Тонких И.М.

Комаров М.М.

Ледовской В.И.

Михайлов А.В.

# ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Описание курса для средних школ, 2-11 классы

Москва, 2016 г.

# Оглавление

1. Основы кибербезопасности. Цели и задачи курса ..... 4

2. Модули курса «Основы кибербезопасности» ..... 8

2.1. Общие сведения о безопасности ПК и Интернета ..... 8

2.2. Техника безопасности и экология ..... 16

2.3. Проблемы Интернет-зависимости ..... 18

2.4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы ..... 20

2.5. Мошеннические действия в Интернете. Киберпреступления ..... 25

2.6. Сетевой этикет. Психология и сеть ..... 27

2.7. Правовые аспекты защиты киберпространства ..... 28

2.8. Государственная политика в области кибербезопасности ..... 30

3. Соответствие содержания материала курса «Основы кибербезопасности» содержанию Стандарта основного общего образования по информатике ..... 31

4. Примеры уроков по курсу «Основы кибербезопасности» ..... 47

4.1. 2 класс. Как принести в класс фотографии и рисунки для урока и не повредить школьному компьютеру? ..... 47

4.2. 3 класс. Как загрязняется компьютер. Гигиена компьютера ..... 52

4.3. 4 класс. Виды Интернет-общения. Безопасно ли общение в Интернете? ..... 56

4.4. 5 класс. Здоровый образ жизни и компьютер. Виды зависимости. Как определить наличие зависимости ..... 61

4.5. 6 класс. Как распространяются вирусы ..... 67

4.6. 7 класс. Утечка и обнародование личных данных ..... 73

4.7. 8 класс. Подмена сайтов в интернете (сайты-клоны). Фальшивые файлообменники ..... 80

4.8. 9 класс. Типы вирусов. Отличия вирусов и закладок ..... 86

4.9. 10 класс. Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo)..... 94

4.10. 11 класс. Настройки безопасности веб-браузеров (фильтры для ограничения потенциально опасного содержимого). Настройки безопасности веб-браузеров (Internet Explorer, Firefox и т.п.) ..... 104

## 1. Основы кибербезопасности. Цели и задачи курса

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов в числе многих других задач выделяются:

- обеспечение различных сфер экономики качественными информационными технологиями;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Компьютерные технологии применяются при изучении практически всех школьных дисциплин уже с младших классов, поэтому, как указано в «Стратегии развития отрасли информационных технологий в Российской Федерации»:

«Необходимо совершенствовать современную профессиональную подготовку учителей информатики и преподавателей дисциплин в сфере информационных технологий», а значит, и в сфере кибербезопасности. Киберугрозы существуют везде, где применяются информационные технологии, следовательно, преподаватель любой дисциплины может в профессиональной деятельности столкнуться и со спамом, и с вирусами, и со взломом компьютера и с многими другими проблемами, на которые нужно не только оперативно реагировать, но и насколько возможно уметь предотвращать их появление, а значит, постоянно упоминать в контексте урока различные аспекты организации информационной безопасности. Преподаватель должен иметь представление о современном уровне развития вычислительной техники, информационный сетей, технологий коммуникации и навигации.

Государство считает необходимым расширение объема преподавания информационных технологий в общеобразовательных организациях. В качестве одной из организационных мер в обеспечении кибербезопасности определена разработка и внедрение в учебный процесс образовательных организаций разного уровня курса по информационной безопасности, включающего модули по обеспечению кибербезопасности, либо дополнение имеющихся курсов упомянутыми модулями. Школьная программа должна соответствовать этим целям, поэтому представляется актуальным дополнить модулями по «Основам кибербезопасности» курсы «Информатика», «Окружающий мир (Природоведение)», «Основы безопасности жизнедеятельности» и, возможно, других предметов.

С учетом роста числа угроз информационной деятельности и стремительного развития информационных технологий представляется необходимым включить в ФГОСы соответствующие требования, что позволило бы органически дополнить образовательный процесс новыми модулями без рассогласования с имеющимися учебными планами. В число требований к результатам подготовки учащихся необходимо включить не только «удовлетворение познавательных интересов,

поиск дополнительной информации»[1], знание «технических устройств (в том числе компьютеров)», умение «искать информацию с применением правил поиска (построения запросов) в базах данных, компьютерных сетях, пользоваться персональным компьютером и его периферийным оборудованием; следовать требованиям техники безопасности, гигиены, эргономики и ресурсосбережения при работе со средствами информационных и коммуникационных технологий», но и знание основ кибербезопасности, умения соблюдать требования кибербезопасности в практической деятельности и организовывать безопасность личного информационного пространства.

Необходимо отметить, что в настоящее время требования ФГОС для уровней начального, общего и полного среднего образования не содержат предметной области «Основы кибербезопасности», но в рамках метапредметных результатов и предметных умений дисциплины «Информатика» вопросы информационной безопасности обозначены:

- требование формирования навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права;
- умения использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;
- понимание основ правовых аспектов использования компьютерных программ и работы в Интернете и т.п.

Базой курса «Основы кибербезопасности» является модель непрерывного информационного образования в школе, причем вопросы кибербезопасности

[1] Об утверждении федерального компонента государственных образовательных стандартов начального общего, основного общего и среднего (полного) общего образования. Приказ Министерства образования Российской Федерации №1089 от 5 марта 2004 года (с изменениями на 23 июня 2015 года)

должны постоянно рассматриваться как при изучении информатики, так и других предметов. Поэтому одна из целей курса – повышение квалификации в области кибербезопасности преподавателей всех дисциплин, в которых так или иначе используются компьютерные технологии. Наиболее очевидной является возможность дополнения вопросами кибербезопасности уроков информатики, если учебный план школы предусматривает ее изучение в продолжение всего школьного курса. Однако можно включить модули по кибербезопасности в курсы «Окружающий мир», «Основы безопасности жизнедеятельности», «Технология», «Обществознание», тем более что вопросы организационного и правового обеспечения информационной безопасности хорошо согласуются с имеющимися требованиями к уровню подготовки учащихся.

Задача курса «Основы кибербезопасности» – совершенствование школьного образования и подготовки в сфере информационных технологий, а также популяризация профессий, связанных с информационными технологиями. Цель изучения «Основ кибербезопасности» – дать общие представления о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.

Воспитательная цель курса – формирование на качественно новом уровне культуры умственного труда и взаимодействия с окружающими, ответственного отношения к вопросам безопасности жизнедеятельности.

## 2. Модули курса «Основы кибербезопасности»

### 2.1. Общие сведения о безопасности ПК и Интернета

**2 класс**

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. Компьютер – как он появился, как появился Интернет
3. Из чего сделан компьютер
4. Как Интернет приходит в дом. Из чего «сделана» сеть
5. Как сохранить результаты своих наблюдений на школьном компьютере и не потерять их. Кому принадлежит файл
6. Как обращаться со своими и чужими файлами, чтобы их не потерять. Как защищают файлы
7. Где узнать прогноз погоды в Интернете. Как научиться не отвлекаться на лишнюю информацию
8. Как найти и сохранить полезные рисунки и фотографии
9. Как учиться в Интернете. Полезные и вредные страницы Интернета
10. Как принести в класс фотографии и рисунки для урока и не повредить школьному компьютеру
11. Цифровой фотоаппарат. Как с ним правильно обращаться и как переносить фотографии на компьютер
12. На каких устройствах можно сохранить информацию и как с ними правильно обращаться (диски, флэш, карты и пр.)
13. Как найти в Интернете полезные страницы со звуковой информацией. Как не тратить лишнее время на поиск
14. Как найти в Интернете полезный фильм и не повредить компьютеру. Как не тратить время на просмотр ненужных фильмов

15. Сколько информации можно скачать из Интернета? Лишняя информация на компьютере
16. Как Интернет помогает транспорту. Что будет, если Интернет перестанет работать?
17. Как компьютер управляет дорожным движением
18. Польза компьютера для разных профессий. Почему компьютер важно защищать
19. Возьми с собой электронного помощника. Мобильные устройства
20. Общение в Интернете – переписка, форумы, социальные сети. Совместные игры в Интернете
21. Как отличать полезную и правдивую информацию
22. Как работать в группе. Как передать товарищам результаты работы и не повредить их компьютерам. Что такое электронная почта

**3 класс**

23. Сохранение полезной информации. Коллекция ссылок. Неосторожность пользователя – опасность для компьютера и данных
24. Можно ли «испортить» Интернет
25. Обмен данными при совместной работе – скайп, IP-телефония, ICQ. Безопасный обмен данными
26. Компьютер и умственный труд. Как «думает» компьютер и что этому может помешать
27. Почему компьютер нужно беречь
28. Польза Интернета и компьютера в сельском хозяйстве. Какой вред могут принести неисправности Интернета и компьютера и что может их вызвать
29. Компьютер и Интернет в промышленности – почему они нуждаются в защите

30. Как найти информацию о городах? Ненужные ссылки, ложные ссылки, реклама. Что такое вредоносные сайты
31. Как Интернет помогает путешествовать – покупка билетов в Интернете и возможные проблемы
32. Интернет в путешествиях – польза и опасности. Сколько стоит Интернет

**4 класс**

33. Как компьютер помогает науке и почему он нуждается в защите. Наука о защите компьютеров
34. Поиск информации в Интернете. Доступ к разрешенной информации – что это такое
35. Поиск в Интернете. Где Интернет хранит свои данные. Как сохранить в сети найденную информацию. Что такое облачные сервисы – безопасны ли они?
36. Поиск документов в сети – все ли найденные данные правдивы и полезны? Как защитить себя от информационной перегрузки
37. Поиск информации в сети: к чему ведет переход по вредоносным ссылкам. Опасная информация в сети
38. Виды Интернет-общения. Безопасно ли общение в Интернете?
39. Когда появились компьютер и Интернет. Как вместе с Интернетом появились его болезни
40. Что такое дистанционное обучение. Есть ли у него минусы?
41. Что такое компьютерная грамотность
42. Интернет, телефон и космос. Польза и опасности мобильной связи
43. День системного администратора и день программиста – что это за профессии? Что они делают для кибербезопасности?

**5 класс**

44. Как устроены компьютер и интернет
45. Что такое программное и аппаратное обеспечение
46. Какие программы должны быть установлены на компьютере
47. Компьютер и системы безопасности
48. Сетевые игры как массовые развлечения. Бесплатные и платные игры
49. Кибербезопасность – что это такое

**6 класс**

50. Как работают мобильные устройства. Угрозы для мобильных устройств
51. Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр)
52. Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации)
53. Кто обеспечивает защиту киберпространства
54. Что такое геоинформационные системы. Глобальные информационные Сети по стихийным бедствиям

**7 класс**

55. Информационная безопасность
56. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные
57. Источники данных в Интернете: почта, сервисы обмена файлами и др. Хранение данных в Интернете
58. Возможности и проблемы социальных сетей
59. Безопасный профиль в социальных сетях. Составление сети контактов

## 8 класс

60. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности
61. Компьютерная и информационная безопасность, обнаружение проблем в сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации
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
63. Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления
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»
65. Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации

66. Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты)
67. Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi
68. Угрозы информации (техногенные, случайные и преднамеренные; природные). Неосторожность пользователя как одна из угроз для информационной безопасности
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
70. Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности)

## 9 класс

71. Кибертерроризм и кибервойны
72. Кибератаки и техногенные катастрофы. Защита IT-инфраструктур критически важных объектов
73. Категории информационной безопасности
74. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение)
75. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности
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

77. Шифрование при передаче конфиденциальной информации. Что такое цифровая подпись
78. Регистрация и аудит в организации безопасности информации. Что такое политика безопасности
79. Риски интернета (контентные, электронные, коммуникационные, потребительские)
80. Безопасный серфинг
81. Безопасные ресурсы для поиска
82. Проблемы электронной торговли
83. Проблемные сайты
84. Ложные ресурсы сети

**10 класс**

85. Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях
86. Интернет как оружие массового поражения
87. Опасная информация в сети (порносайты, киберсекс, сайты азартных игр, сайты о наркотиках, экстремистские, сектантские, террористические и националистические)
88. Социальные последствия безответственного поведения в интернете
89. Угрозы для IOS-устройств. Угрозы для Android-устройств

**11 класс**

90. Проблемы безопасности информационных систем. Методы обеспечения защиты данных в СУБД
91. Защита государственных информационных систем
92. Проблемы безопасности банковских систем
93. Безопасность платежных систем

94. Безопасность геоинформационных систем
95. Безопасность систем бронирования билетов
96. Безопасность корпоративных баз данных
97. Безопасность медицинских информационных систем
98. Безопасность при удаленном доступе к ресурсам компьютера
99. Хакерские атаки. Как уронить сайт. Виды атак
100. Кибербезопасность и киберпространство. Киберкультура
101. Новые технологии и новые угрозы информационной безопасности (применение робототехники и т.п.). Рост числа угроз для мобильных устройств
102. Рост числа атак на инфраструктуру
103. Кибершпионаж
104. Кибероружие
105. Специальности, связанные с защитой киберпространства

## 2.2. Техника безопасности и экология

**2 класс**

1. Правила работы с ПК и электронными книгами
2. Компьютер и электронная книга – как защитить их от воды, жары и холода
3. Для компьютера тоже важен чистый воздух
4. Стоит ли размещать рядом компьютер и домашние растения
5. Компьютер и домашние животные, как защитить их друг от друга
6. Что такое мультимедиа, правила безопасной работы
7. Сканер и принтер – как с ними правильно обращаться
8. Сколько времени можно проводить за компьютером. Как правильно сидеть за компьютером
9. Как правильно включать и выключать компьютер. Как защитить компьютер от повреждений
10. Если компьютер сломался
11. Незнакомцы в Интернете. Странные звонки по мобильному телефону
12. Стоит ли в транспорте включать планшет или мобильные устройства
13. Везде ли есть Интернет? Может ли компьютер заменить компас. Как мобильные устройства помогают ориентироваться на местности

**3 класс**

14. Вредит ли компьютер экологии (излучения, волны)
15. Воздействие компьютера на зрение и др. органы
16. Гигиена при работе с компьютером
17. Как загрязняется компьютер. Гигиена компьютера
18. Стоит ли есть за компьютером
19. Компьютер и кровообращение
20. Польза и вред компьютерных игр. Компьютер и недостаток движения
21. Компьютер и ЗОЖ. Физическое и психическое здоровье
22. Что делать с компьютером в чрезвычайных ситуациях
23. Компьютер на улице и в общественном транспорте

24. Улица и мобильные устройства
25. Компьютер в грозу
26. Что происходит со сломанным компьютером?

**4 класс**

27. Электронная книга. Польза и вред
28. Превращение виртуальных знакомых в реальных

**5 класс**

29. Правила поведения в компьютерном классе
30. Интернет в системе безопасности. Как защитить сам Интернет
31. Техника безопасности при работе с компьютером. Источники питания компьютера
32. Что делать если вода попала в компьютер или ноутбук
33. Может ли загореться компьютер
34. Может ли вирус сломать компьютер? Чем тушить загоревшуюся выч. технику
35. Компьютер и мобильные устройства в чрезвычайных ситуациях
36. Компьютер и мобильные устройства в чрезвычайных ситуациях в метро
37. Компьютер и мобильные устройства в чрезвычайных ситуациях в авиатранспорте
38. Информационная перегрузка
39. Информация, вредная для здоровья
40. Медицинская информация в Интернете – всегда ли она полезна

**6 класс**

41. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности
42. Компьютеры и мобильные устройства в экстремальных условиях
43. Везде ли есть Интернет. ТБ при работе с мобильными устройствами

44. Первая помощь при проблемах в интернете (службы помощи)
45. Компьютер и зрение
46. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM)

**7 класс**

47. Комплекс упражнений при работе за компьютером
48. Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов

**8 класс**

49. Кибератаки на инфраструктуру
50. Компьютер в режиме труда и отдыха. Информационная перегрузка
51. Влияние компьютера на репродуктивную систему

**9 класс**

52. Инструкция по технике безопасности при работе на компьютере. Электропитание и подключение к Интернету
53. Комплексы упражнений для зрения при работе с ПК
54. Вредные факторы работы за компьютером и их последствия
55. Гигиена при работе с ПК

**10 класс**

56. ПК и ЗОЖ. Организация рабочего места

## 2.3. Проблемы Интернет-зависимости

**2 класс**

1. Общий компьютер – как его поделить? Почему родители проверяют, что ты делаешь в Интернете?

