

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования Самарской области
Кинельское управление министерства образования Самарской области
ГБОУ СОШ с. Георгиевка

РАССМОТРЕНО

на заседании
МО "Точных наук"
Руководитель МО

Цыганова Э.В.

Протокол №1 от 28.08.2024 г.

СОГЛАСОВАНО УТВЕРЖДЕНО

заместителем
директора по УВР

Климова Е.Ф.
29.08.2024 г.

и.о. директора ГБОУ СОШ
с. Георгиевка

Шафигулина О.С.
Приказ № 85-ОД от 30.08.2024 г.

Рабочая программа
курса внеурочной деятельности

Информационная безопасность

основного общего образования
педагогическое сопровождение (воспитательная направленность)

7 класс

Георгиевка, 2024

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа курса внеурочной деятельности «Информационная безопасность» (далее — курс) для 7 класса составлена на основе требований Федерального государственного образовательного стандарта основного общего образования к результатам освоения основной программы основного общего образования (приказ Министерства просвещения Российской Федерации от 31.05.2021 № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования») с учётом Программы воспитания (протокол Федерального учебно-методического объединения по общему образованию № 3/22 от 23.06.2022) и Основной образовательной программы основного общего образования (протокол Федерального учебно-методического объединения по общему образованию № 1/22 от 18.03.2022).

Рабочая программа курса даёт представление о цели, задачах, общей стратегии обучения, воспитания и развития обучающихся средствами курса внеурочной деятельности, устанавливает содержание курса, предусматривает его структурирование по разделам и темам; предлагает распределение учебных часов по разделам и темам и последовательность их изучения с учётом межпредметных и внутрипредметных связей, логики учебного процесса и возрастных особенностей обучающихся, включает описание форм организации занятий и учебно-методического обеспечения образовательного процесса.

Рабочая программа курса определяет количественные и качественные характеристики учебного материала, в том числе планируемые результаты освоения обучающимися программы курса внеурочной деятельности на уровне основного общего образования и систему оценки достижения планируемых результатов.

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 тёмные, закрытые субкультуры, несущие угрозу здоровью и даже жизни ребенка.

Курс «Информационная безопасность» структурирован по модульному принципу. Он включает в себя 7 модулей:

- Общие сведения о безопасности ПК и Интернета
- Техника безопасности и экология
- Проблемы Интернет-зависимости
- Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы
- Мошеннические действия в Интернете. Киберпреступления
- Сетевой этикет. Психология и сеть
- Правовые аспекты защиты киберпространства

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.

Данный курс реализуется в рамках социального направления внеурочной деятельности и рассчитан на 34 часа 7 классе (1 час в неделю).

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

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

Патриотическое воспитание:

- ценностное отношение к отечественному культурному, историческому и научному наследию;

- понимание значения информатики как науки в жизни современного общества.

Духовно-нравственное воспитание:

- ориентация на моральные ценности и нормы в ситуациях нравственного выбора;
- готовность оценивать своё поведение и поступки, а также поведение и поступки других людей с позиции нравственных и правовых норм, с учётом осознания последствий поступков;
- активное неприятие асоциальных поступков, в том числе в Интернете.

Гражданское воспитание:

- представление о социальных нормах и правилах межличностных отношений в коллективе, в том числе в социальных сообществах;
- соблюдение правил безопасности, в том числе навыков безопасного поведения в интернет-среде;
- ориентация на совместную деятельность при выполнении учебных и познавательных задач, создании учебных проектов;
- стремление оценивать своё поведение и поступки своих товарищей с позиции нравственных и правовых норм, с учётом осознания последствий поступков.

Ценность научного познания:

- наличие представлений об информации, информационных процессах и информационных технологиях, соответствующих современному уровню развития науки и общественной практики;
- интерес к обучению и познанию;
- любознательность;
- стремление к самообразованию;
- овладение начальными навыками исследовательской деятельности, установка на осмысление опыта, наблюдений, поступков и стремление совершенствовать пути достижения индивидуального и коллективного благополучия;
- наличие базовых навыков самостоятельной работы с учебными текстами, справочной литературой, разнообразными средствами информационных технологий, а также умения
- самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учёбе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности.

Формирование культуры здоровья:

- установка на здоровый образ жизни, в том числе и за счёт освоения и соблюдения требований безопасной эксплуатации средств ИКТ.

