

## Модули

### Общие сведения о безопасности ПК и Интернета

1. Интернет - средство для поиска полезной информации. Где и как искать информацию для урока. Что такое файл. Какие файлы можно скачивать а какие нельзя (2/20)
2. Компьютер – как он появился, как появился Интернет (2/20)
3. Из чего сделан компьютер (2/20)
4. Как Интернет приходит в дом. Из чего «сделана» сеть (2/20)
5. Как сохранить результаты своих наблюдений на школьном компьютере и не потерять их. Кому принадлежит файл (2/20)
6. Как обращаться со своими и чужими файлами, чтобы их не потерять. Как защищают файлы (2/15)
7. Где узнать прогноз погоды в Интернете. Научиться не отвлекаться на лишнюю информацию (2/20)
8. Как найти и сохранить полезные рисунки и фотографии. Не отвлекаться на лишнюю информацию (2/20)
9. Как учиться в Интернете. Полезные и вредные страницы Интернета (2/20)
10. Как принести в класс фотографии и рисунки для урока и не повредить школьному компьютеру (2/15)
11. Цифровой фотоаппарат. Как с ним правильно обращаться и как переносить фотографии на компьютер (2/15)
12. На каких устройствах можно сохранить информацию и как с ними правильно обращаться (диски, флэш, карты и пр.) (2/15)
13. Как найти в Интернете голоса животных - полезные страницы со звуковой информацией. Как не тратить лишнее время на поиск (2/20)
14. Как найти в Интернете полезный фильм о животных и не повредить компьютеру. Как не тратить время на просмотр ненужных фильмов (2/15)
15. Сколько информации можно скачать из Интернета? Лишняя информация на компьютере (2/15)
16. Как Интернет помогает транспорту. Что будет, если Интернет перестанет работать? (2/15)
17. Как компьютер управляет дорожным движением (2/15)
18. Польза компьютера для разных профессий. Почему компьютер важно защищать (2/20)
19. Возьми с собой за город электронного помощника. Мобильные устройства (2/15)
20. Общение в Интернете – переписка, форумы, социальные сети. Совместные игры в Интернете (2/20)
21. Как отличать полезную и правдивую информацию (2/20)
22. Как работать в группе. Как передать товарищам результаты работы и не повредить их компьютерам. Что такое электронная почта (2/20)
23. Сохранение полезной информации. Коллекция ссылок. Неосторожность пользователя – опасность для компьютера и данных (3/20)
24. Опыты в Интернете. Можно ли «испортить» Интернет (3/20)
25. Обмен данными при совместной работе – скайп, IP-телефония, ICQ. Безопасный обмен данными (3/20)
26. Компьютер и умственный труд. Как «думает» компьютер и что этому может помешать (3)

27. Полезные ископаемые, используемые при производстве компьютера. Почему компьютер нужно беречь (3)
28. Польза Интернета и компьютера в сельском хозяйстве. Какой вред могут принести неисправности Интернета и компьютера и что может их вызвать (3)
29. Компьютер и Интернет в промышленности – почему они нуждаются в защите (3)
30. Как найти информацию о городах? Ненужные ссылки, ложные ссылки, реклама. Что такое вредоносные сайты (3)
31. Как Интернет помогает путешествовать – покупка билетов в Интернете и возможные проблемы (3)
32. Интернет в путешествиях – польза и опасности. Сколько стоит Интернет (3)
33. Как компьютер помогает науке и почему он нуждается в защите. Наука о защите компьютеров (4)
34. Поиск информации в Интернете. Доступ к разрешенной информации – что это такое (4)
35. Поиск в Интернете. Где Интернет хранит свои данные. Как сохранить в сети найденную информацию. Что такое облачные сервисы – безопасны ли они? (4)
36. Поиск исторических документов в сети – все ли найденные данные правдивы и полезны? Как защитить себя от информационной перегрузки (4)
37. Поиск информации в сети: к чему ведет переход по вредоносным ссылкам. Опасная информация в сети (4)
38. Виды Интернет-общения. Безопасно ли общение в Интернете? (4)
39. Когда появились компьютер и Интернет. Как вместе с Интернетом появились его болезни (4)
40. Что такое дистанционное обучение. Есть ли у него минусы? (4)
41. Что такое компьютерная грамотность (4)
42. Интернет, телефон и космос. Польза и опасности мобильной связи (4)
43. День системного администратора и день программиста – что это за профессии? Что они делают для кибербезопасности? (4)
44. Как устроены компьютер и интернет (5)
45. Что такое программное и аппаратное обеспечение (5)
46. Какие программы должны быть установлены на компьютере (5)
47. Компьютер и системы безопасности (5)
48. Сетевые игры как массовые развлечения. Бесплатные и платные игры (5)
49. Кибербезопасность – что это такое (5)
50. Как работают мобильные устройства. Угрозы для мобильных устройств (6)
51. Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание картинок, музыки, игр) (6)
52. Виды защиты информации (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации) (6)
53. Кто обеспечивает защиту информации (6)
54. Что такое геоинформационные системы. Глобальные информационные Сети по стихийным бедствиям (6)
55. Информационная безопасность (7)
56. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные (7)
57. Источники данных в Интернете: почта, сервисы обмена файлами и др. Хранение данных в Интернете (7)
58. Возможности и проблемы социальных сетей (7)
59. Безопасный профиль в социальных сетях. Составление сети контактов (7)