**3 класс**

2. Что такое Интернет-сообщество. Как не превратить свою жизнь в виртуальную

**4 класс**

3. Если слишком долго находиться в Интернете: что такое интернет-зависимость?
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?
5. Виртуальная личность – что это такое
6. Зависимость от Интернет-общения
7. Развлечения в Интернете. Игры полезные и вредные. Признаки игровой зависимости
8. Сетевые игры
9. Сайты знакомств

**5 класс**

10. ЗОЖ и компьютер. Виды зависимости. Как определить наличие зависимости
11. Деструктивная информация в Интернете – как ее избежать

**6 класс**

12. Виды Интернет-зависимости

**7 класс**

13. Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред
14. Киберкультура (массовая культура в сети) и личность

15. Психологическое воздействие информации на человека. Управление личностью через сеть

**8 класс**

16. Интернет- и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость
17. Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости)

**9 класс**

18. Интернет как наркотик

**10 класс**

19. Классификация интернет-зависимостей

### 2.4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы

**2 класс**

1. Что такое электронные деньги, как с ними правильно обращаться

**3 класс**

2. Движение в Интернете (серфинг). Знаки Интернета, рассказывающие об опасной информации

**4 класс**

3. Правильно ли работает компьютер? Признаки работы вирусов
4. Ищите в Интернете только то, что вам требуется. Как защититься от вредного контента. Что такое контент-фильтры

5. Поиск информации. Что такое поисковые серверы? Как с их помощью защитить себя от нежелательной информации
6. Поиск информации. Родительский контроль. Какие программы для этого существуют
7. Поиск информации. Обращайте внимание на предупреждения о вредоносном содержимом по найденной ссылке

**5 класс**

8. Вирусы человека и компьютера
9. Цели компьютерных вирусов
10. Лечение компьютера

**6 класс**

11. Как распространяются вирусы
12. Источники и причины заражения
13. Скорая компьютерная помощь. Признаки заражения компьютера
14. Что такое антивирусная защита. Как лечить компьютер
15. Защита мобильных устройств
16. Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные
17. Защита файлов. Что такое право доступа
18. Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети

**7 класс**

19. Защита файлов. Права пользователей
20. Защита при загрузке и выключении компьютера
21. Безопасность при скачивании файлов
22. Безопасность при просмотре фильмов онлайн

23. Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты
24. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.
25. Методы защиты фото и видеоматериалов от копирования в сети
26. Защита от копирования контента сайта
27. Как развивались вирусы
28. Могут ли вирусы воздействовать на аппаратуру ПК
29. Как вирусы воздействуют на файлы
30. Проверка на наличие вирусов. Сканеры и др.
31. Может ли вирус воздействовать на рабочий стол
32. Источники заражения ПК
33. Антивирусное ПО, виды и назначение
34. Методы защиты от вирусов. Как распознаются вирусы

**8 класс**

35. Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты
36. Проверка подлинности (аутентификация) в Интернете
37. Меры безопасности для пользователя WiFi. Настройка безопасности
38. Вирусы для мобильных устройств (мобильные банкеры и др.)
39. Настройка компьютера для безопасной работы
40. Ошибки пользователя (установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.)
41. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях

**9 класс**

42. Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей
43. Простые и динамически изменяющиеся пароли
44. Борьба с утечками информации. Средства контроля доступа
45. Права пользователей. Способы разграничения доступа
46. Средства защиты в сети: межсетевые экраны, криптомаршрутизаторы, серверы аутентификации и т.д. Обманные системы для защиты информации в сетях
47. Защита сайтов
48. Системы обнаружения атак. Безопасность хостинга
49. ТБ при работе с почтой
50. ТБ при загрузке файлов
51. Типы вирусов. Отличия вирусов и закладок
52. Антивирусные программы для ПК: сканеры, ревизоры и др. Выявление неизвестных вирусов

**10 класс**

53. Основные меры кибербезопасности. Безопасность приложений, серверов, конечных пользователей
54. Защита от атак, повышение готовности
55. Аппаратная защита ПО и сети (электронные ключи, аппаратные брандмауэры)
56. Защита ПК на этапе загрузки. Параметры безопасности ПК. Обновления
57. Защита файловой системы. Файловые таблицы. Права доступа
58. Резервное копирование и восстановление данных. Восстановление ОС. Аппаратные и программные средства
59. Чем отличаются методы защиты операционной системы, программного обеспечения и данных

60. Признаки заражения компьютерных программ. Где можно обнаружить подозрительные процессы
61. ОС и их возможности в борьбе с вирусами (Windows. Linux)
62. Разновидности вирусов. Черви, трояны, скрипты и др. Шпионские программы. Шифровальщики. Хакерские утилиты. Сетевые атаки
63. Защитное ПО. Антивирусные программы. Межсетевые экраны. Брандмауэры
64. Антивирусная защита ПК, сети и мобильных пользователей
65. Наиболее известные антивирусные программы. Kaspersky Internet Security. Dr.Web Security Space. ESET NOD32 Smart Security. Бесплатные программы-сканеры
66. Настройка антивирусного ПО
67. Коммерческое и бесплатное антивирусное ПО

**11 класс**

68. Как узнать местоположение компьютера по IP-адресу
69. 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.)
70. Настройки безопасности почтовых программ
71. Защита в поисковых системах (фильтры для ограничения потенциально опасного содержимого). Настройки безопасности веб-браузеров (Internet Explorer, Firefox и т.п.)
72. Электронная почта и системы мгновенного обмена сообщениями. Настройки безопасности Скайп, ICQ и пр.
73. Способы обеспечения безопасности веб-сайта

## 2.5. Мошеннические действия в Интернете. Киберпреступления

**3 класс**

1. Поиск информации. «Ненужные» ссылки и реклама
2. Интернет и экономика – польза и опасность. Кто и как может навредить в Интернете
3. Электронная торговля – ее опасности
4. Сколько стоят ошибки в Интернете

**4 класс**

5. Поиск информации: если у вас требуют личную информацию при скачивании данных. Что такое личная информация
6. Поиск в Интернете. Если вам сообщают о выигрыше в лотерею
7. Поиск в Интернете. Если вам предлагают установить новое приложение
8. Поиск в Интернете. Если вам предлагают бесплатные игры
9. Поиск информации. Если вам предлагают что-то купить

**5 класс**

10. Киберпреступления – что это такое
11. Виды интернет-мошенничества (письма, реклама, охота за личными данными и т.п.)
12. Виртуальные друзья – кто они

**6 класс**

13. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС
14. Прослушивание разговоров. Определение местоположения телефона

**7 класс**

15. Утечка и обнародование личных данных
16. Подбор и перехват паролей. Взломы аккаунтов в социальных сетях
17. Виды мошенничества в Интернете. Фишинг (фарминг)
18. Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею

**8 класс**

19. Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы
20. Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники
21. Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды
22. Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег
23. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса
24. Платные предложения работы. Платный просмотр видеоматериалов
25. Технологии манипулирования в Интернете

**9 класс**

26. ТБ при интернет-общении

**11 класс**

27. ТБ при регистрации на веб-сайтах. ТБ на сайтах знакомств
28. Компьютерное пиратство. Плагиат
29. Кибернаемники и кибердетективы
30. Оценка ущерба от киберпреступлений

## 2.6. Сетевой этикет. Психология и сеть

**2 класс**

1. Что такое интернет-этикет
2. Как вести себя «в гостях» у сетевых друзей

**3 класс**

3. Помогает ли компьютер стать лучше? Общение в социальных сетях
4. Этикет в Интернете при работе с проектом в группе

**5 класс**

5. Что такое нетикет и почему он появился
6. Правила общения в Интернете. Основы сетевого этикета
7. Переписка в сети. Этикет при переписке. Что такое спам
8. Правила поведения в скайпе
9. Что такое форум. Зачем существует модерация
10. Общение в сети и его последствия. Агрессия в сети
11. Психологическое влияние через Интернет
12. Как защитить себя в Интернете

**6 класс**

13. Что такое личные данные. Все, что выложено в Интернет, может стать известно всем
14. «Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам
15. Анонимность в сети
16. Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах
17. Как появился нетикет, что это такое. Общие правила сетевого этикета

18. Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений)
19. Этика дискуссий. Взаимное уважение при интернет-общении
20. Этикет и безопасность. Эмоции в сети, их выражение
21. Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться
22. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибермоббинг, троллинг, буллицид
23. Если вы стали жертвой компьютерной агрессии: службы помощи

**8 класс**

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.

**9 класс**

25. Примеры этических нарушений

**10 класс**

26. Значение сетевого этикета

## 2.7. Правовые аспекты защиты киберпространства

**6 класс**

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

**7 класс**

2. Защита прав потребителей при использовании услуг Интернет
3. Защита прав потребителей услуг провайдера

**8 класс**

4. Как расследуются преступления в сети
5. Ответственность за интернет-мошенничество

**9 класс**

6. Правовые акты в области информационных технологий и защиты киберпространства

**10 класс**

7. Ответственность за киберпреступления
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)
9. Информационное законодательство РФ. Закон РФ "Об информации, информационных технологиях и о защите информации"
10. Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ (ст. 237 УК РФ)
11. Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo)

**11 класс**

12. Правовые основы для защиты от спама
13. Правовые основы защиты интеллектуальной собственности. Авторское право. Правовая охрана программ для ЭВМ и БД
14. Лицензионное ПО. Виды лицензий (OEM, FPP, корпоративные лицензии, подписка). ПО с открытым кодом (GNU GPL, FreeBSD)

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.
16. Уголовный кодекс РФ, раздел «Преступления в сфере компьютерной информации»

## 2.8. Государственная политика в области кибербезопасности

**3 класс**

1. Как государство защищает киберпространство

**4 класс**

2. Войны нашего времени. Что такое кибервойна
3. Что такое информация. Право на информацию в Конституции
4. Почему государство защищает информацию
5. Защита государства и защита киберпространства

**9 класс**

6. Доктрина информационной безопасности

**10 класс**

7. Кибервойска
8. Защита киберпространства как одна из задач вооруженных сил
9. Информационная война. Информационное оружие
10. Патриотизм и интернет

**11 класс**

11. Информационная война. Информационное воздействие
12. Военная, государственная, коммерческая тайна. Защита сайтов государственных органов (электронное правительство)
13. Какие органы власти отвечают за защиту киберпространства

## 3. Соответствие содержания материала курса «Основы кибербезопасности» содержанию Стандарта основного общего образования по информатике[2]

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| **Общие сведения о безопасности ПК и Интернета** | | |
| 2 | Компьютер – как он появился, как появился Интернет | Основные этапы развития средств информационных технологий |
| 2 | Из чего сделан компьютер | |
| 2 | Как Интернет приходит в дом. Из чего «сделана» сеть | |
| 3 | Почему компьютер нужно беречь | |
| 3 | Компьютер и умственный труд. Как «думает» компьютер и что этому может помешать | |
| 4 | Когда появились компьютер и Интернет. Как вместе с Интернетом появились его болезни | |
| 2 | Интернет - средство для поиска полезной информации. Где и как искать информацию для урока. Что такое файл. Какие файлы можно скачивать, а какие нельзя | Локальные и глобальные компьютерные сети.<br>Поиск информации |
| 2 | Как найти и сохранить полезные рисунки и фотографии. | |
| 2 | Сколько информации можно скачать из Интернета? Лишняя информация на компьютере | |
| 2 | Как сохранить результаты своих наблюдений на школьном компьютере и не потерять их. Кому принадлежит файл | Информационные процессы: хранение, передача и обработка информации.<br>Особенности запоминания, обработки и передачи информации человеком. |
| 2 | Как обращаться со своими и чужими файлами, чтобы их не потерять. Как защищают файлы | Создание, именование, сохранение, удаление объектов, организация их семейств. Архивирование и разархивирование. |
| 2 | На каких устройствах можно сохранить информацию и как с ними правильно обращаться (диски, флэш, карты и пр.) | Запись средствами ИКТ информации об объектах и процессах окружающего мира (природных, культурно-исторических, школьной жизни, индивидуальной и семейной истории): |
| 2 | Как принести в класс фотографии и рисунки для урока и не повредить школьному компьютеру | |
| 2 | Цифровой фотоаппарат. Как с ним правильно обращаться и как переносить фотографии на компьютер | |

[2] Об утверждении федерального компонента государственных образовательных стандартов начального общего, основного общего и среднего (полного) общего образования. Приказ Министерства образования Российской Федерации №1089 от 5 марта 2004 года (с изменениями на 23 июня 2015 года)

