виды юридической ответственности.	2	
6	1.4 Субъективная и объективная стороны юридической ответственности	1	
7	Контрольный урок	1	

			стороны юридической ответственности.
Часть 2. Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации)			
8-9	2.1. Общие положения законодательства Российской Федерации о гражданско-правовой ответственности	2	Часть 2. Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации).  Общие положения законодательства Российской Федерации о гражданско-правовой ответственности. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности (защиты информации).  Ответственность за проступок в области присвоение авторства (плагиат). Ответственность за проступок за оскорбления, в том числе в социальных сетях.
10	2.2. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности (защиты информации)	1	
11	2.3. Ответственность за проступок в области присвоение авторства (плагиат)	1	
12-13	2.4. Ответственность за проступок за оскорбления, в том числе в социальных сетях	2	
14	Контрольный урок	1	
Часть 3. Административная ответственность за проступки в области информационной			

безопасности (защиты информации)			
15-16	3.1 Административное правонарушение. Основные понятия административного правонарушения	2	<p>Часть 3. Административная ответственность за проступки в области информационной безопасности (защиты информации).</p> <p>Административное правонарушение. Основные понятия административного правонарушения.</p> <p>Особенности административной ответственности несовершеннолетних.</p> <p>Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение.</p> <p>Ответственность за проступок – за оскорбления, в том числе в социальных сетях.</p> <p>Ответственность за проступок - ложный вызов экстренных служб.</p> <p>Ответственность за проступок - пропаганду в Интернете наркотических и психотропных веществ.</p> <p>Ответственность за проступок – нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные).</p> <p>Ответственность за проступок – нарушение правил защиты информации.</p> <p>Ответственность за проступок – представление ложных</p>
17	3.2 Особенности административной ответственности несовершеннолетних.	1	
18-19	3.3 Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение	2	
20-21	3.4 Ответственность за проступок – за оскорбления, в том числе в социальных сетях	2	
22	3.5. Ответственность за проступок - ложный вызов экстренных служб	1	
23-24	3.6 Ответственность за проступок - пропаганду в Интернете наркотических и психотропных веществ	2	
25-26	3.7 Ответственность за проступок – нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные)	2	
27-28	3.8 Ответственность за проступок – нарушение правил защиты информации	2	
29-30	3.9 Ответственность за проступок – представление ложных	2	



	сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство		порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные). Ответственность за проступок – нарушение правил защиты информации.
31	3.10 Ответственность за проступок – за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт	2	Ответственность за проступок – представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство.
32	3.11 Ответственность за проступок – нарушение правил производства, хранения, продажи и приобретения <sup>1</sup> специальных технических средств, предназначенных для негласного получения информации	2	Ответственность за проступок – за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт. Ответственность за проступок – нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации.
33-34	Защита творческих проектов	2	
35	Промежуточная аттестация	1	
36	Контрольный урок	1	
<b>9 класс</b>			
<b>№ урока</b>	<b>Тема урока/ параграф</b>	<b>Общее</b>	<b>Содержание</b>

	<b>учебного пособия</b>	<b>количество часов</b>	
Часть 1. Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)			
1-2	Введение. 1.1. Основные документы в области информационной безопасности Российской Федерации	2	Часть 1. Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации).  Введение. Основные документы в области информационной безопасности Российской Федерации. Информация как объект правовых отношений. Функции, принципы и виды юридической ответственности. Уголовный кодекс Российской Федерации. Виды наказаний в области уголовной ответственности. Ответственность за преступления в области компьютерной информации и применения компьютеров.
3	1.2 Информация как объект правовых отношений	1	
4	1.3 Функции, принципы и виды юридической ответственности.	1	
5-6	1.4 Уголовный кодекс Российской Федерации	2	
7-8	1.5 Виды наказаний в области уголовной ответственности	2	
9-10	1.6 Ответственность за преступления в области компьютерной информации и применения компьютеров	2	
11	1.7 Ответственность за преступления в области присвоения авторства (плагиат)	1	
12	1.8 Ответственность за преступления в области нарушения авторских прав на лицензионное программное обеспечение	1	
13-14	1.9 Ответственность за преступления в области мошенничества (обмана)	2	
15-16	1.10 Ответственность за преступления в	2	