60. Защита информации как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности (8)
61. Компьютерная и информационная безопасность, обнаружение проблем в сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации (8)
62. Что такое защищенная информационная среда. Защита каналов передачи данных, средства предотвращения утечки информации, защита информации от НСД (антивирусная защита, средства контроля защищенности, средства обнаружения и предупреждения атак), средства аутентификации (8)
63. Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления (8)
64. Требования к безопасности информации: сохранение целостности, конфиденциальности и доступности. Определения по ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения» (8)
65. Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации (8)
66. Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты) (8)
67. Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi (8)
68. Угрозы информации (техногенные, случайные и преднамеренные; природные) Неосторожность пользователя как одна из угроз для информационной безопасности (8)
69. Меры кибербезопасности для конечных пользователей. Использование рекомендованных версий операционных систем и приложений, использование антивирусных средств, настройка веб-браузеров, блокировка скриптов, использование фильтров фишинга, межсетевых экранов. Автоматическое обновление ПО (8)
70. Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности) (8)
71. Кибертерроризм и кибервойны (9)
72. Кибератаки и техногенные катастрофы. Защита IT-инфраструктур критически важных объектов (9)
73. Категории информационной безопасности (9)
74. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение) (9)
75. Защита информации как комплекс мероприятий, направленных на обеспечение информационной безопасности (9)
76. Защита от несанкционированного доступа к информационным ресурсам; защита от искажения и утраты информации; защита от разрушения целостности программных и информационных структур; защита от прерывания обслуживания (9)
77. Шифрование при передаче конфиденциальной информации. Что такое цифровая подпись (9)

78. Регистрация и аудит в организации безопасности информации. Что такое политика безопасности (9)
79. Риски интернета (контентные, электронные, коммуникационные, потребительские) (9)
80. Безопасный серфинг (9)
81. Безопасные ресурсы для поиска (9)
82. Проблемы электронной торговли (9)
83. Проблемные сайты (9)
84. Ложные ресурсы сети (9)
85. Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях (10)
86. Интернет как оружие массового поражения (10)
87. Опасная информация в сети (порносайты, киберсекс, сайты азартных игр, сайты о наркотиках, экстремистские, сектантские, террористические и националистические) (10)
88. Социальные последствия безответственного поведения в интернете (10)
89. Угрозы для IOS-устройств. Угрозы для Android-устройств (10)
90. Проблемы безопасности информационных систем. Методы обеспечения защиты данных в СУБД (11)
91. Защита государственных информационных систем (11)
92. Проблемы безопасности банковских систем (11)
93. Безопасность платежных систем (11)
94. Безопасность геоинформационных систем (11)
95. Безопасность систем бронирования билетов (11)
96. Безопасность корпоративных баз данных (11)
97. Безопасность медицинских информационных систем (11)
98. Безопасность при удаленном доступе к ресурсам компьютера (11)
99. Хакерские атаки. Как уронить сайт. Виды атак (11)
100. Кибербезопасность и киберпространство. Киберкультура (11)
101. Новые технологии и новые угрозы информационной безопасности (применение робототехники и т.п.). Рост числа угроз для мобильных устройств (11)
102. Рост числа атак на инфраструктуру (11)
103. Кибершпионаж (11)
104. Кибероружие (11)
105. Специальности, связанные с защитой информации (11)