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| | | - запись изображений и звука с использованием различных устройств (цифровых фотоаппаратов и микроскопов, видеокамер, сканеров, магнитофонов) |
| 2 | Возьми с собой электронного помощника. Мобильные устройства | Представления о средствах телекоммуникационных технологий: электронная почта, чат, телеконференции, форумы, телемосты, интернет-телефония |
| 3 | Обмен данными при совместной работе – скайп, IP-телефония, ICQ. Безопасный обмен данными | |
| 4 | Интернет, телефон и космос. Польза и опасности мобильной связи | |
| 2 | Как учиться в Интернете. Полезные и вредные страницы Интернета | Информационные ресурсы общества, образовательные информационные ресурсы. |
| 2 | Как отличать полезную и правдивую информацию | |
| 4 | Что такое дистанционное обучение. Есть ли у него минусы? | |
| 2 | Как работать в группе. Как передать товарищам результаты работы и не повредить их компьютерам. Что такое электронная почта | Средства и технологии обмена информацией с помощью компьютерных сетей (сетевые технологии) |
| 2 | Общение в Интернете – переписка, форумы, социальные сети. Совместные игры в Интернете | |
| 4 | Виды Интернет-общения. Безопасно ли общение в Интернете? | |
| 2 | Где узнать прогноз погоды в Интернете. Как найти в Интернете полезные страницы со звуковой информацией. Как не тратить лишнее время на поиск. Как научиться не отвлекаться на лишнюю информацию (2/20) | Использование инструментов поисковых систем (формирование запросов) для работы с образовательными порталами и электронными каталогами библиотек, музеев, книгоиздания, СМИ в рамках учебных заданий из различных предметных областей. |
| 2 | Как найти в Интернете полезный фильм и не повредить компьютеру. Как не тратить время на просмотр ненужных фильмов (2/15) | |
| 2 | Польза компьютера для разных профессий. Почему компьютер важно защищать | Профессии, связанные с построением математических и компьютерных моделей, программированием, обеспечением информационной деятельности индивидуумов и организаций. |
| 4 | Что такое компьютерная грамотность | |
| 4 | День системного администратора и день программиста – что это за профессии? Что они делают для кибербезопасности? | |
| 3 | Сколько стоит Интернет? Можно ли «испортить» Интернет | Стоимость информационных продуктов, услуг связи. |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 3 | Сохранение полезной информации. Коллекция ссылок. Неосторожность пользователя – опасность для компьютера и данных | Сохранение для индивидуального использования информационных объектов из компьютерных сетей (в том числе Интернета) и ссылок на них. |
| 2 | Как Интернет помогает транспорту. Что будет, если Интернет перестанет работать? Как компьютер управляет дорожным движением | Роль информации в современном обществе и его структурах: экономической, социальной, культурной, образовательной. |
| 3 | Компьютер и Интернет в промышленности – почему они нуждаются в защите. Польза Интернета и компьютера в сельском хозяйстве | |
| 3 | Интернет в путешествиях – польза и опасности. Покупка билетов в Интернете и возможные проблемы | |
| 4 | Как компьютер помогает науке и почему он нуждается в защите. Наука о защите компьютеров | |
| 4 | Поиск информации в Интернете. Доступ к разрешенной информации – что это такое | Локальные и глобальные компьютерные сети.<br>Поисковые информационные системы. Организация поиска информации. Защита информации |
| 4 | Поиск информации в сети: к чему ведет переход по вредоносным ссылкам. Опасная информация в сети | |
| 3 | Ненужные ссылки, ложные ссылки, реклама. Что такое вредоносные сайты | |
| 4 | Поиск в Интернете. Где Интернет хранит свои данные. Как сохранить в сети найденную информацию. Что такое облачные сервисы – безопасны ли они? | |
| 4 | Поиск документов в сети – все ли найденные данные правдивы и полезны? Как защитить себя от информационной перегрузки | |
| 5 | Сетевые игры как массовые развлечения. Бесплатные и платные игры | |
| 9 | Риски интернета (контентные, электронные, коммуникационные, потребительские) | |
| 9 | Безопасный серфинг | |
| 9 | Безопасные ресурсы для поиска | |
| 9 | Проблемы электронной торговли | |
| 9 | Проблемные сайты | |
| 9 | Ложные ресурсы сети | |
| 10 | Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях | |
| 10 | Интернет как оружие массового поражения | |
| 3 | Какой вред могут принести неисправности Интернета и компьютера и что может их вызвать | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 5 | Как устроены компьютер и интернет. Кибербезопасность – что это такое | Аппаратные и программные средства организации компьютерных сетей. |
| 5 | Что такое программное и аппаратное обеспечение. Какие программы должны быть установлены на компьютере | Программное обеспечение, его структура. Программное обеспечение общего назначения. |
| 7 | Возможности и проблемы социальных сетей | Организация личной информационной среды. Защита информации. |
| 7 | Безопасный профиль в социальных сетях. Составление сети контактов | |
| 7 | Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные | |
| 8 | Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности | Телекоммуникационные технологии. Использование средств телекоммуникаций в коллективной деятельности. Технологии и средства защиты информации в глобальной и локальной компьютерных сетях от разрушения, несанкционированного доступа. |
| 8 | Компьютерная и информационная безопасность, обнаружение проблем в сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации | |
| 8 | Угрозы информации (техногенные, случайные и преднамеренные; природные) Неосторожность пользователя как одна из угроз для информационной безопасности | |
| 8 | 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 | Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления | |
| 8 | 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 | Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 8 | Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты) | |
| 8 | Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi | |
| 8 | 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 | Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности) | |
| 6 | Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации) | Защита информации |
| 6 | Как работают мобильные устройства. Угрозы для мобильных устройств | |
| 6 | Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр) | |
| 7 | Информационная безопасность | |
| 7 | Источники данных в Интернете: почта, сервисы обмена файлами и др. Хранение данных в Интернете | |
| 9 | Категории информационной безопасности | |
| 9 | Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение) | |
| 9 | Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности | |
| 9 | 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 | Шифрование при передаче конфиденциальной информации. Что такое цифровая подпись | |
| 9 | Регистрация и аудит в организации безопасности информации. Что такое политика безопасности | |
| 9 | Кибертерроризм и кибервойны | |
| 9 | Кибератаки и техногенные катастрофы. Защита IT-инфраструктур критически важных объектов | |
| 10 | Социальные последствия безответственного поведения в интернете | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| | Опасная информация в сети (порносайты, киберсекс, сайты азартных игр, сайты о наркотиках, экстремистские, сектантские, террористические и националистические) | |
| 10 | Угрозы для IOS-устройств. Угрозы для Android-устройств | |
| 11 | Проблемы безопасности информационных систем. Методы обеспечения защиты данных в СУБД | Организация информации в среде коллективного использования информационных ресурсов. Представление о системах управления базами данных, поисковых системах в компьютерных сетях, библиотечных информационных системах. Компьютерные архивы информации: электронные каталоги, базы данных. Организация баз данных. Примеры баз данных: юридические, библиотечные, здравоохранения, налоговые, социальные, кадровые. |
| 11 | Защита государственных информационных систем | |
| 11 | Проблемы безопасности банковских систем | |
| 11 | Безопасность платежных систем | |
| 11 | Безопасность геоинформационных систем | |
| 11 | Безопасность систем бронирования билетов | |
| 11 | Безопасность корпоративных баз данных | |
| 11 | Безопасность медицинских информационных систем | |
| 11 | Безопасность при удаленном доступе к ресурсам компьютера | |
| 11 | Хакерские атаки. Как уронить сайт. Виды атак | |
| 11 | Кибербезопасность и киберпространство. Киберкультура | |
| 11 | Новые технологии и новые угрозы информационной безопасности (применение робототехники и т.п.). Рост числа угроз для мобильных устройств | |
| 11 | Рост числа атак на инфраструктуру | |
| 11 | Кибершпионаж. Кибероружие | |
| 11 | Специальности, связанные с защитой киберпространства | |
| **Техника безопасности и экология** | | |
| 2 | Компьютер и электронная книга – как защитить их от воды, жары и холода. Правила работы с ПК и электронными книгами | Средства ИКТ Безопасность, гигиена, эргономика, ресурсосбережение, технологические требования при эксплуатации компьютерного рабочего места. Типичные неисправности и трудности в использовании ИКТ. Комплектация компьютерного рабочего места в соответствии с целями его использования. |
| 2 | Если компьютер сломался | |
| 2 | Что такое мультимедиа. Сканер и принтер – как с ними правильно обращаться | |
| 2 | Компьютер и домашние животные, как защитить их друг от друга. Стоит ли размещать рядом компьютер и домашние растения. Для компьютера тоже важен чистый воздух | |
| 2 | Как правильно включать и выключать компьютер. Как защитить компьютер от повреждений | |
| 2 | Стоит ли в транспорте включать планшет или мобильные устройства | |
| 3 | Как загрязняется компьютер. Гигиена компьютера | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 3 | Вредит ли компьютер экологии (излучения, волны) | Основные устройства ИКТ. Соединение блоков и устройств компьютера, других средств ИКТ, простейшие операции по управлению (включение и выключение, понимание сигналов о готовности и неполадке и т.д.), использование различных носителей информации, расходных материалов. Гигиенические, эргономические и технические условия безопасной эксплуатации средств ИКТ.<br>Метапредметные связи:<br>ОБЖ. Основные правила пользования бытовыми приборами и инструментами, средствами бытовой химии, персональными компьютерами и др.<br>Природоведение. Здоровье человека и безопасность жизни |
| 3 | Что происходит со сломанным компьютером? | |
| 5 | Правила поведения в компьютерном классе | |
| 5 | Интернет в системе безопасности. Как защитить сам Интернет | |
| 5 | Техника безопасности при работе с компьютером. Источники питания компьютера | |
| 5 | Что делать если вода попала в компьютер или ноутбук | |
| 5 | Может ли загореться компьютер | |
| 5 | Может ли вирус сломать компьютер? Чем тушить загоревшуюся выч. технику | |
| 2 | Везде ли есть Интернет? Может ли компьютер заменить компас. Как мобильные устройства помогают ориентироваться на местности | Метапредметные связи:<br>ОБЖ. Безопасное поведение человека в природных условиях: ориентирование на местности, подача сигналов бедствия, добывание огня, воды и пищи, сооружение временного укрытия.<br>Ситуации криминогенного характера, меры предосторожности и правила поведения. Элементарные способы самозащиты.<br>Природоведение. Здоровье человека и безопасность жизни |
| 2 | Незнакомцы в Интернете. Странные звонки по мобильному телефону | |
| 3 | Что делать с компьютером в чрезвычайных ситуациях | |
| 5 | Компьютер и мобильные устройства в чрезвычайных ситуациях | |
| 5 | Компьютер и мобильные устройства в чрезвычайных ситуациях в метро | |
| 5 | Компьютер и мобильные устройства в чрезвычайных ситуациях в авиатранспорте | |
| 6 | Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности | |
| 6 | Компьютеры и мобильные устройства в экстремальных условиях | |
| 6 | Что такое геоинформационные системы. Глобальные информационные Сети по стихийным бедствиям | |
| 6 | Везде ли есть Интернет. ТБ при работе с мобильными устройствами | |
| 6 | Первая помощь при проблемах в интернете (службы помощи) | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 6 | Кибератаки на инфраструктуру | |
| 2 | Сколько времени можно проводить за компьютером. Как правильно сидеть за компьютером | Основы безопасности жизнедеятельности Здоровый образ жизни. Факторы, укрепляющие и разрушающие здоровье. Вредные привычки и их профилактика. Метапредметные связи: Природоведение. Здоровье человека и безопасность жизни |
| 3 | Польза и вред компьютерных игр. Компьютер и недостаток движения | |
| 3 | Воздействие компьютера на зрение и др. органы. Гигиена при работе с компьютером. Стоит ли есть за компьютером. Компьютер и осанка. Компьютер и кровообращение | |
| 3 | Компьютер и ЗОЖ. Физическое и психическое здоровье | |
| 3 | Компьютер на улице и в общественном транспорте | |
| 3 | Улица и мобильные устройства | |
| 3 | Компьютер в грозу | |
| 4 | Электронная книга. Польза и вред | |
| 4 | Превращение виртуальных знакомых в реальных | |
| 5 | Информационная перегрузка | |
| 5 | Информация, вредная для здоровья | |
| 5 | Медицинская информация в Интернете – всегда ли она полезна | |
| 6 | Компьютер и зрение | |
| 6 | Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM) | |
| 7 | Комплекс упражнений при работе за компьютером | |
| 7 | Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов | |
| 8 | Компьютер в режиме труда и отдыха. Информационная перегрузка | |
| 8 | Влияние компьютера на репродуктивную систему | |
| 9 | Инструкция по технике безопасности при работе на компьютере. Электропитание и подключение к Интернету | |
| 0 | Комплексы упражнений для зрения при работе с ПК | |
| 9 | Вредные факторы работы за компьютером и их последствия | |
| 9 | Гигиена при работе с ПК | |
| 10 | ПК и ЗОЖ. Организация рабочего места | |
| **Проблемы Интернет-зависимости** | | |
| 2 | Общий компьютер – как его поделить? Почему родители проверяют, что ты делаешь в Интернете? | Основы социальной информатики. Этические и правовые нормы информационной деятельности человека |
| 3 | Что такое Интернет-сообщество. Как не превратить свою жизнь в виртуальную | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 4 | Если слишком долго находиться в Интернете: что такое интернет-зависимость? | Метапредметные связи: Основы безопасности жизнедеятельности. Здоровый образ жизни. Факторы, укрепляющие и разрушающие здоровье. Вредные привычки и их профилактика |
| 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 | Виртуальная личность – что это такое | |
| 4 | Зависимость от Интернет-общения | |
| 4 | Развлечения в Интернете. Игры полезные и вредные. Признаки игровой зависимости | |
| 4 | Сетевые игры | |
| 4 | Сайты знакомств | |
| 5 | ЗОЖ и компьютер. Виды зависимости. Как определить наличие зависимости | |
| 5 | Деструктивная информация в Интернете – как ее избежать | |
| 6 | Виды Интернет-зависимости | |
| 7 | Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред | |
| 7 | Киберкультура (массовая культура в сети) и личность | |
| 7 | Психологическое воздействие информации на человека. Управление личностью через сеть | |
| 8 | Интернет- и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость | |
| 8 | Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости) | |
| 9 | Интернет как наркотик | |
| 10 | Классификация интернет-зависимостей | |
| **Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы** | | |
| 3 | Движение в Интернете (серфинг). Знаки Интернета, рассказывающие об опасной информации | Локальные и глобальные компьютерные сети. Поисковые информационные системы. Организация поиска информации. |
| 4 | Ищите в Интернете только то, что вам требуется. Как защититься от вредного контента. Что такое контент-фильтры | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 4 | Поиск информации. Что такое поисковые серверы? Как с их помощью защитить себя от нежелательной информации | |
| 4 | Поиск информации. Родительский контроль. Какие программы для этого существуют | |
| 4 | Поиск информации. Обращайте внимание на предупреждения о вредоносном содержимом по найденной ссылке | |
| 6 | Защита мобильных устройств | |
| 6 | Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети | |
| 7 | Методы защиты фото и видеоматериалов от копирования в сети | |
| 7 | Защита от копирования контента сайта | |
| 8 | Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты | |
| 8 | Проверка подлинности (аутентификация) в Интернете | |
| 8 | Меры безопасности для пользователя WiFi. Настройка безопасности | |
| 9 | Средства защиты в сети: межсетевые экраны, криптомаршрутизаторы, серверы аутентификации и т.д. Обманные системы для защиты информации в сетях | |
| 9 | Защита сайтов | |
| 9 | Системы обнаружения атак. Безопасность хостинга | |
| 9 | ТБ при загрузке файлов | |
| 10 | Основные меры кибербезопасности. Безопасность приложений, серверов, конечных пользователей | |
| 10 | Защита от атак, повышение готовности | |
| 10 | Аппаратная защита ПО и сети (электронные ключи, аппаратные брандмауэры) | |
| 11 | Способы обеспечения безопасности веб-сайта | |
| 6 | Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные | Защита информации. Технологии и средства защиты информации в глобальной и локальной компьютерных сетях от разрушения, несанкционированного доступа. |
| 6 | Защита файлов. Что такое право доступа | |
| 7 | Защита файлов. Права пользователей | |
| 7 | Защита при загрузке и выключении компьютера | |
| 7 | Безопасность при скачивании файлов | |
| 7 | Безопасность при просмотре фильмов онлайн | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 7 | Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты | |
| 7 | Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы. | |
| 11 | Как узнать местоположение компьютера по IP-адресу | |
| 11 | Защита в поисковых системах (фильтры для ограничения потенциально опасного содержимого). Настройки безопасности веб-браузеров (Internet Explorer, Firefox и т.п.) | |
| 8 | Настройка компьютера для безопасной работы | Программные средства создания информационных объектов, организация личного информационного пространства, защиты информации. |
| 8 | Ошибки пользователя (установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.) | |
| 8 | Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях | |
| 9 | Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей | |
| 9 | Простые и динамически изменяющиеся пароли | |
| 9 | Борьба с утечками информации. Средства контроля доступа | |
| 9 | Права пользователей. Способы разграничения доступа | |
| 10 | Защита ПК на этапе загрузки. Параметры безопасности ПК. Обновления | |
| 10 | Защита файловой системы. Файловые таблицы. Права доступа | |
| 10 | Резервное копирование и восстановление данных. Восстановление ОС. Аппаратные и программные средства | |
| 10 | Чем отличаются методы защиты операционной системы, программного обеспечения и данных | |
| 9 | ТБ при работе с почтой | Электронная почта как средство связи; правила переписки, приложения к письмам, отправка и получение сообщения. |
| 11 | 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 | Настройки безопасности почтовых программ | |
| 11 | Электронная почта и системы мгновенного обмена сообщениями. Настройки безопасности Скайп, ICQ и пр. | |
| 4 | Правильно ли работает компьютер? Признаки работы вирусов | Защита информации от компьютерных вирусов |
| 5 | Вирусы человека и компьютера | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 5 | Цели компьютерных вирусов | |
| 5 | Лечение компьютера | |
| 6 | Как распространяются вирусы | |
| 6 | Источники и причины заражения | |
| 6 | Скорая компьютерная помощь. Признаки заражения компьютера | |
| 6 | Что такое антивирусная защита. Как лечить компьютер | |
| 7 | Как развивались вирусы | |
| 7 | Могут ли вирусы воздействовать на аппаратуру ПК | |
| 7 | Как вирусы воздействуют на файлы Проверка на наличие вирусов. Сканеры и др. | |
| 7 | Может ли вирус воздействовать на рабочий стол | |
| 7 | Источники заражения ПК | |
| 7 | Антивирусное ПО, виды и назначение | |
| 7 | Методы защиты от вирусов. Как распознаются вирусы | |
| 8 | Вирусы для мобильных устройств (мобильные банкеры и др.) | |
| 9 | Типы вирусов. Отличия вирусов и закладок | |
| 10 | Признаки заражения компьютерных программ. Где можно обнаружить подозрительные процессы | |
| 10 | ОС и их возможности в борьбе с вирусами (Windows. Linux) | |
| 10 | Разновидности вирусов. Черви, трояны, скрипты и др. Шпионские программы. Шифровальщики. Хакерские утилиты. Сетевые атаки | |
| 10 | Антивирусная защита ПК, сети и мобильных пользователей | |
| 9 | Антивирусные программы для ПК: сканеры, ревизоры и др. Выявление неизвестных вирусов | Виды программного обеспечения |
| 10 | Защитное ПО. Антивирусные программы. Межсетевые экраны. Брандмауэры (10)<br>Наиболее известные антивирусные программы. Kaspersky Internet Security. Dr.Web Security Space. ESET NOD32 Smart Security. Бесплатные программы-сканеры | |
| 10 | Настройка антивирусного ПО<br>Коммерческое и бесплатное антивирусное ПО | Правила подписки на антивирусные программы и их настройка на автоматическую проверку сообщений. |
| **Мошеннические действия в Интернете. Киберпреступления** | | |
| 2 | Что такое электронные деньги, как с ними правильно обращаться (2/15) | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 3 | Поиск информации. «Ненужные» ссылки и реклама | Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предотвращения. |
| 3 | Интернет и экономика – польза и опасность. Кто и как может навредить в Интернете | |
| 3 | Электронная торговля – ее опасности | |
| 3 | Сколько стоят ошибки в Интернете | |
| 4 | Поиск в Интернете. Если вам сообщают о выигрыше в лотерею | |
| 4 | Поиск в Интернете. Если вам предлагают установить новое приложение | |
| 4 | Поиск в Интернете. Если вам предлагают бесплатные игры | |
| 4 | Поиск информации. Если вам предлагают что-то купить | |
| 5 | Киберпреступления – что это такое | |
| 5 | Виртуальные друзья – кто они | |
| 6 | Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические SMS | |
| 6 | Прослушивание разговоров. Определение местоположения телефона | |
| 7 | Виды мошенничества в Интернете. Фишинг (фарминг) | |
| 7 | Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею | |
| 8 | Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы | |
| 8 | Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники | |
| 8 | Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды | |
| | Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег | |
| 8 | Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса | |
| 8 | Платные предложения работы. Платный просмотр видеоматериалов | |
| 8 | Технологии манипулирования в Интернете | |
| 9 | ТБ при интернет-общении | |
| 11 | ТБ при регистрации на веб-сайтах. ТБ на сайтах знакомств | |
| 11 | Компьютерное пиратство. Плагиат | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 11 | Кибернаемники и кибердетективы | |
| 11 | Оценка ущерба от киберпреступлений | |
| 4 | Поиск информации: если у вас требуют личную информацию при скачивании данных. Что такое личная информация | Личная информация, информационная безопасность, информационные этика и право |
| 5 | Виды интернет-мошенничества (письма, реклама, охота за личными данными и т.п.) | |
| 7 | Утечка и обнародование личных данных | |
| 7 | Подбор и перехват паролей. Взломы аккаунтов в социальных сетях | |
| **Сетевой этикет. Психология и сеть** | | |
| 2 | Что такое интернет-этикет | Основы социальной информатики<br>Этические и правовые нормы информационной деятельности человека.<br>Информационная этика и право, информационная безопасность. Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предотвращения. |
| 2 | Как вести себя «в гостях» у сетевых друзей | |
| 3 | Помогает ли компьютер стать лучше? Общение в социальных сетях | |
| 3 | Этикет в Интернете при работе с проектом в группе | |
| 5 | Что такое нетикет и почему он появился | |
| 5 | Правила общения в Интернете. Основы сетевого этикета | |
| 5 | Переписка в сети. Этикет при переписке. Что такое спам | |
| 5 | Правила поведения в скайпе | |
| 5 | Что такое форум. Зачем существует модерация | |
| 5 | Общение в сети и его последствия. Агрессия в сети | |
| 5 | Психологическое влияние через Интернет | |
| 5 | Как защитить себя в Интернете | |
| 6 | Что такое личные данные. Все, что выложено в Интернет, может стать известно всем | |
| 6 | «Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам | |
| 6 | Анонимность в сети | |
| 6 | Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах | |
| 6 | Как появился нетикет, что это такое. Общие правила сетевого этикета | |
| 6 | Этика дискуссий. Взаимное уважение при интернет-общении | |
| 6 | Этикет и безопасность. Эмоции в сети, их выражение | |
| 6 | Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 6 | Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибермоббинг, троллинг, буллицид | |
| 6 | Если вы стали жертвой компьютерной агрессии: службы помощи | |
| 9 | Примеры этических нарушений | |
| 10 | Значение сетевого этикета | |
| 6 | Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений) | Примеры организации коллективного взаимодействия: форум, телеконференция, чат. |
| 8 | 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. | |
| | **Правовые аспекты защиты** киберпространства | |
| 6 | Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация | Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предотвращения<br>Метапредметные связи:<br>Обществознание. Правовое регулирование общественных отношений |
| 7 | Защита прав потребителей при использовании услуг Интернет | |
| 7 | Защита прав потребителей услуг провайдера | |
| 8 | Как расследуются преступления в сети | |
| 8 | Ответственность за интернет-мошенничество | |
| 9 | Правовые акты в области информационных технологий и защиты киберпространства | |
| 10 | Ответственность за киберпреступления | |
| 10 | 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 | Информационное законодательство РФ. Закон РФ "Об информации, информационных технологиях и о защите информации" | |
| 10 | Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ (ст. 237 УК РФ) | |
| 10 | Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo) | |
| 11 | Правовые основы для защиты от спама | |

| Класс | Темы курса «Основы кибербезопасности» | Обязательный минимум содержания образовательных программ |
|---|---|---|
| 11 | Правовые основы защиты интеллектуальной собственности. Авторское право. Правовая охрана программ для ЭВМ и БД | |
| 11 | Лицензионное ПО. Виды лицензий (OEM, FPP, корпоративные лицензии, подписка). ПО с открытым кодом (GNU GPL, FreeBSD) | |
| 11 | 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 | Уголовный кодекс РФ, раздел «Преступления в сфере компьютерной информации» | |
| **Государственная политика в области кибербезопасности** | | |
| 3 | Как государство защищает информацию | Информационные ресурсы и каналы государства, общества, организации, их структура.<br>Защита информации |
| 4 | Войны нашего времени. Что такое кибервойна | |
| 4 | Что такое информация. Право на информацию в Конституции | |
| 4 | Почему государство защищает информацию | |
| 4 | Защита государства и защита киберпространства | |
| 9 | Доктрина информационной безопасности | |
| 10 | Кибервойска | |
| 10 | Защита киберпространства как одна из задач вооруженных сил | |
| 10 | Информационная война. Информационное оружие | |
| 10 | Патриотизм и интернет | |
| 11 | Информационная война. Информационное воздействие. Военная, государственная, коммерческая тайна. Защита сайтов государственных органов (электронное правительство) | |
| 11 | Какие органы власти отвечают за защиту киберпространства | |

## 4. Примеры уроков по курсу «Основы кибербезопасности»

### 4.1. 2 класс. Как принести в класс фотографии и рисунки для урока и не повредить школьному компьютеру?

**Окружающий мир**: «Какие бывают растения»

**Характеристика деятельности учащихся**: Понимать учебную задачу урока и стараться её выполнить; устанавливать по схеме различия между группами растений; работать в паре: называть и классифицировать растения, осуществлять самопроверку; приводить примеры деревьев, кустарников, трав своего края; определять растения с помощью атласа – определителя; оценивать эстетическое воздействие растений на человека; работать со взрослыми: наблюдать и готовить рассказ (фоторассказ) о красоте растений; формулировать выводы из изученного материала, отвечать на итоговые вопросы и оценивать свои достижения на уроке.