Трудовое воспитание:

- интерес к практическому изучению профессий в сферах деятельности, связанных с информатикой, программированием и информационными технологиями, основанными на достижениях науки информатики и научно-технического прогресса.

Экологическое воспитание:

- наличие представлений о глобальном характере экологических проблем и путей их решения, в том числе с учётом возможностей ИКТ.

Адаптация обучающегося к изменяющимся условиям социальной среды:

- освоение обучающимся социального опыта, основных социальных ролей, соответствующих ведущей деятельности возраста, норм и правил общественного поведения, форм социальной жизни в группах и сообществах, в том числе в виртуальном пространстве.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Универсальные познавательные действия

Базовые логические действия:

- умение определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логические рассуждения, делать умозаключения (индуктивные, дедуктивные и по аналогии) и выводы;
- умение создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач;
- самостоятельно выбирать способ решения учебной задачи (сравнивать несколько вариантов решения, выбирать наиболее подходящий с учётом самостоятельно выделенных критериев).

Базовые исследовательские действия:

- формулировать вопросы, фиксирующие разрыв между реальным и желательным состоянием ситуации, объекта, и самостоятельно устанавливать искомое и данное;
- оценивать применимость и достоверность информации, полученной в ходе исследования;
- прогнозировать возможное дальнейшее развитие процессов, событий и их последствия в аналогичных или сходных ситуациях, а также выдвигать предположения об их развитии
- в новых условиях и контекстах.

Работа с информацией:

- выявлять дефицит информации, данных, необходимых для решения поставленной задачи;
- применять основные методы и инструменты при поиске и отборе информации из источников с учётом предложенной учебной задачи и заданных критериев;
- выбирать, анализировать, систематизировать и интерпретировать информацию различных видов и форм представления;
- выбирать оптимальную форму представления информации и иллюстрировать решаемые задачи несложными схемами, диаграммами, иными графическими объектами и их комбинациями;
- оценивать достоверность информации по критериям, предложенным учителем или сформулированным самостоятельно;
- запоминать и систематизировать информацию.

Универсальные коммуникативные действия

Общение:

- сопоставлять свои суждения с суждениями других участников диалога, обнаруживать различие и сходство позиций;
- публично представлять результаты выполненного опыта (исследования, проекта);
- выбирать формат выступления с учётом задач презентации и особенностей аудитории и в соответствии с ним составлять устные и письменные тексты с использованием иллюстративных материалов.

Совместная деятельность (сотрудничество):

- понимать и использовать преимущества командной и индивидуальной работы при решении конкретной проблемы, в том числе при создании информационного продукта;
- принимать цель совместной информационной деятельности по сбору, обработке, передаче и формализации информации, коллективно строить действия по её достижению: распределять роли, договариваться, обсуждать процесс и результат совместной работы;
- выполнять свою часть работы с информацией или информационным продуктом, достигая качественного результата по своему направлению и координируя свои действия с другими членами команды;

- оценивать качество своего вклада в общий информационный продукт по критериям, самостоятельно сформулированным участниками взаимодействия;
- сравнивать результаты с исходной задачей и вклад каждого члена команды в достижение результатов, разделять сферу ответственности и проявлять готовность к предоставлению отчёта перед группой.

Универсальные регулятивные действия

Самоорганизация:

- выявлять в жизненных и учебных ситуациях проблемы, требующие решения;
- составлять алгоритм решения задачи (или его часть), выбирать способ решения учебной задачи с учётом имеющихся ресурсов и собственных возможностей, аргументировать выбор варианта решения задачи;
- составлять план действий (план реализации намеченного алгоритма решения), корректировать предложенный алгоритм с учётом получения новых знаний об изучаемом объекте.

Самоконтроль (рефлексия):

- владеть способами самоконтроля, самомотивации и рефлексии;
- учитывать контекст и предвидеть трудности, которые могут возникнуть при решении учебной задачи, адаптировать решение к меняющимся обстоятельствам;
- вносить коррективы в деятельность на основе новых обстоятельств, изменившихся ситуаций, установленных ошибок, возникших трудностей;
- оценивать соответствие результата цели и условиям.

Эмоциональный интеллект:

- ставить себя на место другого человека, понимать мотивы и намерения другого.