### **Техника безопасности и экология**

1. Правила работы с ПК и электронными книгами. Спроси учителя (2/20)
2. Компьютер и электронная книга – как защитить их от воды, жары и холода (2/15)
3. Для компьютера тоже важен чистый воздух (2/15)
4. Стоит ли размещать рядом компьютер и домашние растения (2/15)
5. Компьютер и домашние животные, как защитить их друг от друга (2/15)
6. Что такое мультимедиа, правила безопасной работы (2/15)
7. Сканер и принтер – как с ними правильно обращаться. Спроси у взрослых (2/15)
8. Сколько времени можно проводить за компьютером. Как правильно сидеть за компьютером (2/20)
9. Как правильно включать и выключать компьютер. Как защитить компьютер от повреждений (2/15)

10. Если компьютер сломался (2/15)
11. Незнакомцы в Интернете. Странные звонки по мобильному телефону (2/20)
12. Стоит ли в транспорте включать планшет или мобильные устройства (2/10)
13. Везде ли есть Интернет? Может ли компьютер заменить компас. Как мобильные устройства помогают ориентироваться на местности (2/20)
14. Вредит ли компьютер экологии (излучения, волны) (3/20)
15. Воздействие компьютера на зрение и др. органы (3/20)
16. Гигиена при работе с компьютером (3/20)
17. Как загрязняется компьютер. Гигиена компьютера (3/20)
18. Компьютер и осанка (3/20)
19. Стоит ли есть за компьютером (3/20)
20. Компьютер и кровообращение (3/20)
21. Польза и вред компьютерных игр. Компьютер и недостаток движения (3/20)
22. Компьютер и ЗОЖ. Физическое и психическое здоровье (3/20)
23. Что делать с компьютером в чрезвычайных ситуациях (3/20)
24. Компьютер на улице и в общественном транспорте (3/20)
25. Улица и мобильные устройства (3/20)
26. Компьютер в грозу (3)
27. Что происходит со сломанным компьютером? (3)
28. Электронная книга. Польза и вред (4)
29. Превращение виртуальных знакомых в реальных (4)
30. Правила поведения в компьютерном классе (5)
31. Интернет в системе безопасности. Как защитить сам Интернет (5)
32. Техника безопасности при работе с компьютером. Источники питания компьютера (5)
33. Что делать если вода попала в компьютер или ноутбук (5)
34. Может ли загореться компьютер (5)
35. Может ли вирус сломать компьютер? Чем тушить загоревшуюся выч. технику (5)
36. Компьютер и мобильные устройства в чрезвычайных ситуациях (5)
37. Компьютер и мобильные устройства в чрезвычайных ситуациях в метро (5)
38. Компьютер и мобильные устройства в чрезвычайных ситуациях в авиатранспорте (5)
39. Информационная перегрузка (5)
40. Информация, вредная для здоровья (5)
41. Медицинская информация в Интернете – всегда ли она полезна (5)
42. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности (6)
43. Компьютеры и мобильные устройства в экстремальных условиях (6)
44. Везде ли есть Интернет. ТБ при работе с мобильными устройствами (6)
45. Первая помощь при проблемах в интернете (службы помощи) (6)
46. Компьютер и зрение (6)
47. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM) (6)
48. Кибератаки на инфраструктуру (8)
49. Компьютер в режиме труда и отдыха. Информационная перегрузка (8)
50. Комплекс упражнений при работе за компьютером (7)
51. Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов (7)
52. Влияние компьютера на репродуктивную систему (8)
53. Инструкция по технике безопасности при работе на компьютере. Электропитание и подключение к Интернету (9)
54. Комплексы упражнений для зрения при работе с ПК (10 мин) (9)
55. Вредные факторы работы за компьютером и их последствия (9)
56. Гигиена при работе с ПК (10 мин) (9)
57. ПК и ЗОЖ. Организация рабочего места (10)