На этапе представления учащимися подготовленных с помощью старших фотографий (в соответствии с домашним заданием) предлагается тема из модуля «Общие сведения о безопасности ПК и Интернета».

**Цель**: знакомство с правилами обращения с устройствами внешней памяти.

**Задачи:**

**образовательные:**

познакомить с приемами и копирования файлов на различные устройства и основными способами проверки внешних устройств на наличие вирусов

**развивающие:**

способствовать формированию информационной культуры учащихся

**воспитательные:**

воспитывать ответственное отношение к работе с ПК.

*Знания:*

основные приемы работы с компьютером

основные правила работы с носителями информации

*Умения:*

выполнять основные действия с файлами

*Навыки:*

копирование файлов

проверка файлов на вирусы

**Методы и формы обучения:** словесный (рассказ), наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

**Используемая литература и web-ресурсы**:


1. Полежаева О.А. Методическое пособие для учителей. Информатика. УМК для начальной школы. 2-4 классы. – М.: БИНОМ. Лаборатория знаний, 2013. – 136 с.: ил.
2. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/__12697.pdf


**Этапы урока:**

1) Постановка цели урока (1 мин).

2) Актуализация знаний (2 мин).

3) Изучение нового материала и практическая работа (5 мин).

Подключение устройства памяти к компьютеру.

Запуск антивируса для проверки устройства.

4) Закрепление изученного материала (2 мин).

**Технические средства:**

Компьютеры и различные устройства для хранения информации.

**Ход урока**

1) **Постановка цели урока**.

**Деятельность учителя**: Вы уже учились находить в Интернете нужную информацию и сохранять ее на компьютере. Вы знаете, что такое файл и что с ним можно делать. Но что делать, если нужно перенести файл с одного компьютера на другой? Для этого есть много способов. Рассмотрим один из них.

Давайте вспомним, что такое файл и где он находится.

**Деятельность учащихся**: файл – это часть информации, хранящейся на диске компьютера или не другом устройстве. В файле может содержаться текст, рисунок, музыка, фильм и многое другое. Каждый файл имеет собственное имя, по которому его можно найти. Информацию, найденную в сети, можно сохранить в виде файла на диске.

2) **Изучение нового материала**

**Деятельность учителя**: Посмотрите, сколько существует разных устройств, на которых записаны файлы (следует демонстрация дискеты, флеш-накопителя, CD-диска, фотоаппарата, смартфона). Покажите, на каких устройствах сохранили файлы вы.

Вы видите, как эти устройства отличаются друг от друга. Но есть у них и общее – чтобы узнать, что на них хранится, их нужно подключить к компьютеру.

Для каждого из устройств есть свой способ подключения к компьютеру (далее рассказ сопровождается демонстрацией). Дискета вставляется в специальный дисковод для гибких дисков. Правда, на дискету можно записать совсем немного информации. Оптический диск позволяет сохранить в сотни раз больше информации, чем дискета. Для CD и DVD тоже существует свой дисковод. Flash-накопители несмотря на свои маленькие размеры могут хранить в десятки раз больше информации, чем оптический диск. Подключаются они через специальные USB-разъемы. Обратите внимание, что такое устройство должно вставляться аккуратно и правильно – если вставить флеш-накопитель не удается, то скорее всего его просто неправильно повернули. Но не только флеш-накопитель нужно вставлять правильно – это касается всех устройств. При неправильном обращении можно повредить и устройство памяти и компьютер. Также нужно

уметь правильно извлекать устройство из компьютера. Файлы можно хранить и на других устройствах. Например, есть память у цифрового фотоаппарата. Его тоже можно подключить к компьютеру через разъем USB, но с помощью специального кабеля (или переходного устройства), который позволяет соединить разъем USB компьютера и разъем Micro-USB фотоаппарата. Таким же способом можно подключить к компьютеру смартфон или плеер. Некоторые устройства подключаются через разъем Mini USB, похожий на Micro-USB, но несколько большего размера. Например, такие разъемы бывают на переносных жестких дисках (винчестерах). Бывают и другие виды разъемов. Кабель для подключения к компьютеру должен всегда храниться вместе с таким устройством памяти и подключать каждое устройство нужно через собственный кабель или точно такой же.

Через кардридер можно подключать к компьютеру карты памяти (флеш-карты). Карты памяти используются в цифровых фотоаппаратах, сотовых телефонах, ноутбуках, цифровых аудиопроигрывателях.

Можно подключаться к компьютеру и вовсе без проводов. Для этого в составе компьютера должно быть устройство bluetooth-адаптер, а сам компьютер должен находиться от вашего устройства хранения данных на дальше чем на 10-100 м. Так можно подключить к компьютеру сотовый телефон. Через bluetooth информацией могут обмениваться, например, два телефона, компьютер и принтер и т.д.

Как видите, файлы можно сохранять на многих устройствах. И если правильно подключить устройство памяти, то список хранящихся на нем файлов можно увидеть в Проводнике и скопировать их на жесткий диск (или записать на них файлы с жесткого диска компьютера на устройство).

Но знает ли кто-нибудь, что такое вирусы?

**Деятельность учащихся**: найти ответ в процессе обсуждения.

**Деятельность учителя**: Вирус – это программа, которую вы скорее всего даже и не обнаружите на своем устройстве. Но она может причинить компьютеру

не меньший вред, чем человеку – вирус серьезной болезни. В самых плохих случаях вы можете потерять всю информацию с вашего компьютера. Вирус передается от одного компьютера другому разными путями, и очень часто – через устройства памяти, которые уже подключались к зараженному компьютеру. Чтобы не заразить компьютер, всегда проверяйте подключаемое устройство с помощью специальной программы – антивирус.

Сейчас вы подключите к компьютеру ваш съемный накопитель. Если сразу не получается, проверьте, все ли правильно вы делаете. После подключения не спешите открывать устройство в проводнике, сначала запустим антивирус. Для этого найдем в «Мой компьютер» имя нашего устройства.

**Деятельность учащихся**: подключение флеш-памяти или др. устройства, запуск «Мой компьютер».

**Деятельность учителя**: сейчас вы щелкнете правой кнопки мыши на значке устройства памяти и выберете в меню пункт «Проверить на вирусы». Если вирус обнаружен, программа-антивирус сообщит об этом.

**Деятельность учащихся**: запуск проверки устройства.

**Деятельность учителя**: сейчас вы скопируете с рабочего стола на свое устройство памяти файл «Правила работы с устройствами хранения информации». Сделать это можно несколькими способами. Пока рассмотрим копирование через контекстное меню и команду «Отправить». Дома откройте этот файл и прочитайте.

**Деятельность учащихся**: копирование файла на устройство.

**Деятельность учителя**: сейчас вы скопируете файл с вашего устройства в папку «Мои документы». Для этого найдите в «Мой компьютер» значок вашего устройства и откройте его левой кнопкой мыши. Выберите файл и вызовите правой кнопкой контекстное меню. Найдите пункт «Отправить». Укажите куда скопировать файл («Мои документы»).

Запомните правила переноса файлов на компьютер:

1) правильно подключайте устройство к компьютеру

2) никогда не открывайте файлы и не копируйте их без проверки антивирусом

3) всегда помните, как запускается программа-антивирус

**Деятельность учащихся**: копирование файла на компьютер.

**Деятельность учителя**: а теперь откройте ваш файл с изображением растений и продолжим беседу о них.

### 4.2. 3 класс. Как загрязняется компьютер. Гигиена компьютера

**Окружающий мир**: «Надёжная защита организма»

**Характеристика деятельности учащихся**: Понимать учебную задачу урока и стремиться её выполнить. В процессе изучения темы используется презентация «Кожа – надежная защита организма».

После показа презентации можно перейти к теме о гигиене компьютера.

**Цель**: знакомство с правилами эксплуатации ПК.

**Задачи:**

**образовательные:**

познакомить с навыками ухода за персональным компьютером

**развивающие:**

способствовать формированию информационной культуры учащихся

**воспитательные:**

воспитывать дисциплинированность при работе с ПК.

*Знания:*

основные приемы работы с компьютером;

опасности при работе с электрическими приборами.

*Умения:*

основные приемы навигации по файловой системе;

основные приемы поиска информации в сети Интернет.

*Навыки:*

поиск и просмотр файлов.

**Тип урока**: урок изучения нового материала.

**Методы и формы обучения:** словесный (рассказ), видеометод, наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

**Используемая литература и web-ресурсы**:


1. Полежаева О.А. Методическое пособие для учителей. Информатика. УМК для начальной школы. 2-4 классы. – М.: БИНОМ. Лаборатория знаний, 2013. – 136 с.: ил.
2. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/__12697.pdf


**Этапы урока:**

1) Постановка цели урока (1 мин).

2) Актуализация знаний (2 мин).

2) Изучение нового материала (5 мин).

Объяснение нового материала.

Просмотр презентации.

4) Закрепление изученного материала (2 мин).

**Технические средства:** проектор, компьютеры.

**Ход урока**

1) **Постановка цели урока**.

**Деятельность учителя**: Мы с вами узнали о значении кожи для человеческого организма, узнали о том, как кожа защищает нас, как она помогает нам

дышать, регулировать наша температуру. В этом нам как всегда помог компьютер. Компьютер очень помогает нам – в учебе и в отдыхе. А правильно ли мы обращаемся с компьютером?

Давайте сначала вспомним, как работать за компьютером, чтобы не повредить своему здоровью (опрос по материалам 2 класса).

**Деятельность учащихся**: за компьютером нельзя проводить больше 15 минут подряд, нужно сидеть прямо, чтобы не искривить позвоночник, нельзя сидеть слишком близко к экрану, не сидеть за компьютером перед сном, со всеми вопросами сразу обращаться к взрослым и т.п.

3) **Изучение нового материала**

**Деятельность учителя**: вы помните, как беречь свое здоровье. А кто позаботится о здоровье компьютера? У него ведь тоже есть свои «органы», даже своя «кожа». Мы знаем о том, что за своей кожей нужно следить, содержать ее в чистоте. А как обращаться с компьютером, чтобы его «организм» не заболел? Здоровье компьютера зависит от двух главных вещей. Первое – это порядок в программах и в той информации, которая на компьютере хранится. Об этом мы с вами постоянно говорим на наших кибер-разминках. Второе – это порядок и чистота внутри и снаружи компьютера.

**Деятельность учащихся**: просмотр презентации «Что у компьютера внутри» (см. рис. 1).

**Деятельность учителя** (пояснения при просмотре презентации): теперь вы видели, как выглядит компьютер, с которым обращаются правильно и что бывает с теми компьютерами, о которых не заботятся. А почему грязный компьютер ломается? Главные причины поломок:

- пыль вредна не только для нас, она самый большой враг компьютера. Из-за пыли части компьютера не могут достаточно охлаждаться, перегреваются и выходят из строя. А еще из-за пыли вентиляторы могут просто перестать вращаться;

- жара: части компьютера при работе выделяют много тепла. Это тепло отводится с помощью кулеров (вентиляторов) и просто за счет свежего прохладного воздуха в помещении. В жарком помещении компьютеры очень быстро нагреваются до недопустимой температуры;

- сырость: если пары воды конденсируются в компьютере, это может привести к короткому замыканию, и компьютер перегорит.

Лучше всего, если пока компьютер почистит кто-нибудь из взрослых. При чистке компьютера нужно соблюдать правила:

- чистить только выключенный компьютер;

- протирать монитор специальными салфетками или слегка влажной чистой тканью; не использовать для чистки такие вещества как спирт или ацетон;

- чистить клавиатуру пылесосом и ежедневно протирать кнопки;

- почаще протирать «мышь» влажной тканью или специальными средствами;

- чистить хотя бы раз в месяц системный блок внутри осторожно с помощью пылесоса и мягкой кисточки;

- протирать корпус снаружи мягкой влажной тканью.

Как вы думаете, какая часть компьютера пачкается больше всего?

**Деятельность учащихся**: найти ответ (клавиатура) и пояснить его.

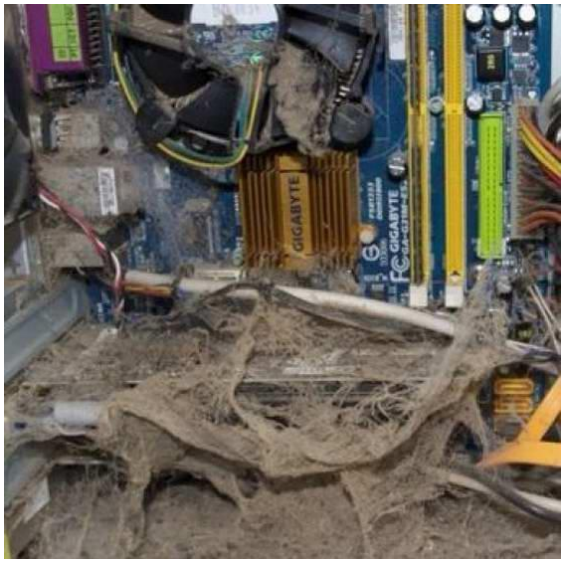
**Деятельность учителя**: Что вы можете сделать для того, чтобы здоровье компьютера оставалось в порядке как можно дольше? Соблюдайте следующие правила:

- Вряд ли от чистки будет много толку, если компьютер постоянно стоит в пыльном месте, или около батареи, или на солнце – так он даже и после чистки быстро перегреется и запылится.

- Нельзя держать компьютер в тесноте и заваливать его части посторонними предметами – например, складывать книги на системный блок.

- И уж совсем не следует есть за компьютером и браться за него мокрыми, жирными или просто грязными руками.

- И еще важное правило: не заставляйте компьютер работать слишком долго, ведь у каждой детали компьютера есть свой срок службы. Чем дольше компьютер работает зря, тем быстрее он сломается просто от «старости». Но и слишком часто включать и выключать компьютер тоже не надо. Лучше точно определить, когда вы собираетесь пользоваться компьютером и не включать его в другое время.




4) **Закрепление изученного материала**

Назвать несколько вещей, вредных для человеческой кожи и компьютера (пыль и грязь, жара).

**Деятельность учителя**: Сегодня мы рассмотрели правила ухода за компьютером. Если вы будете их соблюдать, компьютер прослужит долго, и вы не потеряете из-за его поломки полезную информацию, которую хотели бы сохранить. Дома посмотрите, правильно ли расположен ваш компьютер, узнайте, давно ли его чистили. Помогите родителям, когда они будут чистить компьютер: например, протрите корпус или клавиатуру.

### 4.3. 4 класс. Виды Интернет-общения. Безопасно ли общение в Интернете?

**Окружающий мир**: «Правила вежливости».

**Тематическое планирование**: Правила этикета в общении. Формулы приветствия и прощания. Этикет общения по телефону. Правила поведения в общественном транспорте.

В процессе изучения темы рассматриваются вопросы интернет-общения.

**Задачи:**

**образовательные:**

познакомить с видами общения в Интернете

выяснить степень осведомленности учащихся о безопасной работе в сети

познакомить с правилами безопасной работы при Интернет-общении

**развивающие:**

способствовать формированию информационной культуры учащихся

**воспитательные:**

воспитывать ответственное отношение к общению в сети

*Знания:*

основные виды программ для общения в сети;

чего не следует делать при сетевом общении.

*Умения:*

основные приемы работы с программой Skype.

*Навыки:*

Создание контактов в Skype

**Тип урока**: урок изучения нового материала.

**Методы и формы обучения:** словесный (рассказ), видеометод, наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

**Программно-дидактическое обеспечение:** презентации «Как можно общаться в Интернете», «Средства для общения в Интернете», «Проблемы при общении в Интернете».

**Используемая литература и web-ресурсы**:

3. Полежаева О.А. Методическое пособие для учителей. Информатика. УМК для начальной школы. 2-4 классы. – М.: БИНОМ. Лаборатория знаний, 2013. – 136 с.: ил.
4. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/__12697.pdf

**Этапы урока:**

1) Постановка цели урока и актуализация знаний (2 мин).

2) Изучение нового материала (5 мин).

Объяснение нового материала.

Просмотр презентации.

3) Практическая работа (3 мин).

Информация о домашнем задании.

**Технические средства:** проектор, компьютеры.

**Ход урока**

1) **Постановка цели урока**.

**Деятельность учителя**: Вы узнали о том, что такое правила общения. Общаться можно не только лично, но и в Интернете. Вы наверняка уже общались так со своими друзьями и близкими и знаете, что Интернет позволяет передавать письма, рисунки, фотографии, музыку, фильмы, а также речь.

2) **Актуализация знаний**

**Деятельность учителя**: Расскажите, что такое электронная почта? Что можно пересылать с электронными письмами? Назовите почтовые программы, которые вы знаете.

**Деятельность учащихся**: вспомнить о программах для передачи электронной почты, о правилах пересылки вложенных файлов и т.п.

3) **Изучение нового материала**

**Деятельность учащихся**: просмотр презентации «Как можно общаться в Интернете».

**Деятельность учителя** (пояснения при просмотре презентаций): Интернет позволяет связать между собой любых людей в мире, поэтому, как только он появился, стали создаваться разные способы для общения в Интернете (Skype, Viber, Телеграмм, ICQ, QIP, Мэйл Агент и т.п.).

Общение в Интернете может преследовать разные цели: простая передача информации, диалог, общение в группе, совместная работа, самовыражение. В зависимости от того, с какой целью люди общаются в Интернете, они выбирают средства общения. Если нужно провести совместное обсуждение – используются конференции, позволяющие видеть и слышать друг друга, как если бы участники находились в одном помещении, хотя они могут при этом быть и в разных странах. Если достаточно только обмениваться короткими сообщениями, используются чаты. Интернет-площадки, на которых проводятся обсуждения по выбранным темам, называются Интернет-форумами. Еще одно удобное средство мгновенного обмена текстовыми сообщениями – Интернет-пейджеры, такие как ICQ или QIP. Эта программа позволяет в любой момент узнать, кто из ваших постоянных собеседников находится в сети и готов к общению. Еще более удобная программа – Skype, которая позволяет совершать звонки по Интернет-телефону (в том числе и видеозвонки), а также вести переписку и проводить конференции. Кроме того, общение в сети возможно с помощью многочисленных программ для смартфонов (Fring и др.).