	области нарушения тайны переписки, телефонных переговоров или иных сообщений		<p>нарушения авторских прав на лицензионное программное обеспечение.</p> <p>Ответственность за преступления в области мошенничества (обмана).</p> <p>Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений. Ответственность за преступления – за проведение скрытой (негласной) аудиозаписи.</p> <p>Ответственность за преступления – за заведомо ложное сообщение о теракте.</p> <p>Ответственность за преступления – за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг).</p> <p>Ответственность за преступления – за мошенничество в сфере компьютерной информации.</p> <p>Ответственность за преступления – за незаконное распространение порнографических материалов.</p> <p>Ответственность за преступления – за заведомо ложный донос.</p> <p>Контрольный урок</p>
17-18	1.11 Ответственность за преступления – за проведение скрытой (негласной) аудиозаписи	2	
19	1.12 Ответственность за преступления – за заведомо ложное сообщение о теракте	1	
20-21	1.13 Ответственность за преступления – за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг)	2	
22	1.14 Ответственность за преступления – за мошенничество в сфере компьютерной информации	1	
23-24	1.15 Ответственность за преступления – за незаконное распространение порнографических материалов	2	
25	1.16 Ответственность за преступления – за заведомо ложный донос	1	
26	Контрольный урок	1	

			преступления – за заведомо ложный донос.
Часть 2. Проектные задания			
27	2.1 Лицензионное соглашение свободного ПО Линукс	1	Часть 2. Проектные задания.  Лицензионное соглашение свободного ПО Линукс. Как купить лицензию на платную антивирусную программу. Что такое СС лицензия. Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию. Как задавать безопасный пароль. Настройки телефона, планшета для защиты от несанкционированного доступа.  Защита персональных данных. Обзор. Личный контент в облаке и система его защиты.  Обзор. Личный контент в облаке и система его защиты.
28	2.2 Как купить лицензию на платную антивирусную программу 2.3 Что такое СС лицензия	1	
29	2.4 Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию  2.5 Как задавать безопасный пароль. Настройки телефона, планшета для защиты от несанкционированного доступа	1	
30	2.6 Защита персональных данных. Обзор. Личный контент в облаке и система его защиты	1	
31-32	Защита творческих проектов	2	
33	Промежуточная аттестация	1	
34	Контрольное занятие.	1	

## КРИТЕРИИ И НОРМЫ ОЦЕНИВАНИЯ УЧАЩИХСЯ

### Формы контроля:

*Устно:*

- устный ответ (устные ответы на вопрос, ответ по плану);
- сообщение;

- проект;
- создание иллюстраций, их презентация и защита;
- инсценирование.

*Письменно:*

- составление таблиц;
- тестирование;
- промежуточная аттестация;
- контрольная работа.

**Критерии оценивания:**

**Устный ответ** (развернутый ответ на вопрос, отзыв)

Критерии оценивания устного ответа:

Высокий уровень (Отметка «5») оценивается ответ, обнаруживающий прочные знания и глубокое понимание текста изучаемой темы; умение пользоваться теоретическими знаниями, привлекать текст темы для аргументации своих выводов.

Повышенный уровень (Отметка «4») оценивается ответ, который показывает прочное знание и достаточно глубокое понимание текста изучаемой темы; умение пользоваться основными теоретическими знаниями; умение привлекать текст темы для обоснования своих выводов. Однако допускается одна-две неточности в ответе.

Базовый уровень (Отметка «3») оценивается ответ, свидетельствующий в основном о знании и понимании текста изучаемой темы; знании основных вопросов теории, но недостаточном умении пользоваться этими знаниями при анализе темы; недостаточном умении привлекать текст темы для подтверждения своих выводов. Допускается несколько ошибок в содержании ответа.

Низкий уровень (Отметка «2») оценивается ответ, обнаруживающий незнание существенных вопросов содержания темы; незнание элементарных теоретических понятий.

**Сообщение:**

Высокий уровень (Отметка «5») оценивается сообщение, соответствующий критериям:

1. Соответствие содержания заявленной теме
2. Умение логично и последовательно излагать материалы доклада.
3. Свободное владение материалом, умение ответить на вопросы по теме сообщения.
4. Наличие презентации, схем, таблиц, иллюстраций и т.д.

Повышенный уровень (Отметка «4») оценивается сообщение, удовлетворяющий тем же требованиям, что и для оценки «5», но допускает 1-2 ошибки, которые сам же исправляет, и 1-2 недочета в последовательности излагаемого.