## **Проблемы Интернет-зависимости**

1. Общий компьютер – как его поделить? Почему родители проверяют, что ты делаешь в Интернете? (2/20)
2. Что такое Интернет-сообщество. Как не превратить свою жизнь в виртуальную (3/20)
3. Если слишком долго находиться в Интернете: что такое интернет-зависимость? (4)
4. Социальные сети. Детские социальные сети. Какую информацию о себе следует выкладывать в сеть? Какая информация принадлежит вам? Не слишком ли много у вас друзей в социальной сети? (4)
5. Виртуальная личность – что это такое (4)
6. Зависимость от Интернет-общения (4)
7. Развлечения в Интернете. Игры полезные и вредные. Признаки игровой зависимости (4)
8. Сетевые игры (4)
9. Сайты знакомств (4)
10. ЗОЖ и компьютер. Виды зависимости. Как определить наличие зависимости (5)
11. Деструктивная информация в Интернете – как ее избежать (5)
12. Виды Интернет-зависимости (6)
13. Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред (7)
14. Киберкультура (массовая культура в сети) и личность (7)
15. Психологическое воздействие информации на человека. Управление личностью через сеть (7)
16. Интернет- и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость (8)
17. Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости) (8)
18. Интернет как наркотик (9)
19. Классификация интернет-зависимостей (10)

## **Методы обеспечения безопасности ПК и Интернета**

1. Что такое электронные деньги, как с ними правильно обращаться (2/15)
2. Движение в Интернете (серфинг). Знаки Интернета, рассказывающие об опасной информации (3/20)
3. Ищите в Интернете только то, что вам требуется. Как защититься от вредного контента. Что такое контент-фильтры (4)
4. Поиск информации. Что такое поисковые серверы? Как с их помощью защитить себя от нежелательной информации (4)
5. Поиск информации. Родительский контроль. Какие программы для этого существуют (4)

6. Поиск информации. Обращайте внимание на предупреждения о вредоносном содержимом по найденной ссылке (4)
7. Защита мобильных устройств (6)
8. Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные (6)
9. Защита файлов. Что такое право доступа (6)
10. Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети (6)
11. Защита файлов. Права пользователей (7)
12. Защита при загрузке и выключении компьютера (7)
13. Безопасность при скачивании файлов (7)
14. Безопасность при просмотре фильмов онлайн (7)
15. Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты (7)
16. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы. (7)
17. Методы защиты фото и видеоматериалов от копирования в сети (7)
18. Защита от копирования контента сайта (7)
19. Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты (8)
20. Проверка подлинности (аутентификация) в Интернете (8)
21. Меры безопасности для пользователя WiFi. Настройка безопасности (8)
22. Настройка компьютера для безопасной работы (8)
23. Ошибки пользователя (установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.) (8)
24. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях (8)
25. Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей (9)
26. Простые и динамически изменяющиеся пароли (9)
27. Борьба с утечками информации. Средства контроля доступа (9)
28. Права пользователей. Способы разграничения доступа (9)
29. Средства защиты в сети: межсетевые экраны, криптомаршрутизаторы, серверы аутентификации и т.д. Обманные системы для защиты информации в сетях (9)
30. Защита сайтов (9)
31. Системы обнаружения атак. Безопасность хостинга (9)
32. ТБ при работе с почтой (9)
33. ТБ при загрузке файлов (9)
34. Основные меры кибербезопасности. Безопасность приложений, серверов, конечных пользователей (10)
35. Защита от атак, повышение готовности (10)
36. Аппаратная защита ПО и сети (электронные ключи, аппаратные брандмауэры) (10)
37. Защита ПК на этапе загрузки. Параметры безопасности ПК. Обновления (10)
38. Защита файловой системы. Файловые таблицы. Права доступа (10)
39. Резервное копирование и восстановление данных. Восстановление ОС. Аппаратные и программные средства (10)