Все эти программы очень удобны и полезны. Но проблемы живого человеческого общения перешли и в Интернет. Недостатки воспитания, стремление солгать, навредить окружающим, оскорбить, оклеветать или унизить, желание заявить о себе в духе старухи Шапокляк «Хорошими делами прославиться нельзя» – все это есть и в сети. Общение в сети может не только нанести обиду или поссорить людей – есть и более опасные последствия необдуманных поступков. И здесь тоже «все как в жизни»: незнакомые люди могут дать вам дурной

совет, они могут предложить вам безобидные с виду, но очень опасные по последствиям развлечения, наконец, просто оказаться преступниками.

Самая распространенная проблема, которую создают себе люди при общении в сети, объясняется их неразборчивостью и легкомыслием. Если вы знаете человека, которого хотите включить в свой список контактов для общения – это хорошо; но часто вам предлагают стать собеседником совершенно незнакомых людей. В сети человек зачастую не виден, он скрыт псевдонимом, как маской. Создать контакт очень легко, а вот во что выльется сетевое общение – известно не всегда. Хорошо, если проблему удастся решить простым удалением нежелательного контакта. Ваш собеседник в сети может вас обманывать и притворяться тем, кем в действительности не является. Но и для вас есть опасность увлечься своей кажущейся невидимостью и безнаказанностью и самому начать обманывать или унижать людей, что уж конечно не сделает вас лучше. Можно спросить: а почему тогда не сообщить в сети все сведения о себе, которые позволили бы людям общаться именно с тобой, а не с твоим ником? Это, конечно, было бы очень хорошим решением, если бы вашей информацией не смогли воспользоваться киберпреступники. Ведь если ваши личные данные станут достоянием злоумышленника, то возможны любые неприятности: преступник сможет действовать от вашего имени, он сможет подменять вашу информацию другой, вредной для вас; наконец, он может узнать сведения о членах вашей семьи. Поэтому при всех недостатках псевдонимов ими приходится пользоваться.

Кроме того, многие программы для интернет-общения предлагают рекламу, или установку новых программ, или ссылки на какие-то новые ресурсы. Как можно знать, какие из них полезны? Помните простое правило – не подбирайте что попало в Интернете, как и на улице. Все эти предложения могут привести к довольно печальным последствиям, из которых заражение вашего компьютера или смартфона вирусами будет еще не самым страшным.

Ну и конечно, очень просто увлечься сетевым общением и начать тратить на него даже то время, которое необходимо для важных дел – уроков, спорта, работы по дому, общения с родными и вполне реальными друзьями.

С какими из перечисленных проблем вам, возможно, уже приходилось сталкиваться?

3) **Практическая работа**

**Деятельность учителя**: сейчас мы запустим программу Skype и посмотрим, что такое контакт и как им управлять (удаление, блокирование, разблокирование, черный список и т.д.).

**Деятельность учащихся**: изучение контактов в Skype.

4) **Закрепление изученного материала**

Опрос:

1) назвать как можно больше известных инструментов для сетевого общения

2) перечислить известные опасности интернет-общения

3) привести правила безопасности для сетевого общения

**Деятельность учителя**: Сегодня мы рассмотрели некоторые способы общения в интернете. Их, конечно, гораздо больше. И опасностей тоже гораздо больше. Нужно хорошо запомнить основные правила безопасности и всегда выполнять их, как правила дорожного движения. Дома спросите родителей о том, какими программами для общения вам разрешается пользоваться и расскажите о тех правилах безопасности, которые вы узнали. Обсудите их с родителями. Найдите новую информацию по запросу «Правила безопасности при работе в сети».

### 4.4. 5 класс. Здоровый образ жизни и компьютер. Виды зависимости. Как определить наличие зависимости

**Основы безопасности жизнедеятельности**: «Здоровье и здоровый образ жизни. Движение и здоровье».

**Тематическое планирование**: Как сберечь зрение? Различные виды нарушения осанки и их причины. Личная гигиена.

При изучении темы происходит знакомство с основами физической и психологической безопасности при работе с ПК и Интернетом.

**Задачи:**

**образовательные:**

познакомить с видами Интернет-зависимости

познакомить с правилами психологической самозащиты при работе с Интернетом и ПК

**развивающие:**

способствовать формированию информационной культуры учащихся

**воспитательные:**

воспитывать ответственное отношение к физическому и психическому здоровью.

*Знания:*

основные источники зависимости;

основные виды зависимости;

меры борьбы с зависимостью

*Умения:*

определять степень опасности использования ресурса

*Навыки:*

основные приемы работы с ПК и Интернетом.

**Тип урока**: урок изучения нового материала.

**Методы и формы обучения:** словесный (рассказ), видеометод, наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

**Программно-дидактическое обеспечение:** презентация «Вредные привычки».

**Используемая литература и web-ресурсы**:

5. Босова Л.Л., Босова А.Ю. Информатика и ИКТ. Поурочное планирование для 5 класса. Методическое пособие. – М.: БИНОМ. Лаборатория знаний, 2012.

6. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/__12697.pdf

**Этапы урока:**

1) Постановка цели урока (1 мин).

2) Актуализация знаний (1 мин).

3) Изучение нового материала (7 мин).

Объяснение нового материала.

Просмотр презентации.

4) Закрепление изученного материала (1 мин).

Информация о домашнем задании.

**Технические средства:** проектор, компьютеры.

**Ход урока**

1) **Постановка цели урока**.

**Деятельность учителя**: Вы уже знаете, как правильно сидеть за компьютером, сколько времени можно за ним проводить. Компьютер – одно из самых полезных устройств, но и он может стать причиной больших бед.

Все вы знаете, что существуют вредные привычки, опасные для здоровья человека и для окружающих. Хуже того – это зависимости, т.к. они становятся потребностями человека, без них он не может существовать. Курение, алкоголизм, наркомания – это смертельно опасные зависимости, которые легко приобрести, но от которых очень трудно избавиться. К сожалению даже такие полезные изобретения как компьютер и Интернет тоже могут стать источниками смертельно опасных зависимостей.

2) **Актуализация знаний**

**Деятельность учителя**: Вы знаете многие способы использования компьютера для работы и отдыха. Не замечали ли вы, на что вы тратите за компьютером больше времени – на работу или на развлечения?

**Деятельность учащихся**: вспомнить об учебных и офисных программах, браузерах, средствах интернет-общения, играх и т.п.

3) **Изучение нового материала**

**Деятельность учащихся**: просмотр презентации «Как развивается компьютерная зависимость».

**Деятельность учителя** (пояснения при просмотре презентации): Любое занятие может превратиться в привычку – как полезное, так и вредное. Хорошие привычки – вовремя делать уроки, читать, убирать комнату, заниматься спортом. Привычка часами смотреть телевизор или играть в компьютерные игры – это уже хуже. С возрастом, к сожалению, человеку становится известно все больше вредных занятий – курение, употребление алкоголя и наркотиков, азартные игры – и это еще далеко не все, что может причинить вред. Но хуже всего то, что знакомство со всеми вредными занятиями очень легко может перерасти в крепкую дружбу. Последствия же такой дружбы – разрушенная жизнь и горе семьи и друзей. Может возникнуть вопрос – а причем здесь компьютер? Это же не наркотик, не сигареты – какие от него проблемы?

Как безобидное, в общем-то, занятие может превратиться в привычку, а привычка в зависимость? Психологи говорят о следующих этапах развития зависимости. Сначала тратится время в поисках «подходящей» виртуальной реальности. Становится ясно, во что человек готов «погрузиться с головой», не считаясь со временем и здоровьем. Что это будет для каждого конкретного человека – бесконечное общение в социальных сетях, компьютерные игры или постоянные путешествия по Интернету в поисках зачастую ненужной и бессмысленной информации? Но вот занятие выбрано и на него тратится все больше времени. Постепенно простая трата времени перерастает в нечто более серьезное: реальная жизнь становится неинтересна, все цели и смысл переносятся на жизнь виртуальную – вам будет важнее мнение посторонних людей в социальных сетях, чем мнение ваших близких, лайки под постами станут важнее, чем реальные успехи и достижения; ваш персонаж в компьютерной игре будет для вас заменой собственной личности – и что из того, что в жизни вы слабы и беспомощны, зато в

игре вы повелитель вселенной. Бурная стадия зависимости постепенно угасает, но не исчезает. Вся реальная жизнь становится только неизбежным злом, с которым хотелось бы сталкиваться как можно реже. Уроки, прогулки, даже еда и сон – все это воспринимается как препятствие на пути к цели – компьютерной игре или общению в социальной сети. Даже важные события в жизни семьи не вызывают интереса – ведь они отвлекают от «смысла жизни».

Известны многие виды Интернет- и компьютерной зависимости:

1) информационная зависимость (стремление постоянно путешествовать по Интернету в бесцельных поисках информации);
2) игровая зависимость;
3) зависимость то интернет-общения;
4) зависимость от азартных игр в интернете;
5) стремление к поиску информации агрессивного или непристойного содержания;
6) постоянное стремление к просмотру или скачиванию фильмов или музыки;
7) стремление к совершению вредных действий (целенаправленное нарушение правил сетевого этикета, распространение ненужной или вредной информации и т.п.).

Интернет-зависимые (или зависимые от компьютера) как большинство психически нездоровых людей не осознают тяжести своего состояния и с раздражением и агрессией относятся к попыткам отвлечь их от источника зависимости. Но это происходит когда болезнь зашла уже слишком далеко. До этого еще можно и самостоятельно обнаружить у себя признаки формирующейся зависимости и, если хватит силы воли, вовремя остановиться.

Как узнать, что привычка начала переходить в болезнь? Проверьте себя. Если вы честно ответите «да» на большую часть следующих вопросов – вы в опасности:

1. Вы испытываете радость и удовольствие при занятиях с компьютером и отвращение ко всем остальным видам деятельности;

2. Друзья постепенно перестают с вами общаться, но вас это не расстраивает;
3. Вас интересует только то, что связано с предметом вашего увлечения – играми, социальными сетями и т.п.;
4. Все разговоры вы стремитесь свести к обсуждению источника вашей зависимости, независимо от того, кто ваш собеседник;
5. Вы считаете, что следует потратить все деньги на покупку новых игр или на увеличение мощности компьютера и вас раздражает, если родители с вами в этом не соглашаются;
6. Вы проводите за компьютером слишком много времени и не замечаете этого, вас раздражают замечания родителей об этом;
7. Вы воспринимаете людей, которые могут попросить вас освободить компьютер для себя, как личных врагов;
8. Вы любитель поиска информации, вы постоянно переходите по ссылкам с одного сайта на другой, поглощаете информацию без разбора, не разбираясь, правдива она или ложна, ценна или бессмысленна;
9. События, о которых вы читаете в Интернете, вызывают у вас чрезмерно острую реакцию (гнев, счастье, ненависть);
10. У вас начались проблемы со здоровьем: бессонница, раздражительность, боль в спине, жжение в глазах, головная боль и пр.

Однако с любой проблемой можно справиться, если осознавать в этом необходимость.

Конечно, когда болезнь зашла слишком далеко, без лечения и врача не обойтись. Но никакой врач не сможет помочь тому, кто не хочет помочь себе сам. Для того чтобы не попасть в компьютерную зависимость, помогут следующие действия:

1) Если вы проводите за компьютером по несколько часов, начните постепенно уменьшать время пребывания за компьютером, хотя бы на 10 минут каждый день;
2) Не старайтесь при каждой неприятности отвлекаться от нее с помощью компьютера;

3) Больше будьте на воздухе, двигайтесь, постарайтесь заняться спортом;
4) Старайтесь побольше общаться с друзьями лично, а не в сети;
5) Если у вас появилось свободное время, не торопитесь за компьютер – попробуйте выяснить, нет ли для вас более полезного занятия (уроки, работа по дому);
6) Определите для себя время на развлечения за ПК и не выходите за эти пределы;
7) Если вы работаете с компьютером в учебных целях, следите за тем, чтобы не отвлекаться на ненужные ресурсы;
8) Ложитесь раньше спать, отрегулируйте режим питания, не ешьте за компьютером.

4) **Закрепление изученного материала**

Опрос:

1) перечислить виды компьютерной и интернет-зависимости;

2) перечислить признаки зависимости в поведении и образе жизни человека.

**Деятельность учителя**: Сегодня мы рассмотрели, как работа с ПК и интернетом может привести к проблемам. Обсудите дома с родителями, не замечали ли они у вас каких-либо признаков зависимости от компьютера. Внимательно отнеситесь к их замечаниям. Найдете в Интернете информацию по запросу «Признаки игромании».

### 4.5. 6 класс. Как распространяются вирусы

**Основы безопасности жизнедеятельности**: «Влияние неблагоприятной окружающей среды на здоровье человека».

**Тематическое планирование**: Влияние производственной деятельности человека на окружающую среду. Влияние неблагоприятной окружающей среды на здоровье человека. Как повысить устойчивость организма к неблагоприятному воздействию внешней среды?

После перечисления неблагоприятных для здоровья человека процессов можно указать, что для здоровья компьютера тоже имеются неблагоприятные факторы и перейти к знакомству с основами антивирусной защиты компьютера.

**Задачи:**

**образовательные:**

познакомить с источниками распространения компьютерных вирусов

выяснить степень осведомленности учащихся о вирусах

познакомить с правилами защиты ПК от вирусов

**развивающие:**

способствовать формированию информационной культуры учащихся

**воспитательные:**

воспитывать ответственное отношение к обращению с компьютером и Интернетом.

*Знания:*

основные понятия о компьютерных вирусах;

как избежать заражения компьютера.

*Умения:*

основные приемы работы с антивирусными программами.

*Навыки:*

запуск программы-антивируса для сканирования компьютера и внешних носителей информации.

**Тип урока**: урок изучения нового материала.

**Методы и формы обучения:** словесный (рассказ), видеометод, наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

**Программно-дидактическое обеспечение:** презентации «Что такое компьютерные вирусы», «Откуда приходят вирусы».

**Используемая литература и web-ресурсы**:

7. Босова Л.Л., Босова А.Ю. Информатика и ИКТ. 5-7 классы. Методическое пособие. – М.: БИНОМ. Лаборатория знаний, 2011.
8. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/__12697.pdf

**Этапы урока:**

1) Постановка цели урока (1 мин).

2) Актуализация знаний (1 мин).

2) Изучение нового материала (5 мин).

Просмотр презентации.

3) Практическая работа (3 мин).

4) Информация о домашнем задании.

**Технические средства:** проектор, компьютеры.

**Ход урока**

1) **Постановка цели урока**.

**Деятельность учителя**: Мы знаем, что загрязнение воды и воздуха способствует развитию различных заболеваний. У компьютеров тоже могут возникнуть свои болезни. Часть из них может быть вызвана проблемами «окружающей среды» компьютера – пылью, грязью. Однако есть и другая опасность, от которой требуется защита. Все вы знаете о том, что существуют компьютерные вирусы, а возможно и сталкивались с последствиями заражения своих компьютеров.

2) **Актуализация знаний**

**Деятельность учителя**: Мы с вами уже не раз говорили о том, как важно при передаче и получении информации не допустить заражения компьютера вирусами.

**Деятельность учащихся**: вспомнить о мерах предосторожности при переносе файлов, при скачивании информации из сети и т.п.

3) **Изучение нового материала**

Просмотр презентации «Что такое компьютерные вирусы», «Откуда приходят вирусы».

**Деятельность учителя** (комментарии при показе презентации): Вирус – это программа, написанная с целью причинить вред компьютеру. Его поведение похоже на поведение биологического вируса – он так же, попадая в «организм» компьютера, способен размножаться и внедряться в файлы, нарушая или делая невозможной работу компьютера. Если поначалу вирусы создавались больше из хулиганских побуждений, то теперь это серьезное и опасное оружие, способное причинить огромный вред не только отдельному компьютеру, но даже системе безопасности целой страны. Конечно, не будь компьютеров и интернета – не было бы и компьютерных вирусов. Но ведь люди и сами всегда испытывают на себе атаки вирусов, и, тем не менее, человечество до сих пор живо. Оружие человека в борьбе с вирусами – защитные силы организма и медицина. Есть такие защитные силы и медицина и для компьютеров.

В мире существуют сотни тысяч вредоносных программ. У них есть своя классификация.

Вирусами называют программы, которые размножаются в компьютере и при этом уничтожают или искажают данные, нарушают работу операционной системы, ограничивают доступ к файлам, замедляют работу компьютера и т.п. Чаще всего вирусы передаются с переносных устройств хранения информации – дискет, флеш-памяти, карт памяти и т.п.

Сетевые черви могут самостоятельно распространяться по сети. Проникают они в компьютер с электронной почтой, через обмен сообщениями. Сетевой червь, поселившись в компьютере, может воспользоваться списком адресов, которые в нем хранятся, и начать рассылать от имени этого компьютера сообщения со ссылками на вредоносные ресурсы (источники вирусов).

Троянские программы обычно не разрушают информацию на компьютере, но могут собирать сохранившуюся на ПК личную информацию пользователя и пересылать ее злоумышленникам. Они могут следить за тем, какие клавиши нажимает пользователь, или предоставлять удаленный доступ к компьютеру посторонним лицам.

Еще один вид вредоносных программ вызывает демонстрацию на компьютере рекламной информации; часто такие программы занимаются сбором данных о пользователе.

Вирусы различаются и по целям заражения (файлы, оперативная память), по способу действия, по уровню наносимого вреда.

Так какие же бывают источники заражения компьютеров?

Перенос вирусов возможен с дискет, флеш-накопителей, мобильных телефонов, т.е. с любых внешних запоминающих устройств. Вирусы распространяются и через электронную почту, точнее, через пересылаемые с ней файлы (вложения). В этих файлах могут содержаться вирусные программы или ссылки, при переходе по которым можно попасть на сайт, который содержит вредоносную программу. Почтовые вирусы могут сделать и ваш компьютер источником заражения в сети. Вредоносные вложения распространяются через системы мгновенного обмена сообщениями (ICQ, QIP). Вредоносный код может содержаться и на веб-страницах, которые в посещаете в Интернете. Эти страницы часто «украшены» различным активным содержимым, позволяющим запускать программы для воспроизведения различных файлов, например, музыки. Вирусные программы часто маскируются под такое ПО.