Базовый уровень (Отметка «3») ставится, если ученик обнаруживает знание и понимание основных положений темы сообщения, но:

1. излагает материал неполно и допускает неточности в изложении фактов;
2. не умеет достаточно глубоко и доказательно обосновывать свои суждения и привести свои примеры;
3. излагает материал непоследовательно, допускает ошибки в языковом оформлении излагаемого.

Низкий уровень (Отметка «2») ставится, если ученик обнаруживает незнание большей части излагаемого материала, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

***Создание иллюстраций, их презентация и защита:***

<i>Критерии</i>	<i>Баллы</i>
Красочность. Эстетическое оформление	1
Соответствие рисунка содержанию темы	1
Можно ли понять тему по иллюстрациям без предварительного чтения	1
Самостоятельность выполнения задания	1
Качество презентации и защиты иллюстрации	1

«5» высокий уровень - 5 баллов (выполнены правильно все требования);

«4» повышенный уровень – 3-4 балла (не соблюдены 1-2 требования);

«3» базовый уровень – 2 балла (допущены ошибки по трем требованиям);

«2» низкий уровень – менее 2 баллов (допущены ошибки более, чем по трем требованиям).

***Инсценирование***

<i>Критерии</i>	<i>Баллы</i>
Выразительная игра	1
Правильность произношения слов	1
Выбор костюмов	1
Музыкальное сопровождение	1
Самостоятельность выполнения задания	1

«5» высокий уровень - 5 баллов (выполнены правильно все требования);

«4» повышенный уровень – 3-4 балла (не соблюдены 1-2 требования);

«3» базовый уровень – 2 балла (допущены ошибки по трем требованиям);  
 «2» низкий уровень – менее 2 баллов (допущены ошибки более, чем по трем требованиям).

***Составление таблиц***

<i>Критерии</i>	<i>Баллы</i>
Правильность заполнения	1
Полнота раскрытия материала	1
Наличие вывода	1
Эстетичность оформления	1
Самостоятельность выполнения задания	1

«5» высокий уровень - 5 баллов (выполнены правильно все требования);  
 «4» повышенный уровень – 3-4 балла (не соблюдены 1-2 требования);  
 «3» базовый уровень – 2 балла (допущены ошибки по трем требованиям);  
 «2» низкий уровень – менее 2 баллов (допущены ошибки более, чем по трем требованиям).

***Тестирование***

Высокий уровень (Отметка «5») Выполнено 90-100% заданий теста  
 Повышенный уровень (Отметка «4») Выполнено 70-89% заданий теста  
 Базовый уровень (Отметка «3») Выполнено 50-69% заданий теста  
 Низкий уровень (Отметка «2») Выполнено менее 50% заданий теста

***Промежуточная аттестация***

Высокий уровень (Отметка «5») ставится за правильное выполнение 100% заданий, самостоятельность, тщательность и своевременность выполнения работ, умение пользования справочным материалом;

Повышенный уровень (Отметка «4») ставится за правильное выполнение 90% заданий, самостоятельно, но с небольшим затруднением, выполнение заданий; умение пользования справочным материалом, но ориентируется в нём с трудом, допускает незначительные ошибки.

Базовый уровень (Отметка «3») ставится за правильное выполнение 65%- 90% заданий, самостоятельное выполнение заданий вызывает затруднение, допускает существенные ошибки.

Низкий уровень (Отметка «2») ставится за правильное выполнение менее 65% задани, не выполняет обязательные работы, допускает существенные ошибки.

***Контрольная работа (состоит из теста и краткого ответа на один из проблемных вопросов (по выбору ученика))***

Высокий уровень (Отметка «5») ставится за правильное выполнение 100% заданий тестовой части и ответ на один из проблемных вопросов, обнаруживающий прочные знания и глубокое понимание текста изучаемой темы.

Повышенный уровень (Отметка «4») ставится за правильное выполнение 90% заданий тестовой части и ответ на один из проблемных вопросов, достаточно полно и убедительно раскрывающий тему, обнаруживающий хорошее знание темы. Допускаются две-три неточности в содержании, незначительные отклонения от темы.

Базовый уровень (Отметка «3») ставится за правильное выполнение 65%- 90% заданий тестовой части.

Низкий уровень (Отметка «2») ставится за правильное выполнение менее 65% заданий тестовой части.