40. Чем отличаются методы защиты операционной системы, программного обеспечения и данных (10)
41. Как узнать местоположение компьютера по IP-адресу (11)
42. Онлайн сервисы для безопасности пользователя в интернете (проверка компьютера и файлов на вирусы онлайн, онлайн деактивация SMS-вирусов, проверка сайта на вирусы, проверка файлов по e-mail, определение адреса страницы, проверка стоимости СМС и др.) (11)
43. Настройки безопасности почтовых программ (11)
44. Защита в поисковых системах (фильтры для ограничения потенциально опасного содержимого). Настройки безопасности веб-браузеров (Internet Explorer, Firefox и т.п.) (11)
45. Электронная почта и системы мгновенного обмена сообщениями. Настройки безопасности Скайп, ICQ и пр. (11)
46. Способы обеспечения безопасности веб-сайта (11)

### **Вирусы и антивирусы**

1. Правильно ли работает компьютер? Признаки работы вирусов (4)
2. Вирусы человека и компьютера (5)
3. Цели компьютерных вирусов (5)
4. Лечение компьютера (5)
5. Как распространяются вирусы (6)
6. Источники и причины заражения (6)
7. Скорая компьютерная помощь. Признаки заражения компьютера (6)
8. Что такое антивирусная защита. Как лечить компьютер (6)
9. Как развивались вирусы (7)
10. Могут ли вирусы воздействовать на аппаратуру ПК (7)
11. Как вирусы воздействуют на файлы (7)
12. Проверка на наличие вирусов. Сканеры и др. (7)
13. Может ли вирус воздействовать на рабочий стол (7)
14. Источники заражения ПК (7)
15. Антивирусное ПО, виды и назначение (7)
16. Методы защиты от вирусов. Как распознаются вирусы (7)
17. Вирусы для мобильных устройств (мобильные банкеры и др.) (8)
18. Типы вирусов. Отличия вирусов и закладок (9)
19. Антивирусные программы для ПК: сканеры, ревизоры и др. Выявление неизвестных вирусов (9)
20. Признаки заражения компьютерных программ. Где можно обнаружить подозрительные процессы (10)
21. ОС и их возможности в борьбе с вирусами (Windows. Linux) (10)
22. Разновидности вирусов. Черви, трояны, скрипты и др. Шпионские программы. Шифровальщики. Хакерские утилиты. Сетевые атаки (10)
23. Защитное ПО. Антивирусные программы. Межсетевые экраны. Брандмауэры (10)
24. Антивирусная защита ПК, сети и мобильных пользователей (10)
25. Наиболее известные антивирусные программы. Kaspersky Internet Security. Dr.Web Security Space. ESET NOD32 Smart Security. Бесплатные программы-сканеры (10)
26. Настройка антивирусного ПО (10)
27. Коммерческое и бесплатное антивирусное ПО (10)



## **Мошеннические действия в Интернете. Киберпреступления**

1. Поиск информации. «Ненужные» ссылки и реклама (3/20)
2. Интернет и экономика – польза и опасность. Кто и как может навредить в Интернете (3)
3. Электронная торговля – ее опасности (3)
4. Сколько стоят ошибки в Интернете (3)
5. Поиск информации: если у вас требуют личную информацию при скачивании данных. Что такое личная информация (4)
6. Поиск в Интернете. Если вам сообщают о выигрыше в лотерею (4)
7. Поиск в Интернете. Если вам предлагают установить новое приложение (4)
8. Поиск в Интернете. Если вам предлагают бесплатные игры (4)
9. Поиск информации. Если вам предлагают что-то купить (4)
10. Киберпреступления – что это такое (5)
11. Виды интернет-мошенничества (письма, реклама, охота за личными данными и т.п.) (5)
12. Виртуальные друзья – кто они (5)
13. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС (6)
14. Прослушивание разговоров. Определение местоположения телефона (6)
15. Утечка и обнародование личных данных (7)
16. Подбор и перехват паролей. Взломы аккаунтов в социальных сетях (7)
17. Виды мошенничества в Интернете. Фишинг (фарминг) (7)
18. Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею (7)
19. Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы (8)
20. Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники (8)
21. Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды (8)
22. Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег (8)
23. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса (8)
24. Платные предложения работы. Платный просмотр видеоматериалов (8)
25. Технологии манипулирования в Интернете (8)
26. ТБ при интернет-общении (9)
27. ТБ при регистрации на веб-сайтах. ТБ на сайтах знакомств (11)
28. Компьютерное пиратство. Плагиат (11)
29. Кибернаемники и кибердетективы (11)
30. Оценка ущерба от киберпреступлений (11)