С какими из перечисленных проблем вам, возможно, уже приходилось сталкиваться?

3) **Практическая работа**

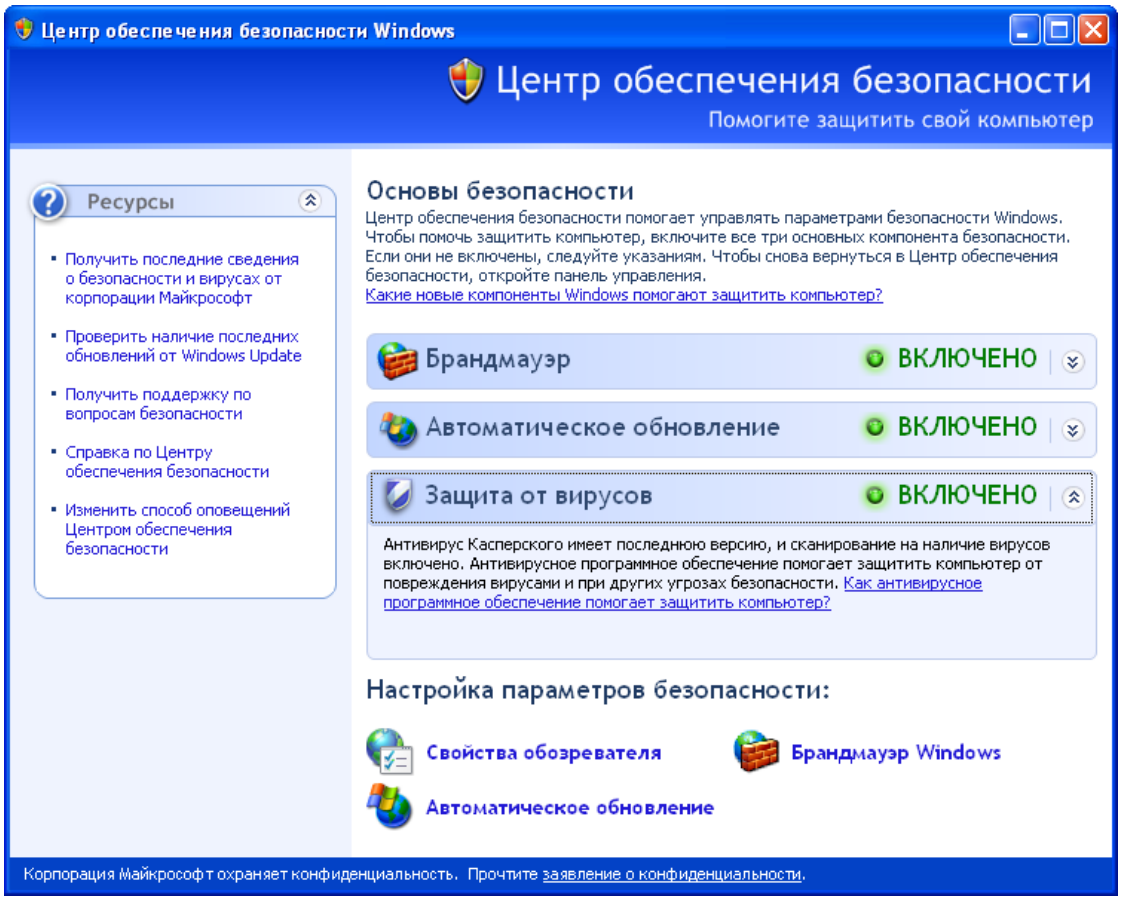
Поиск антивирусного ПО, установленного на компьютере.

Как узнать, какое антивирусное ПО установлено на компьютере? Можно, например, в меню Пуск вызвать Панель управления, найти Центр обеспечения

безопасности – Защита от вирусов  и там прочитать информацию об установленном антивирусном ПО.

Сейчас вы найдете ярлык антивирусной программы на вашем ПК (например, Kaspersky Anti-Virus). Откройте окно программы и найдите справочную информацию о ее работе. Справка – необходимый инструмент для правильной работы с программным обеспечением.

Обсуждение найденного материала.




**Деятельность учащихся**:

1) Найти на школьном ПК ярлыки антивирусного ПО.
2) Запустить антивирусную программу и просмотреть справку о ее работе.

**Деятельность учителя**: Всегда помните правила защиты компьютера от вирусов:

1) Установить антивирусное ПО и своевременно его обновлять.
2) Периодически запускать проверку компьютера на наличие вирусов.
3) Не открывать электронные письма с вложениями от незнакомых адресатов.

4) Не откликаться в интернете на предложения установить новую программу или провести проверку вашего компьютера на вирусы.
5) Не переходить по присланным от неизвестных источников случайным ссылкам.
6) Всегда проверять внешние устройства памяти на наличие вирусов.
7) Пользоваться настройками безопасности браузеров и почтовых программ.

4) **Закрепление изученного материала**

Опрос:

1) назовите известные вам источники заражения компьютера

2) перечислите известные вам антивирусные программы

Чем больше вы будете работать с ПК или другими устройствами, тем больше вы будете узнавать об угрозах для них. Никогда не пренебрегайте правилами безопасной работы, старайтесь находить и запоминать информацию о новых источниках заражения для компьютеров. Дома проверьте, есть ли у вас антивирусное ПО, давно ли оно обновлялось. Проведите полную проверку компьютера на наличие вредоносных объектов.

### 4.6. 7 класс. Утечка и обнародование личных данных

**Информатика**: «Компьютер как универсальное устройство обработки информации»

**Тематическое планирование**: Обработка информации. Обработка, связанная с получением новой информации. Поиск информации.

При изучении процесса поиска информации в Интернете можно рассмотреть тему предотвращения утечки личных данных.

**Задачи:**

**образовательные:**

познакомить с каналами утечки личных данных в Интернете

выяснить степень осведомленности учащихся о защите личных данных

познакомить с некоторыми правилами защиты личных данных

**развивающие:**

способствовать формированию информационной культуры учащихся

**воспитательные:**

воспитывать ответственное отношение к обращению с Интернетом.

*Знания:*

основные понятия о личных данных и их защите

как избежать потери личных данных

*Умения:*

основные приемы работы с ресурсами Интернет

*Навыки:*

Настройка браузера

**Тип урока**: урок изучения нового материала.

**Методы и формы обучения:** словесный (рассказ), видеометод, наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

**Программно-дидактическое обеспечение:** презентация «Что такое персональные данные», «Кому нужны ваши личные данные»

**Используемая литература и web-ресурсы**:


1. Босова Л.Л., Босова А.Ю. Информатика и ИКТ. 5-7 классы. Методическое пособие. – М.: БИНОМ. Лаборатория знаний, 2011.
2. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/__12697.pdf


**Этапы урока:**

1) Постановка цели урока (1 мин).

2) Актуализация знаний (1 мин).

3) Изучение нового материала (6 мин).

Объяснение нового материала.

Просмотр презентации.

4) Закрепление изученного материала (2 мин).

Опрос.

Информация о домашнем задании.

**Технические средства:** проектор, компьютеры.

**Ход урока**

1) **Постановка цели урока**.

**Деятельность учителя**: Каждый, кто искал информацию в Интернете, наверняка сталкивался с просьбами сообщить что-либо о себе – хотя бы номер мобильного телефона. Часто это происходит при попытках скачать файлы из сети. Но есть и много других случаев, когда пользователя просят сообщить различные данные – например, при регистрации на различных ресурсах, при создании почтового ящика и т.п. И конечно, в большинстве случаев возникает вопрос – а нужно ли это делать? Зачем нужна эта информация? Почему о ней спрашивают?

2) **Актуализация знаний**

**Деятельность учителя**: Вы знаете, что такое социальные сети, форумы, почтовые сервисы и другие средства общения в Интернете. Вспомните, как вы получали доступ к этим средствам и какую информацию о себе сообщали.

**Деятельность учащихся**: вспомнить примеры вопросов, задаваемых при регистрации на различных ресурсах (например, почтовый сервер и т.п.)

3) **Изучение нового материала**

**Деятельность учащихся**: просмотр презентации «Что такое персональные данные», «Кому нужны ваши персональные данные».

**Деятельность учителя**: Все сведения, касающиеся конкретного человека (ФИО, адрес, телефон и т.п.) – это персональные данные. К персональным данным относятся паспортные и биографические данные, сведения о профессии и образовании, адрес и телефон, сведения о составе семьи и многое другое. Персональные данные охраняются законом (ФЗ о персональных данных) с целью защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Вы можете убедиться, как много сведений о вас становится известно при такой, казалось бы, безобидной процедуре как регистрация в социальной сети. Так, например, в Одноклассниках вас попросят сообщить имя, фамилию, пол, дату рождения, адрес электронной почты, страну и город проживания, а при завершении регистрации еще и номер телефона (демонстрация на проекторе страницы регистрации). Дальше будет еще больше «возможностей». Вы начинаете размещать на предоставленной вам странице свою фотографию и фотографии своих друзей, видео и музыку и вообще все, что сочтете нужным, даже то, о чем сообщать не следовало бы. Примерно так же обстоят дела и в фэйсбуке (демонстрация страницы регистрации). Почтовые сервисы, сайты знакомств – везде требуются личные данные. Еще более важные сведения сообщаются при поиске работы (демонстрация резюме), при различных видах платежных операций, при обращении на сайты госструктур и т.д. Кроме подобных данных пользователи оставляют в Интернете много другой информации, не предназначенной для посторонних – это переписка, файлы, хранящиеся на облачных сервисах и т.п.

Конечно, в ряде случаев подлинную информацию предоставлять не обязательно. Анонимность при использовании многих сервисов даже приветствуется. Но очень часто без предоставления подлинной информации обойтись нельзя – например, при пользовании электронными госуслугами, медицинскими системами и т.п.

При этом все, кто получает от пользователей личную информацию, обязуются обеспечить ее безопасность, т.е. гарантируют, что в чужие руки она не попадет. И, тем не менее, это часто случается. Незаконное получение и обнародование (распространение) чужой личной информации является преступлением.

Подсчитано, что каждый пятый человек старше 18 лет становился жертвой кибератаки в социальных сетях или через мобильные устройства. Чаще всего целью получения личных данных является доступ к банковским счетам.

Что такое утечка данных? Это следствие действий посторонних лиц, которые с помощью различных технических приемов смогли получить права доступа к личной информации, в результате чего она перестает быть конфиденциальной и может быть использована в противоправных или аморальных целях.

Зачем и кому могут понадобиться ваши личные данные? Казалось бы, кому они нужны кроме вас?

Ими могут воспользоваться рекламодатели (для увеличения числа рассылок).

Чужие личные данные используются для получения кредитов и краж средств из банков.

Данные могут быть украдены из хулиганских побуждений (обнародовать переписку, например).

Данные могут быть украдены для последующей перепродажи.

Интересно, что понятию «утечка персональных данных» в английском языке соответствует Identity theft (кража личности).

Утечка данных возможна с компьютера, ноутбука, мобильного устройства. При этом данные попадают к киберпреступникам через Интернет, электронную почту. Кроме того, устройство можно просто потерять – и тогда даже флешка может стать источником личных данных.

Ценность для злоумышленников представляют и учетные записи электронной почты. Адрес электронной почты может использоваться для подтверждения регистрации на других веб-сайтах.

Кто является виновником утечек?

Инсайдеры

Недостатки («уязвимости») ПО

Хакеры

Провайдеры

Незащищенные каналы связи

Социальные сети

Пользователи

Утечки персональных данных обнаруживаются постоянно, причем часто это «работа» даже не злоумышленников, а именно тех ресурсов, которыми мы пользуемся. Причиной утечек могут быть недостатки программного обеспечения, но часто сами владельцы сервисов собирают информацию о пользователях в различных целях. Так, корпорация Apple неоднократно обвинялась в шпионаже за пользователями их смартфонов. Google и вовсе заявлял, что не несет ответственности за сохранность личных данных своих пользователей, установивших различные приложения. На данный момент наиболее надежным в плане защиты личных данных считается компания Mozilla. Не раз обнаруживалась утечка личных данных пользователей интернет-магазинов, по вине которых стало возможным найти с помощью поисковых ресурсов информацию о покупках, и даже паспортные данные и номера кредитных карт покупателей. Взламываются и базы данных о покупках авиа- и железнодорожных билетов. После таких взломов в открытый доступ попадает информация, охраняемая законом. Кто угодно при наличии определенных знаний может воспользоваться чужими личными данными.

Очень часто киберпреступникам не нужно устраивать никаких атак и взломов – пользователи сами сообщают им личные данные. Для этого есть много приемов: фишинговые рассылки (например, рассылаются анкеты с предложениями работы), распространение вредоносных программ и т.д.

Пока нельзя утверждать, что какие-либо данные полностью защищены, даже если по отношению к ним приняты все возможные меры защиты. Методы защиты совершенствуются, но и взломщики не останавливаются. Например, появились даже устройства, которые действуют как вирусы: с виду это обычная мышка, а на самом деле кейлоггер – устройство, отслеживающее все, что пользователь вводит в компьютер.

Как избежать утечек личных данных?

Прежде всего, не сообщать личные данные всем желающим.

Пользоваться постоянно обновляемым надежным ПО (ОС, браузер, антивирус).

Своевременно проводить проверку компьютера на вирусы.

Проверять на вирусы каждое подключаемое устройство хранения информации (флеш-память, карты памяти и пр.).

Не переходить бездумно по всем встречающимся ссылкам, увеличивая риск натолкнуться на вредоносный ресурс.

Доверять только проверенным крупным сервисам.

Не откликаться на подозрительные e-mail сообщения.

Не запускать неизвестные программы, в том числе предлагаемые в интернете.

Не использовать слишком простые пароли или одинаковые пароли для всех сервисов.

Прежде чем вводить пароль, убедитесь, что в адресной строке браузера находится правильный адрес сайта, т.к. вы можете столкнуться с поддельной формой регистрации (они размещаются на веб-страницах с адресами, похожими на настоящие).

Не соглашайтесь на предложение «Запомнить пароль», особенно при работе на чужом компьютере.

Если вы авторизовались на сайте, то не оставляйте компьютер без присмотра; даже если вы отошли ненадолго, выполните операцию «Завершение работы» и закройте браузер.

Старайтесь не держать на компьютере отсканированные копии документов.

4) **Закрепление изученного материала**

Опрос:

1) назовите известные вам причины утечек личных данных

2) перечислите известные вам меры защиты от утечек

Информация о домашнем задании

Сегодня мы узнали только о некоторых проблемах безопасности персональных данных. Это очень серьезная часть всей системы кибербезопасности. Способы хищения личных данных постоянно изменяются, поэтому составить раз и навсегда список рекомендаций по безопасной работе вряд ли получится. Но одно правило все же остается неизменным – будьте внимательны и осторожны и при получении и при передаче информации. Дома узнайте, какие меры для защиты личных данных используются на вашем компьютере.

### 4.7. 8 класс. Подмена сайтов в интернете (сайты-клоны). Фальшивые файлообменники

**Информатика:** Коммуникационные технологии

**Тематическое планирование**: WWW-технология. Всемирная паутина (настройка браузера, адрес Web-страницы, сохранение и печать Web-страниц).

**Цель**: знакомство с видами мошеннических действий в сети

**Задачи:**

**образовательные:**

познакомить с некоторыми видами мошеннических действий в Интернете

выяснить степень осведомленности учащихся о защите от мошеннических действий в Интернете

познакомить с некоторыми правилами безопасной работы в сети

**развивающие:**

способствовать формированию информационной культуры учащихся

**воспитательные:**

воспитывать ответственное отношение к обращению с Интернетом.

*Знания:*

основные понятия о мошеннических действиях и защите от них

*Умения:*

основные приемы работы с ресурсами Интернет

*Навыки:*

Настройка параметров безопасности

**Тип урока**: урок изучения нового материала.

**Методы и формы обучения:** словесный (рассказ), видеометод, наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

**Программно-дидактическое обеспечение:** презентация «Ложные сайты», «Файлообменные ресурсы Интернета»

**Используемая литература и web-ресурсы**:


1. Босова Л.Л., Босова А.Ю. Учебник по информатике за 8 класс. – М.: БИНОМ. Лаборатория знаний, 2013.
2. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/__12697.pdf


**Этапы урока:**

1) Постановка цели урока и актуализация знаний (1 мин).

2) Изучение нового материала (6 мин).

Объяснение нового материала.

Просмотр презентации.

3) Практическая работа (3 мин).

Поиск информации в сети Интернет.

Обсуждение найденного материала.

4) Закрепление изученного материала

Информация о домашнем задании.

**Технические средства:** проектор, компьютеры.

**Ход урока**

1) **Постановка цели урока**.

В сети существует множество опасных ресурсов: одни являются источниками вирусов, другие охотятся за личными данными пользователей, третьи принадлежат наркоторговцам или экстремистам. Но едва ли кто-то будет преднамеренно искать себе проблемы в Интернете. Как же можно заставить пользователя попасть на вредоносные ресурсы?

**2) Актуализация знаний**

**Деятельность учителя**: Вы уже знаете о некоторых приемах, которыми пользуются злоумышленники в Интернете для заражения компьютеров вирусами, кражи личных данных и других преступных целей, знаете о том, что такое утечка личных данных и какими способами она организуется; знаете, что такое вирусы и какими путями они приникают в компьютер. Вспомните основные правила безопасности при работе в Интернете.

**Деятельность учащихся**: вспомнить основные правила безопасной работы в сети.

3) **Изучение нового материала**

**Деятельность учащихся**: просмотр презентации «Ложные сайты», «Файлообменные ресурсы Интернета».

**Деятельность учителя** (пояснения при просмотре): Среди различных вредоносных программ существует вирус подмены страниц. Его задача – перенаправить пользователя с той страницы, к которой он обращается, на другую, часто имеющую вредоносное содержание. Часто ложные страницы очень похожи на настоящие, так что пользователь может и не догадаться о подмене. На таких страницах пользователя можно заставить раскрыть свой пароль или ввести другие личные данные, заставить его перевести деньги злоумышленникам и т.п. Иногда и без перехода на другие страницы действие вируса может проявляться в том, что при регистрации или авторизации на сайте предлагается подтвердить свои данные с помощью SMS. Кроме того, переходы на ненужные ресурсы ведут к росту трафика. Такой вирус часто классифицируют как рекламное ПО или троян.