### ***Критерии оценивания проектной и исследовательской деятельности***

УУД	Критерии	Баллы
Регулятивные УУД		
Определять и формулировать цель деятельности (понять свои интересы, увидеть проблему, задачу, выразить её словесно) на уроках, внеурочной деятельности, жизненных ситуациях	Умеет самостоятельно поставить и сформулировать задание, определять его цель	2
	Умеет при помощи учителя поставить и сформулировать задание, определять его цель. Иногда выполняет эти действия самостоятельно, но неуверенно	1
	Не способен сформулировать словесно задание, определить цель своей деятельности. Попытки являются единичными и неуверенными	0
Составлять план действий по решению проблемы (задачи) на уроках, внеурочной деятельности, жизненных ситуациях	Умеет самостоятельно прогнозировать результат, составлять алгоритм деятельности при решении проблем учебного, творческого и поискового характера	2
	Умеет самостоятельно прогнозировать результат в основном учебных (по образцу) заданий, планировать алгоритм его выполнения	1
	Не умеет самостоятельно прогнозировать результат даже учебных (по образцу) заданий, планировать алгоритм его выполнения	0
Соотносить результат своей деятельности с целью или с образцом, предложенным учителем	В процессе выполнения задания постоянно соотносит промежуточные и конечные результаты своей деятельности с целью или с образцом, предложенным учителем	2
	В процессе выполнения задания соотносит конечные результаты своей деятельности с целью или с образцом, предложенным учителем – из-за этого теряет много времени	1
	Выполняет задания, не соотнося с целью или с образцом, предложенным учителем. Самостоятельно не может найти ошибку в своей деятельности	0
Самостоятельно осуществлять действия по	Умеет самостоятельно корректировать работу по ходу выполнения задания	2



	реализации плана достижения цели, сверяясь с результатом	Умеет корректировать работу по ходу выполнения задания при указании ему на ошибки извне (учителем или одноклассниками)	1
		Не умеет корректировать работу по ходу выполнения задания при указании ему на ошибки извне (учителем или одноклассниками)	0
Оценка результатов своей работы.		Умеет самостоятельно оценивать результат своей работы. Умеет оценить действия других учеников, выделяет критерии оценки.	2
		Умеет самостоятельно оценивать результат своей работы по предложенным учителем критериям оценки. Не умеет оценить действия других учеников.	1
		Может с помощью учителя соотнести свою работу с готовым результатом, оценка необъективна.	0
ИТОГО: 10-9 баллов высокий уровень, 8-5 баллов средний уровень, 0-4 балла низкий уровень.			
Познавательные УУД			
	Самостоятельно предполагать информацию, которая нужна для обучения, отбирать источники информации среди предложенных	Самостоятельно осуществляет поиск и выделяет необходимую информацию. Применяет методы информационного поиска, в том числе с помощью компьютерных средств.	2
		Самостоятельно осуществляет поиск и выделяет необходимую информацию при помощи учителя или одноклассников	1
		Затрудняется в поиске и выделении необходимой информации даже при оказании ему помощи.	0
Добывать новые знания из различных источников различными способами		Систематически самостоятельно применяет методы информационного поиска, добывает новые знания, в том числе с помощью компьютерных средств.	2
		Эпизодично и, в основном, по заданию учителя применяет методы информационного поиска, в том числе с помощью компьютерных средств.	1
		Не умеет применять методы информационного поиска, в том числе с помощью компьютерных средств.	0
Перерабатывать информацию из одной формы в другую, выбирать наиболее удобную форму. Представлять информацию в виде текста, таблицы, схемы, в том числе с помощью ИКТ		Выбирает наиболее эффективные способы решения задач в зависимости от конкретных условий. Умеет представить результаты работы (исследования) в заданном формате, составить текст отчёта и презентацию с использованием ИКТ.	2
		Выбирает наиболее простые способы решения задач (действует по образцу). Не всегда умеет представить результаты работы (исследования) в заданном формате, составить презентацию с использованием ИКТ.	1
		Затрудняется перерабатывать информацию из одной формы в другую. Не может представлять информацию в виде текста, таблицы, схемы, в том числе с помощью ИКТ	0
	Перерабатывать информацию для получения нового результата.	Умеет выполнять логические действия абстрагирования, сравнения, нахождения общих закономерностей, анализа, синтеза; осуществлять эвристические действия; выбирать стратегию	2