Принятие себя и других:

осознавать невозможность контролировать всё вокруг даже в условиях открытого доступа к любым объёмам информации.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

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

В результате освоения программы курса ученик 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 медиаинформационной 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 используются диагностические тесты и опросы, проектные работы и конкурсы по информационной безопасности.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

7 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов).

Как работают мобильные устройства. Угрозы для мобильных устройств.

Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).

Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).

Кто обеспечивает защиту киберпространства.

Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.

Модуль 2. Техника безопасности и экология (5 часов).

Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.

Компьютеры и мобильные устройства в экстремальных условиях.

Везде ли есть Интернет. ТБ при работе с мобильными устройствами.

Первая помощь при проблемах в интернете (службы помощи).

Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).

Модуль 3. Проблемы Интернет-зависимости (2 часа).

Виды Интернет-зависимости.

Компьютер и зрение.

Модуль 4. Методы обеспечения безопасности ПК и Интернета.

Вирусы и антивирусы (8 часов).

Вирусы и антивирусы.

Как распространяются вирусы.

Источники и причины заражения.

Скорая компьютерная помощь. Признаки заражения компьютера.

Что такое антивирусная защита. Как лечить компьютер.

Защита мобильных устройств.

Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.

Защита файлов. Что такое право доступа.

Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (2 часа).

Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.

Прослушивание разговоров. Определение местоположения телефона.

Модуль 6. Сетевой этикет. Психология и сеть (10 часов).

Что такое личные данные. Все, что выложено в Интернет, может стать известно всем. «Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.

Анонимность в сети.

Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.

Как появился нетикет, что это такое. Общие правила сетевого этикета.

Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).

Этика дискуссий. Взаимное уважение при интернет-общении.

Этикет и безопасность. Эмоции в сети, их выражение.

Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.

Если вы стали жертвой компьютерной агрессии: службы помощи.

Модуль 7. Правовые аспекты защиты киберпространства (2 часа).

Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.

Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

№ п/п	Наименование модулей	Кол-во часов
1	Общие сведения о безопасности ПК и Интернета	5
2	Техника безопасности и экология.	5
3	Проблемы Интернет-зависимости	2
4	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	8
5	Мошеннические действия в Интернете. Киберпреступления	2
6	Сетевой этикет. Психология и сеть	10
7	Правовые аспекты защиты киберпространства	2

	Всего часов:	34
--	---------------------	-----------

Поурочное планирование

7 класс (34 часа)

№ урока	Тема	Кол-во часов
	Общие сведения о безопасности ПК и Интернета	5
1	Как работают мобильные устройства. Угрозы для мобильных устройств.	1
2	Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).	1
3	Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).	1
4	Кто обеспечивает защиту киберпространства.	1
5	Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.	1
	Техника безопасности и экология.	5
6	Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.	1
7	Компьютеры и мобильные устройства в экстремальных условиях.	1
8	Везде ли есть Интернет. ТБ при работе с мобильными устройствами.	1
9	Первая помощь при проблемах в интернете (службы помощи).	1
10	Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).	1
	Проблемы Интернет-зависимости.	2
11	Виды Интернет-зависимости.	1
12	Компьютер и зрение.	1
	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	8
13	Как распространяются вирусы.	1
14	Источники и причины заражения.	1
15	Скорая компьютерная помощь. Признаки заражения компьютера.	1
16	Что такое антивирусная защита. Как лечить компьютер.	1
17	Защита мобильных устройств.	1
18	Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.	1
19	Защита файлов. Что такое право доступа.	1
20	Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.	1
	Мошеннические действия в Интернете. Киберпреступления.	2
21	Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.	1
22	Прослушивание разговоров. Определение местоположения телефона.	1
	Сетевой этикет. Психология и сеть.	10
23	Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.	1
24	«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.	1
25	Анонимность в сети.	1

26	Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.	1
27	Как появился нетикет, что это такое. Общие правила сетевого этикета.	1
28	Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).	1
29	Этика дискуссий. Взаимное уважение при интернет-общении.	1
30	Этикет и безопасность. Эмоции в сети, их выражение.	1
31	Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.	1
32	Если вы стали жертвой компьютерной агрессии: службы помощи.	1
	Правовые аспекты защиты киберпространства.	2
33	Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.	1
34	Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	1