Ссылка на вредоносный сайт может, например, внедряться в результаты поиска, причем внешне ее отличить трудно. Бывает и так, что результаты поиска не изменяются, но при попытке перейти по выбранной ссылке пользователь попадает на другую страницу.

Очень опасный вид сайтов-клонов – сайты, подделывающиеся под сайты госслужб или банков. Обычно адреса таких сайтов почти полностью совпадают с настоящими, поэтому для того чтобы попасть на них, пользователю бывает достаточно просто допустить ошибку при ввода адреса. Особенно важно уметь обнаружить подделку при работе с онлайн-сервисами банков.

Иногда подмена происходит при долгом отсутствии пользователя – вирус отслеживает активность мыши и в случае, если сайт открыт слишком долго, а пользователя за компьютером нет, подменяет этот сайт другим. Источником вируса может быть тот самый первоначально открытый сайт.

Один из видов мошенничества, связанный с ложными сайтами – обман рекламодателей. Реклама может появляться при упоминании в поисковом запросе заданных для нее ключевых слов. Но в результате действия вируса пользователь переходит по ложной ссылке, причем и на сайт рекламодателя он тоже не попадает, хотя рекламодатель уверен, что все в порядке, и оплачивает рекламу.

Вирус подмены страниц можно получить с программой, загруженной из сети. Так, известный файлообменный сервис Letitbit.net предлагает бесплатный ускоритель закачки файлов, вместе с которым пользователь получает скрытую библиотеку ссылок.

Избавиться от таких вирусов очень сложно. Некоторые пользователи переустанавливают браузер. Но неплохо работает специальное приложение к Антивирусу Касперского Я.Онлайн или утилита CureIt от Доктор Веб.

Чтобы отличить ложный сайт, особенно если он очень похож на настоящий, нужно внимательно проверять адрес сайта, т.к. адреса подделок часто отличаются от настоящих на одну-две буквы. Кроме того, крупные организации используют защищенные соединения, о чем говорит наименование протокола с

механизмами шифрования https (HyperText Transfer Protocol Secure) в адресе сайта:


Если сайт распознан как поддельный, его открытие в браузерах блокируется. Пользователь может сообщить о поддельном сайте самостоятельно – например, в InternetExplorer есть переход Сервис – Фильтр фишинга – сообщить о веб-узле.

Еще один подделываемый ресурс Интернета – файлообменники (файловый хостинг), позволяющие пользователям загружать свои файлы на сервер; после этого файл получает ссылку, которую можно распространять, чтобы, перейдя по ней, другие пользователи могли скачать этот файл. Скачивать файлы в файлообменниках можно бесплатно или через оплаченный премиум-аккаунт (с высокой скоростью, с возможностью докачивания, без рекламы). За частое скачиваемые файлы пользователь может получать плату от ресурса. Наиболее известные файлообменные серверы – Depositfiles и Letitbit. Бывают и платные файлообменные ресурсы.

Фальшивые файлообменники требуют с пользователя деньги за скачивание файлов, но взамен пользователь ничего хорошего не получает. Как раз на такие фальшивки пользователя перенаправляют вирусы подмены страниц. Фальшивые ресурсы обычно позволяют пользователю скачать некий exe-файл, якобы позволяющий продолжить скачивание. Однако затем сообщается, что скачанный архив защищен паролем и чтобы его открыть, нужно послать SMS-сообщения на указанный номер.


Деньги, полученные от пользователя таким образом, пропадают – все равно ожидаемых файлов так получить нельзя. Зарубежные ресурсы такого рода занимаются также шантажом и вымогательством – они сообщают о якобы незаконном скачивании и предлагают заплатить немалый штраф.

Список таких файлообменников имеется на сайтах разработчиков антивирусов, но не все пользователи обращаются к этим сведениям, да к тому же постоянно возникают новые фальшивки.

Вопрос: С какими из перечисленных проблем вам, возможно, уже приходилось сталкиваться?

Как избежать проблем с фальшивыми ресурсами?

- Будьте внимательны при переходе по ссылкам в Интернете, особенно на незнакомые ресурсы
- Пользуйтесь своевременно обновляемым антивирусным ПО
- Внимательно проверяйте адрес ресурса
- Если сайт кажется вам подозрительным, немедленно уходите с него
- Не сообщайте никаких данных о себе, особенно если вы не ожидали увидеть какие-либо вопросы
- Никогда не запускайте никаких предложенных вам программ
- Обращайте внимание на просьбы об оплате через СМС – чаще всего это признак мошеннических действий

- Не надейтесь за небольшие деньги или бесплатно скачать дорогостоящее ПО – скорее всего, это мошенническое предложение
- Всегда помните о «бесплатном сыре» Интернета

3) **Практическая работа**

**Деятельность учителя**: Найдите список фальшивых файлообменников. Попробуйте выполнить переход на один из них. Убедитесь, что сайт заблокирован. Найдите список надежных файлообменников. Откройте один из них и ознакомьтесь с правилами работы с ним.

Информация о домашнем задании

Сегодня мы узнали еще о нескольких видах мошеннических действий в Интернете. Однако с каждый днем их становится все больше. Поэтому нужно постоянно следить за новыми событиями в области обеспечения кибербезопасности и самое главное – всегда быть внимательными при работе с ресурсами Интернета. Дома попытайтесь скачать какой-нибудь полезный файл и известного и надежного ресурса (например, Файлы@Mail.ru). Составьте отчет о проделанной работе со скриншотами каждого этапа.

### 4.8. 9 класс. Типы вирусов. Отличия вирусов и закладок

**Информатика**: «Локальные и глобальные компьютерные сети»

**Тематическое планирование**: Сообщение, канал связи, компьютерная сеть, скорость передачи информации, локальная сеть, глобальная сеть

Рассматривая вопросы организации сетей и работы с ними, перейти к вопросам защиты от вирусов, которые могут быть получены из сети.

**Задачи:**

**образовательные:**

познакомить с классификацией вирусов и другого вредоносного ПО

выяснить степень осведомленности учащихся о видах вирусов

**развивающие:**

способствовать формированию информационной культуры учащихся

**воспитательные:**

воспитывать ответственное отношение к обращению с ПК и Интернетом.

*Знания:*

основные понятия о вирусах

*Умения:*

основные приемы безопасной работы с ресурсами Интернет и ПК

*Навыки:*

Настройка параметров безопасности

**Тип урока**: урок изучения нового материала.

**Методы и формы обучения:** словесный (рассказ), видеометод, наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

**Программно-дидактическое обеспечение:** презентация «Классификация компьютерных вирусов».

**Используемая литература и web-ресурсы**:


9. Босова Л.Л., Босова А.Ю. Учебник по информатике за 9 класс. – М.: БИНОМ. Лабора-тория знаний, 2013.
10. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/__12697.pdf


**Этапы урока:**

1) Постановка цели урока (1 мин).

2) Актуализация знаний (1 мин).

3) Изучение нового материала (7 мин).

Объяснение нового материала.

Просмотр презентации.

4) Закрепление изученного материала (1 мин).

Опрос.

Информация о домашнем задании.

**Технические средства:** проектор, компьютеры.

**Ход урока**

1) **Постановка цели урока**.

**Деятельность учителя**: Мы уже много раз говорили о вирусах и другом вредоносном ПО, обсуждали пути их распространения и меры защиты. Сегодня наша цель – рассмотреть несколько способов классификации вирусов.

2) **Актуализация знаний**

**Деятельность учителя**: Вспомните, какие бывают компьютерные вирусы и каковы последствия заражения ими ПК.

**Деятельность учащихся**: вспомнить основные разновидности вредоносного ПО.

3) **Изучение нового материала**

**Деятельность учащихся**: просмотр презентации «Классификация компьютерных вирусов».

**Деятельность учителя** (пояснения при просмотре презентации): Вредоносным является любое ПО, предназначенное для несанкционированного использования ресурсов ПК или доступа к данным для их копирования, изменения, подмены или уничтожения, а также для нейтрализации средств защиты.

Существует свыше ста тысяч известных вирусов и вредоносных программ и число их постоянно растет. Вредоносная программа представляет угрозу информации, хранящейся в компьютерной системе, создает возможность нецелевого использования ресурсов ПК или каким-либо образом препятствует нормальному функционированию ПК. К вредоносным программам относятся компьютерные вирусы, трояны, сетевые черви и др.

Если говорить об угрозах безопасности информации, то вредоносное ПО нарушает конфиденциальность, целостность и доступность информации. Нарушение конфиденциальности происходит за счет краж паролей, удаленного управления, краж и распространения информации. Нарушение целостности происходит за счет модификации и шифрования, а также уничтожения информации (вплоть до форматирования дисков). Нарушение доступности происходит за счет перегрузки каналов инфицированными рассылками, блокирования доступа к сайтам; возможен даже вывод ПК из строя за счет порчи BIOS.

Вирусы – разновидность вредоносного ПО, отличающаяся способностью создавать свои копии и внедрять их в файлы и системные области компьютера. Стадии размножения вируса: проникновение, активация, поиск объектов для заражения, подготовка и внедрение вирусных копий.

Существует много способов классификации вирусов. Их можно классифицировать, например, по среде обитания (объектам заражения), по нацеленности на определенную ОС, по алгоритмам работы, по виду наносимого вреда.

По объектам заражения вирусы делятся на:

1. Загрузочные вирусы: заражают загрузочные сектора постоянных и сменных носителей информации (например, жестких дисков).
2. Файловые вирусы: вирусы, воздействующие на ресурсы ОС путем полного или частичного изменения содержимого файлов. Возможна также подмена файлов, т.е. создается файл-двойник, которому передается при запуске управление вместо настоящего файла. Существуют вирусы, поражающие архивы и командные файлы.
3. Макровирусы, написанные на языке макрокоманд и исполняемые в среде какого-либо приложения, чаще всего Microsoft Office; заражают файлы-документы и электронные таблицы.
4. Сетевые вирусы.

Вирусы делятся по способам заражения на резидентные и нерезидентные. Резидентные вирусы находятся в памяти до выключения или перезагрузки. Нерезидентные вирусы являются активными только ограниченное время.

По деструктивным возможностям вирусы бывают:

1. безвредные, почти не влияющие на работу компьютера, они только занимают место на диске;
2. неопасные: занимают память и сопровождаются графическими и звуковыми эффектами;
3. опасные: приводят к сбоям в работе;
4. очень опасные: могут вызвать потерю программ и данных.

Сетевой червь – еще одна разновидность вредоносного ПО – распространяется по сетевым каналам, способен к преодолению систем защиты компьютерных сетей и к созданию и распространению своих копий. По типам используемых протоколов черви делятся на следующие типы:

1. Сетевые черви используют для распространения протоколы Интернет и локальных сетей, чаще TCP/IP. Сетевые черви могут активироваться и без непосредственного участия пользователя (запуска), им бывает достаточно просто приникнуть в компьютер.
2. Пакетные черви попадают на компьютер в виде сетевых пакетов и отыскивает в оперативной памяти конфиденциальную информацию. После перезагрузки системы следы сетевого червя обнаружить нельзя.
3. Почтовые черви распространяются в формате сообщений электронной почты.
4. IRC-черви распространяются по каналам IRC (Internet Relay Chat, протокол для коммуникации пользователей в режиме реального времени).
5. P2P-черви распространяются через файлообменные сети.
6. IM-черви распространяются через системы мгновенного обмена сообщениями (ICQ и др.); часто они распространяют ссылки на зараженные страницы.

Троянские кони (программы) в отличие от собственно вирусов не создают копии. Трояны могут маскироваться под какое-либо приложение (например, под антивирус) и активироваться при его запуске; могут они проникать в компьютер вместе с вирусами. Разновидности троянских программ:

1. Шпионы: могут, например, следить за клавиатурой, чтобы узнавать пароли и передавать их злоумышленнику.

2. Похитители паролей из файлов, в которых они хранятся.
3. Утилиты для скрытого удаленного управления компьютером (утилиты скрытого администрирования).
4. Люки для ограниченного управления компьютером пользователя, обычно для запуска файлов.
5. Анонимные smtp-серверы для рассылок спама.
6. Логические бомбы: срабатывают в определенный момент и выполняют вредоносные действия.
7. Модификаторы настроек браузера.
8. Программы для несанкционированной загрузки на компьютер из сети новых версий вирусов.

Отдельная категория – упаковщики. Они архивируют содержимое файла так, что потом корректное разархивирование невозможно.

Как черви, так и вирусы могут вызывать следующие проблемы:

1. Перегрузка каналов связи за счет передачи по Интернету огромных объемов запросов, зараженных писем. Во время таких эпидемий возникают проблемы при пользовании Интернетом.
2. DDoS-атаки: зараженные системы начинают массово обращаться к какому-либо ресурсу, что вызывает отказ в обслуживании и ресурс становится недоступен.
3. Уничтожение данных на компьютере, выбранных по определенному признаку или случайным образом.
4. Нарушение работы приложений; например, могут начаться перезагрузки компьютера
5. Снижение производительности работы приложений или системы в целом за счет загрузки ресурсов компьютера вредоносными программами

Вредоносные утилиты не представляют опасности для компьютера, но могут выполнять следующие действия:

1. Конструкторы служат для создания новых вирусов, червей и троянских программ.

2. DoS: отправляют компьютеру-жертве многочисленные запросы, что вызывает при недостаточности ресурсов отказ в обслуживании
3. Программы-флудеры заполняют каналы электронной почты, каналы передачи текстовых сообщений, каналы систем мгновенного обмена сообщениями и др. бесполезными сообщениями.
4. Программы, предупреждающие о несуществующих угрозах.
5. Программы для подмены адреса отправителя сообщения или сетевого ресурса и др. утилиты.

Существуют программы, не являющиеся вредоносными, но в ряде случаев могущие представлять опасность. По классификации Лаборатории Касперского это:

1. Программы Adware для показа рекламы на компьютере, перенаправления запросов поиска на рекламные сайты и сбора маркетинговой информации о пользователе; часто устанавливаются без ведома пользователя.
2. Программы, отображающие порнографический контент; тоже часто устанавливаются без ведома пользователя.
3. Программы, которые могут причинить вред, если используются злоумышленниками: утилиты удаленного администрирования; программы дозвона; программы управления паролями; веб-службы вроде FTP, Telnet и др.; программы для загрузки файлов; программы для мониторинга активности компьютеров и т.п.

Наряду с вирусами опасность представляют программные закладки, т.е. скрытно внедренные в систему программы, позволяющие злоумышленнику осуществлять несанкционированный доступ к ресурсам системы за счет изменения свойств защиты. Программные закладки могут перехватывать пароли, трафик, способствуют проникновению компьютерных вирусов; при этом они не обнаруживаются стандартными антивирусными средствами. По способу внедрения программные закладки бывают:

1. программно-аппаратные, располагаются в основном в BIOS;
2. загрузочные, связанные с программами начальной загрузки;

3. драйверные, связаны с драйверами периферийных устройств;
4. прикладные, связаны с прикладным ПО;
5. исполняемые, связаны с программными модулями;
6. имитаторы интерфейса служебных программ; исполнение предполагает ввод конфиденциальной информации;
7. закладки, замаскированные под программы для оптимизации работы ПК, компьютерных игр и т.п.

Существуют также информационные процессы, не являющиеся вирусами, но имеющие вредоносные последствия – спам (массовая рассылка электронной почты, вызывающая загрузку сети) и фишинг (попытки получить персональные данные пользователей).

Как защититься от вирусов? Здесь уместно вспомнить все правила безопасной работы с ПК и Интернетом:

Пользуйтесь своевременно обновляемым легальным антивирусным ПО.

Периодически выполняйте полную проверку компьютера на вирусы.

Всегда проверяйте переносные устройства хранения информации перед тем как их открыть.

Будьте внимательны при переходе по ссылкам в Интернете, особенно на незнакомые ресурсы.

Никогда не запускайте никаких предложенных вам программ.

Периодически выполняйте резервное копирование важной информации.

4) **Закрепление изученного материала**

Опрос:

1) назовите основные виды вредоносного ПО

2) назовите несколько антивирусных программ

5) **Закрепление итогов урока**

Информация о домашнем задании

Сегодня мы рассмотрели несколько видов классификации вредоносного ПО. Необходимо постоянно следить за безопасностью вашего компьютера, чтобы максимально возможно обеспечить защиту данных. Дома найдите схемы

классификации вредоносного ПО. Составьте отчет-презентацию о проделанной работе с результатами поиска.

### 4.9. 10 класс. Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo)

**Информатика:** Базы данных.

**Тематическое планирование:** Основа информационных систем. Виды моделей данных, используемых в БД. Реляционная модель данных. СУБД. Структура записей (имена и типы полей, главные ключи) для БД.

При изучении баз данных добавляется тема и правовой охране БД.

**Цель**: знакомство с основами правовой охраны программ для ЭВМ и БД

**Задачи:**

**образовательные:**

познакомить законодательными аспектами охраны программ и данных

выяснить степень осведомленности учащихся о коммерческом и бесплатном ПО

**развивающие:**

способствовать формированию информационной культуры учащихся

**воспитательные:**

воспитывать ответственное отношение к авторскому праву

*Знания:*

основные понятия об авторском праве и правовой защите программ

*Умения:*

находить данные о правовых аспектах защиты информации и киберпространства

*Навыки:*

поиск информации в Интернете

**Тип урока**: урок изучения нового материала.

**Методы и формы обучения:** словесный (рассказ), видеометод, наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

**Программно-дидактическое обеспечение:** презентация «Правовая охрана программ для ЭВМ и БД»

**Используемая литература и web-ресурсы**:


11. Угринович Н.Д. Информатика и ИКТ. 10 класс. – М.: БИНОМ. Лаборатория знаний, 2012.
12. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/__12697.pdf


**Этапы урока:**

1) Постановка цели урока и актуализация знаний (2 мин).

2) Изучение нового материала (7 мин).

Объяснение нового материала.

Просмотр презентации.

3) Практическая работа (2 мин).

Поиск информации в сети Интернет.

Обсуждение найденного материала.

4) Закрепление изученного материала (1 мин).

Информация о домашнем задании.

**Технические средства:** проектор, компьютеры.

**Ход урока**

1) **Постановка цели урока**.