Анализировать, сравнивать, группировать различные объекты, явления, факты	решения; строить и проверять элементарные гипотезы. Способен переработать информацию для получения результата	
	Частично владеет навыками исследовательской деятельности; самостоятельно план проверки предложенной учителем гипотезы; осуществляет наблюдения и эксперименты; умеет классифицировать и обобщать.	1
	Не владеет навыками исследовательской деятельности. Не способен переработать информацию для получения результата	0
Уметь передавать содержание в сжатом, выборочном или развернутом виде, планировать свою работу по изучению незнакомого материала	Определяет основную и второстепенную информацию. Умеет передавать содержание в сжатом, выборочном или развернутом виде. Умеет хранить, защищать, передавать и обрабатывать информацию.	2
	Не всегда определяет основную и второстепенную информацию. Периодически может передавать содержание в сжатом, выборочном или развернутом виде.	1
	Неправильно определяет основную и второстепенную информацию. Не умеет передавать содержание в сжатом, выборочном или развернутом виде.	0
ИТОГО: 10-9 баллов высокий уровень, 8-5 баллов средний уровень, 0-4 балла низкий уровень.		
<b>Коммуникативные УУД</b>		
Доносить свою позицию до других с помощью монологической и диалогической речи с учетом своих учебных и жизненных ситуаций	Умеет оформлять свои мысли в устной или письменной форме с учетом своих учебных и жизненных речевых ситуаций. Критично относится к своему мнению. Осознанно и произвольно строит речевое высказывание в устной и письменной форме.	2
	Умеет использовать речь для регуляции своего действия. Не всегда может донести свою позицию до других.	1
	Не умеет оформлять свои мысли в устной или письменной форме с учетом своих учебных и жизненных речевых ситуаций.	0
Читать различную литературу, понимать прочитанное, владеть навыками смыслового чтения.	Структурирует знания. Понимает цель чтения и осмысливает прочитанное. Умеет задавать вопросы; строить понятные для партнера высказывания, учитывающие, что партнер знает и видит, а что нет.	2
	Умеет читать вслух и про себя тексты учебников, других художественных и научно-популярных книг, извлекать из текста информацию в соответствии с коммуникативной задачей.	1
	Умеет читать вслух и про себя тексты учебников, других художественных и научно-популярных книг. Не умеет извлекать из текста информацию в соответствии с коммуникативной задачей.	0
Понимать возможность различных точек зрения на вопрос. Учитывать	Умеет учитывать разные мнения и стремится к координации различных позиций в сотрудничестве. Умеет договариваться и приходить к общему	2

	разные мнения и уметь обосновывать собственное.	решению в совместной деятельности, в том числе в ситуации столкновения интересов. Умеет контролировать действия партнера.	
		Умеет участвовать диалоге; слушать и понимать других, высказывать свою точку зрения на события, поступки. Умеет отстаивать свою точку зрения, соблюдая правила речевого этикета; аргументировать свою точку зрения с помощью фактов и дополнительных сведений. Понимает и принимает факт, что у людей могут быть различные точки зрения, в том числе не совпадающие с его собственной.	1
		Не умеет участвовать диалоге. Отстаивая свою точку зрения, не соблюдает правила речевого этикета. Не может аргументировать свою точку зрения с помощью фактов и дополнительных сведений. Не считается с другой точкой зрения на проблему.	0
Договариваться с людьми, согласуя с ними свои интересы и взгляды, для того чтобы сделать что-то сообща	Умеет адекватно использовать все коммуникативные средства для решения различных коммуникативных задач, строить монологические высказывания (в том числе сопровождая его аудиовизуальной поддержкой). Владеет диалогической формой коммуникации, используя, в том числе средства и инструменты ИКТ и дистанционного взаимодействия.	2	
	Умеет адекватно использовать речевые средства для решения различных коммуникативных задач, строить сложные монологические высказывания, владеет диалогической речью, выполняя различные роли в группе, умеет сотрудничать в совместном решении проблемы (задачи).	1	
	Не умеет договариваться с людьми, работать в группе, не владеет диалогической речью, не может выполнять различные роли в группе, не умеет сотрудничать в совместном решении проблемы (задачи).	0	
ИТОГО: 10-9 баллов высокий уровень, 8-5 баллов средний уровень, 0-4 балла низкий уровень.			
Личностные УУД			
Самооценка. Оценивать ситуации и поступки (ценностные установки)	Формирует самоуважение и эмоционально-положительное отношение к себе, видны готовность открыто выразить и отстаивать свою позицию, критичность к своим поступкам и умение адекватно их оценивать.	2	
	Проявляет интересы, инициативы и любознательность, учится с четкой организацией своей деятельности. Не всегда открыто выражает и отстаивает свою позицию. Не всегда адекватно себя оценивает.	1	
	В учении не проявляет интересы, инициативы и любознательность. Отмалчивается, не выражает и не отстаивает свою позицию. Не адекватно себя оценивает.	0	
Объяснять смысл своих	Выполняет самостоятельные поступки и действия	2	