## **Сетевой этикет. Психология и сеть**

1. Что такое интернет-этикет (2/20)
2. Как вести себя «в гостях» у сетевых друзей (2/15)
3. Помогает ли компьютер стать лучше? Общение в социальных сетях (3/20)
4. Этикет в Интернете при работе с проектом в группе (3)
5. Что такое нетикет и почему он появился (5)

6. Правила общения в Интернете. Основы сетевого этикета (5)
7. Переписка в сети. Этикет при переписке. Что такое спам (5)
8. Правила поведения в скайпе (5)
9. Что такое форум. Зачем существует модерация (5)
10. Общение в сети и его последствия. Агрессия в сети (5)
11. Психологическое влияние через Интернет (5)
12. Как защитить себя в Интернете (5)
13. Что такое личные данные. Все, что выложено в Интернет, может стать известно всем (6)
14. «Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам (6)
15. Анонимность в сети (6)
16. Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах (6)
17. Как появился нетикет, что это такое. Общие правила сетевого этикета (6)
18. Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений) (6)
19. Этика дискуссий. Взаимное уважение при интернет-общении (6)
20. Этикет и безопасность. Эмоции в сети, их выражение (6)
21. Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться (6)
22. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибермоббинг, троллинг, буллицид (6)
23. Если вы стали жертвой компьютерной агрессии: службы помощи (6)
24. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Сетевой этикет. Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др. (8)
25. Примеры этических нарушений (9)
26. Значение сетевого этикета (10)

## **Правовые аспекты защиты информации**

1. Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация (6)
2. Защита прав потребителей при использовании услуг Интернет (7)
3. Защита прав потребителей услуг провайдера (7)
4. Как расследуются преступления в сети (8)
5. Ответственность за интернет-мошенничество (8)
6. Правовые акты в области информационных технологий и защиты информации (40 мин) (9)
7. Ответственность за киберпреступления (10)
8. Конституционное право на поиск, получение и распространение информации. Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию" (действует с 1 сентября 2012 года) (10)
9. Информационное законодательство РФ. Закон РФ "Об информации, информационных технологиях и о защите информации" (10)

10. Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ (ст. 237 УК РФ) (10)
11. Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo) (10)
12. Правовые основы для защиты от спама (11)
13. Правовые основы защиты интеллектуальной собственности. Авторское право. Правовая охрана программ для ЭВМ и БД (11)
14. Лицензионное ПО. Виды лицензий (ОЕМ, FPP, корпоративные лицензии, подписка). ПО с открытым кодом (GNU GPL, FreeBSD) (11)
15. Право на информацию, на сокрытие данных, категории информации. Персональные и общедоступные данные, ограниченный доступ. Закон «О персональных данных». Указ президента РФ о создании действенной системы противодействия компьютерным атакам от 15 января 2013 г. (11)
16. Уголовный кодекс РФ, раздел «Преступления в сфере компьютерной информации» (11)

### **Государственная политика в области информационной безопасности**

1. Как государство защищает информацию (3)
2. Войны нашего времени. Что такое кибервойна (4)
3. Что такое информация. Право на информацию в Конституции (4)
4. Почему государство защищает информацию (4)
5. Защита государства и защита информации (4)
6. Доктрина информационной безопасности (9)
7. Кибервойска (10)
8. Защита информации как одна из задач вооруженных сил (10)
9. Информационная война. Информационное оружие (10)
10. Патриотизм и интернет (10)
11. Информационная война. Информационное воздействие (11)
12. Военная, государственная, коммерческая тайна. Защита сайтов государственных органов (электронное правительство) (11)
13. Какие органы власти отвечают за защиту информации (11)