оценок, мотивов, целей (личностная саморефлексия, способность к саморазвитию, мотивация к познанию, учебе)	(в том числе руководящего плана), принимает ответственность за их результаты. Целеустремленно и настойчиво идет к достижению целей, готов к преодолению трудностей.	
	Проявляет самостоятельность, инициативу и ответственность как личность. Иногда не доходит до цели, боится преодоления трудностей.	1
	Не проявляет или проявляет крайне редко самостоятельность, инициативу и ответственность как личность. Выполняет только самые простые задания, нацелен на неуспешность.	0
Самоопределяться в жизненных ценностях (на словах) и поступать в соответствии с ними, отвечая за свои поступки (личностная позиция, российская и гражданская идентичность)	Проявляет толерантность и противодействует действиям и влияниям, представляющим угрозу жизни, здоровью и безопасности личности и общества в пределах своих возможностей. Осознает себя гражданином, имеет активную сформированную гражданскую позицию. Участвует в социальном проектировании.	2
	Проявляет уважение к другим людям, самодостоинство. Понимает и принимает возможность человека быть самим собой и принимать самостоятельные решения в самых разных социальных, профессиональных и личностных ситуациях. Осознает себя гражданином, имеет активную, но не до конца сформированную гражданскую позицию.	1
	Не проявляет уважение к другим людям. Не принимает возможность человека быть самим собой. Осознает себя гражданином, имеет пассивную, не сформированную гражданскую позицию.	0
ИТОГО: 6-5 баллов высокий уровень, 4-3 баллов средний уровень, 0-2 балла низкий уровень.		
<p>ИТОГИ ФОРМИРОВАНИЯ УУД (регулятивных, познавательных, коммуникативных, личностный)</p> <p>34-31 баллов - высокий уровень – соответствует оценке «5»</p> <p>30-16 баллов - средний уровень – соответствует оценке «4»</p>		

## ПРИЛОЖЕНИЕ

1. Контрольные работы
2. Примерные темы проектов

### Контрольные работы

#### 5 класс

№ урока	Тема
5	Правила работы с мобильным телефоном.

19	Правила безопасной работы в сети Интернет с планшетом или на компьютере.
25	Путешествуем в сети Интернет.
35	Годовая
<b>Итого</b>	<b>4 часа</b>

#### 6 класс

№ урока	Тема
18	Пространство Интернета на планете Земля.
35	Годовая
<b>Итого</b>	<b>2 часа</b>

#### 7 класс

№ урока	Тема
10	Современное информационное пространство и искусственный интеллект.
21	Современная информационная культура.
35	Годовая
<b>Итого</b>	<b>2 часа</b>

#### 8 класс

№ урока	Тема
7	Понятие юридической ответственности за правонарушение в области информационной безопасности.
14	Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации).
36	Годовая
<b>Итого</b>	<b>3 часа</b>

#### 9 класс

№ урока	Тема
26	Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации).
34	Годовая

<b>Итого</b>	<b>2 часа</b>
--------------	---------------

### Примерные темы проектов

#### 5 класс

<b>№ урока</b>	<b>Тема</b>
32-33	Конкурс рисунков «Правила поведения в сети Интернет»
	Конкурс кроссвордов - презентаций «Цифровая гигиена»
<b>Итого</b>	<b>1</b>

#### 6 класс

<b>№ урока</b>	<b>Тема</b>
32-33	Создание электронного издания «Пространство Интернета на планете Земля»
	Презентация по теме «Правила для пользователей сети Интернет»
<b>Итого</b>	<b>1</b>

#### 7 класс

<b>№ урока</b>	<b>Тема</b>
32-33	Создание медиажурнала «Кибербудущее» в электронной форме в виде страницы сайта или в виде презентации.
<b>Итого</b>	<b>1</b>

#### 8 класс

<b>№ урока</b>	<b>Тема</b>
32-33	Презентация «Виды ответственности за правонарушения в области информационной безопасности»
<b>Итого</b>	<b>1</b>

#### 9 класс

<b>№ урока</b>	<b>Тема</b>
31-32	Создание личного сайта с наполнение (документы Microsoft Word, Microsoft Office Excel, Microsoft Power Point, фото и т.д.)

<b>Итого</b>	<b>1</b>
--------------	----------