**Деятельность учителя**: Базой данных является совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы

могли быть найдены и обработаны с помощью ЭВМ. Сейчас мы работали с БД Microsoft ACCESS. Это проприетарное ПО, для его использования необходимо приобрести лицензию. Однако все вы слышали о таких понятиях как плагиат, крак, пиратство, ломаная программа и т.п. Все это незаконные виды деятельности, связанные с нарушением авторских прав. У всех книг, фильмов, музыки, программ и устройств есть авторы (изобретатели). Поэтому, если сами авторы не решат предоставить свои произведения в свободное пользование, данные произведения являются интеллектуальной собственностью автора и как всякая собственность охраняются законом.

**Актуализация знаний**

Вспомните, с какими видами нарушения авторских прав вам приходилось встречаться.

**Деятельность учащихся**: вспомнить примеры нарушения авторских прав.

2) **Изучение нового материала**

**Деятельность учащихся**: Просмотр презентации «Правовая охрана программ для ЭВМ и БД».

**Деятельность учителя** (пояснения при просмотре презентации): Основные угрозы безопасности информации – это утечки, потеря целостности, нарушение работоспособности системы и незаконное тиражирование (воспроизведение). Последнее чаще всего связано с нарушениями авторских прав.

Законы, связанные с охраной программ для ЭВМ и баз данных, изложены в части IV ГК РФ. Программы защищаются законом об авторском праве, а базы данных, кроме того, законом о правах, смежных с авторскими. Авторско-правовая охрана программ и БД в нашей стране базируется на международных нормативных актах, связанных с защитой авторского права. В соответствии с Договором Всемирной Организации Интеллектуальной Собственности (ВОИС) по авторскому праву (вступил в силу в 2002 г.) по Статье 4 «Компьютерные программы» программы для ЭВМ охраняются как литературные произведения, а по Статье 5 «Компиляция данных (базы данных)» компиляции данных в любой форме, которые по подбору и расположению данных являются результатом

творчества, охраняются как таковые (такая охрана не распространяется на сами данные).

Источниками авторско-правовой охраны программ и БД являются:

1. Конституция РФ, в ст. 44 которой гарантируется свобода творчества; указано также, что интеллектуальная собственность охраняется законом.
2. Гражданский кодекс РФ, Часть 4, Раздел VII, статьи с 1225-1551, всего 327 статей - «Права на результаты интеллектуальной деятельности и средства индивидуализации».

По статье 1225 «Охраняемые результаты интеллектуальной деятельности и средства индивидуализации» результатами интеллектуальной деятельности, которым предоставляется правовая охрана (интеллектуальной собственностью), являются, среди прочих объектов, программы для ЭВМ и базы данных.

В соответствии со ст. 1225-1551 интеллектуальной собственностью являются результаты интеллектуальной деятельности (РИД), на которые возникают интеллектуальные права:

1. Имущественное право: автора или иной правообладатель вправе использовать РИД любым способом (п. 1 ст. 1229 ГК РФ)
2. Личные неимущественные права авторов произведений (моральная составляющая авторских прав): право авторства, право на защиту репутации, право на имя, право на неприкосновенность произведения, право на обнародование произведения
3. Иные права: право на отзыв произведения, право автора на долю доходов от перепродажи произведения (право следования), право доступа

Для предоставления программе или БД авторско-правовой охраны необходимо и достаточно, чтобы они были оригинальными, т.е. не были заимствованием известных ранее программ или БД. Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей. В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя.

По ст. 1260 авторско-правовая охрана предоставляется базе данных как составному произведению; авторско-правовая охрана БД признается не в отношении содержания (контента), а в отношении подбора или расположения включенных в БД материалов. По ст. 1304 смежные с авторскими права обеспечивают правовую охрану от несанкционированного и повторного использования составляющих базу данных материалов.

Автор может передать права на использование своего произведения по лицензионному договору.

Статья 1273. Свободное воспроизведение произведения в личных целях

1. Допускается без согласия автора и без выплаты вознаграждения воспроизведение гражданином при необходимости и исключительно в личных целях правомерно обнародованного произведения, за исключением:

1) воспроизведения баз данных или их существенных частей;

2) воспроизведения программ для ЭВМ, кроме случаев, предусмотренных статьей 1280 настоящего Кодекса.

Статья 1280. Свободное воспроизведение программ для ЭВМ и баз данных. Декомпилирование программ для ЭВМ

1. Лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных (пользователь), вправе без разрешения автора или иного правообладателя и без выплаты дополнительного вознаграждения:

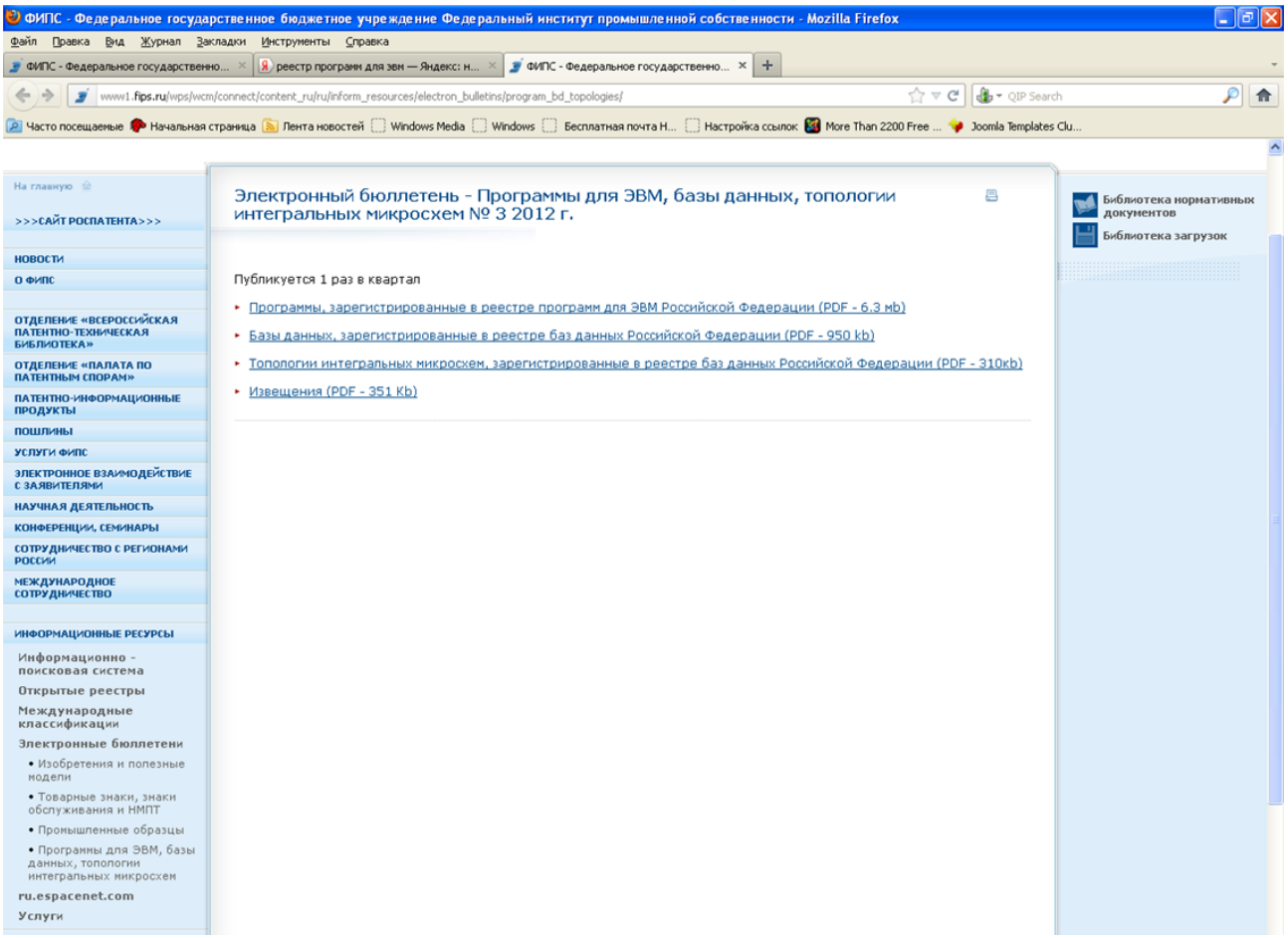
1) внести в программу для ЭВМ или базу данных изменения, необходимые для функционирования таких программы или базы;

2) изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования.

2. Пользователь программы для ЭВМ вправе без согласия правообладателя и без выплаты дополнительного вознаграждения изучать, исследовать или испытывать функционирование такой программы в целях определения идей и принципов, лежащих в основе любого элемента программы.

3. Пользователь вправе без согласия правообладателя и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ), если это необходимо для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой.

На сайте ФИПС (Федерального института промышленной собственности) публикуется Электронный бюллетень «Программы для ЭВМ, базы данных, топологии интегральных микросхем:




Приобретение программного продукта - это приобретение лицензии (права) на его использование. Для каждой используемой программы необходима лицензия.

Когда пользователь приобретает ПО, то, в отличие от других товаров, он не обладает неограниченными полномочиями по его дальнейшему владению, использованию и распоряжению.

Схемы лицензирования программного обеспечения:

1. OEM. Предустановленное программное обеспечение. Original Equipment Manufacturer – наиболее дешевый вариант приобретения лицензии. Программное обеспечение должны быть куплено в составе компьютера или сервера и может быть использовано только совместно с ним.
2. Full Package Product (FPP). Коробочные продукты, пакетное лицензирование. Применяется частными лицами или малым бизнесом (до 5 персональных компьютеров). Правило лицензирования: 1 компьютер - 1 коробка.

Коробочные и OEM-лицензии содержат «Лицензионное Соглашение Конечного Пользователя» (EULA - End User License Agreement), где фиксируются условия лицензии. Оно может поставляться в бумажном или в электронном виде с дистрибутивом программы. Устанавливая программу на устройство, пользователь автоматически соглашается с условиями EULA.

3. Volume Licensing. Корпоративные лицензии. Для компаний, которым необходимо приобрести большое количество лицензий, допускается приобрести одну именную лицензию (документ, в котором содержится информация о заказе: покупатель, перечень программного обеспечения, ключи для инсталляции ПО). Компания может получить скидки за объем заказа, расширенную техническую поддержку и т.п.
4. Subscription. Подписка. Оплачиваются ежегодные платежи, при этом каждый год можно менять количество лицензий на различные продукты. Преимуществом подписки являются низкие единовременные затраты.

Почти у всех производителей программного обеспечения есть специальные цены для лицензирования государственных и образовательных учреждений. Целью таких акций является привлечение будущих клиентов из числа нынешних учащихся. Примером является программа университетской подписки Microsoft

Developer Network Academic Alliance (MSDN AA), в рамках которой предоставляется бесплатное ПО преподавателям и студентам. Программное обеспечение, полученное в рамках подписки MSDN Academic Alliance, может быть использовано только в некоммерческих - научно-исследовательских и учебных целях.

Программное обеспечение может распространяться на условии открытого кода (OpenWare), или же без такого условия. При распространении ПО на условиях открытого кода правообладатель передает пользователю также исходные коды программы. Пользователю может предоставляться право модифицировать исходные тексты в целях их переработки и совершенствования. Последующее использование полученных в результате такой переработки программных продуктов различается в зависимости от вида лицензии. Условие OpenWare не означает бесплатности ПО. Наиболее распространенные группы типовых лицензий на передачу программного обеспечения с открытым кодом:

1) GNU GPL (General Public License) – все программные продукты, полученные в результате переработки или модернизации распространяемого на таких условиях программного кода, также могут распространяться далее только на условиях GNU GPL.

2) FreeBSD (лицензия университета Беркли) – программные продукты, полученные в результате переработки предоставленного программного кода, могут распространяться на любых условиях, в том числе и на возмездной основе.

Лицензии на распространение ПО, не содержащие условия об открытости исходных кодов, более разнообразны, однако практически во всех таких лицензиях содержится запрет на любую модификацию программного кода.

Виды лицензирования можно также различать по условию возмездности:

1. Бесплатное программное обеспечение (FreeWare). Разновидности бесплатного ПО: Free (бесплатное использование и распространение с запретом на внесение изменений в код), Free GPL (с возможностью изменения кода), Adware

(бесплатная программа с дополнительными компонентами, например, с рекламой).

2. условно-бесплатное ПО: пользователь получает возможность бесплатно использовать программу в течение ограниченного времени (Trial) или предоставляется функционально ограниченная версия программы (Shareware). Еще один вариант Demoware – демоверсия (ПО не имеет функциональных и временных ограничений, но ограничения накладываются на результат, например, его нельзя сохранять; ограничения снимаются при оплате ПО).

3. Коммерческое ПО: пользователь должен оплатить программный продукт, причем ему предоставляется значительно больший объем гарантий и обязательств правообладателя, чем в лицензиях на бесплатные или условно-бесплатные программы.

Лицензионные права различаются для разных категорий продуктов:

1. Персональные операционные системы, настольные приложения, игры, мультимедийные программы лицензируются по принципу одна лицензия на один компьютер.
2. Средства разработки лицензируются по принципу одна лицензия для одного физического лица.
3. Серверные продукты используют две схемы лицензирования: лицензирование сервер/клиент (серверная лицензия для установки на сервер плюс клиентские лицензии для устройств или пользователей, обращающихся к службам сервера) и лицензирование на процессор (процессорная лицензия для каждого процессора сервера).

Схемы лицензирования ПО могут существенно различаться у разных производителей. С развитием компьютерного оборудования и программного обеспечения усложняются схемы лицензирования. Наиболее известные компании–разработчики программных средств управления лицензиями: Agilis Software, IBM, IntraWare, Macrovision, SafeNet и др.

Примеры бесплатного программного обеспечения (FreeWare): аудиоплеер AIMP 3.60 Build 1479, функциональный офисный пакет для устройств на Android WPS Office 6.5.2, видеоредактор для создания и редактирования видеоклипов VSDC 2.3.1 и т.д.

Примеры условно-бесплатного ПО: программа для создания PDF-документов PDF Maker Pilot; программа для генерирования устойчивых к подбору паролей и их защищенного хранения на ПК Password Manager 3.81; программа для записи видео роликов с экрана компьютера LiteCam HD 5.0.0.5 и др.

Примеры коммерческого ПО: это практически все наиболее известные и используемые программные продукты - Антивирусное ПО Лаборатории Касперского, офисные пакеты Microsoft Office, операционные системы семейства Windows и т.д.

Как следует действовать в Интернете, чтобы избежать нарушения авторских прав?

1. При скачивании контента выясните, разрешается ли его распространять бесплатно. Платный контент можно приобрести, в том числе, в официальных интернет-магазинах.

2. При приобретении контента на дисках и других носителях проверяйте защищенность упаковки, наличие голограмм и информации о производителе и издателе.

3. Прежде чем совершить покупку, узнайте по возможности больше информации об авторах и производителях продукта, об официальных распространителях продукции, о рекомендуемых ценах. Если вам предлагают продукт по цене значительной меньше установленной, то вероятнее всего вы имеете дело с мошенниками, незаконно продающими авторскую продукцию без ведома правообладателя. Не позволяйте вовлечь себя в противоправную деятельность.

4. Уважайте труд авторов и не поощряйте преступные действия.

3) **Практическая работа**

**Деятельность учителя**: Найдите в Интернете предложения о скачивании какого-либо программного продукта. Узнайте, разрешено ли бесплатное распространение этого продукта.

**Деятельность учащихся**: поиск и анализ информации в соответствии с заданием

4) **Закрепление изученного материала**

Опрос:

1) назовите известные вам виды нарушения авторских прав на ПО и БД;

2) назовите несколько способов защиты от незаконного скачивания.

Сегодня мы рассмотрели правовые основы охраны ПО и БД. Защита контента от незаконного тиражирования и воспроизведения – один из важных аспектов безопасности. Дома найдите примеры предложений о незаконном распространении известных программных продуктов. Составьте отчет о проделанной работе со скриншотами результатов поиска.

### 4.10. 11 класс. Настройки безопасности веб-браузеров (фильтры для ограничения потенциально опасного содержимого). Настройки безопасности веб-браузеров (Internet Explorer, Firefox и т.п.)

**Информатика:** Wordl Wide Web – Всемирная паутина.

**Тематическое планирование**: Что такое WWW. Веб-страница, Веб-сервер, протокол передачи гипертекста, браузер. Поисковая служба Интернета. Поисковые каталоги и указатели.

При изучении браузера добавляется тема о настройках безопасности.

**Цель**: знакомство с  настройками безопасности веб-браузеров

**Задачи:**

**образовательные:**

познакомить с приемами защиты в поисковых системах

выяснить степень осведомленности учащихся о фильтрах для ограничения потенциально опасного содержимого

**развивающие:**

способствовать формированию информационной культуры учащихся

**воспитательные:**

воспитывать ответственное отношение к работе в Интернете

*Знания:*

основные понятия о фильтрах для ограничения потенциально опасного содержимого

*Умения:*

находить сведения о настройках безопасности веб-браузеров

*Навыки:*

работа с браузером

**Тип урока**: урок изучения нового материала.

**Методы и формы обучения:** словесный (рассказ), видеометод, наглядный (демонстрация), практический; интерактивная форма обучения (обмен мнениями, информацией), опрос.

**Программно-дидактическое обеспечение:** презентация «Настройки безопасности веб-браузеров»

**Используемая литература и web-ресурсы**:

13. Угринович Н.Д. Информатика и ИКТ. 11 класс. – М.: БИНОМ. Лаборатория знаний, 2011.
14. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/__12697.pdf

**Этапы урока:**

1) Постановка цели урока и актуализация знаний (2 мин).

2) Изучение нового материала (5 мин).

Объяснение нового материала.

Просмотр презентации.

3) Практическая работа (2 мин).

Поиск информации в сети Интернет.

Обсуждение найденного материала.

4) Закрепление изученного материала (1 мин).

Опрос.

Информация о домашнем задании.

**Технические средства:** проектор, компьютеры.

**Ход урока**

1) **Постановка цели урока**.

**Деятельность учителя**: Мы уже много раз говорили об угрозах информационной безопасности, существующих в Интернете. Сегодня наша цель – рассмотреть несколько способов защиты от этих угроз.

**Актуализация знаний**

Приведите примеры путей распространения вредоносного ПО.

**Деятельность учащихся**: вспомнить основные пути распространения вирусов.

3) **Изучение нового материала**

**Деятельность учащихся**: Просмотр презентации «Настройки безопасности веб-браузеров».

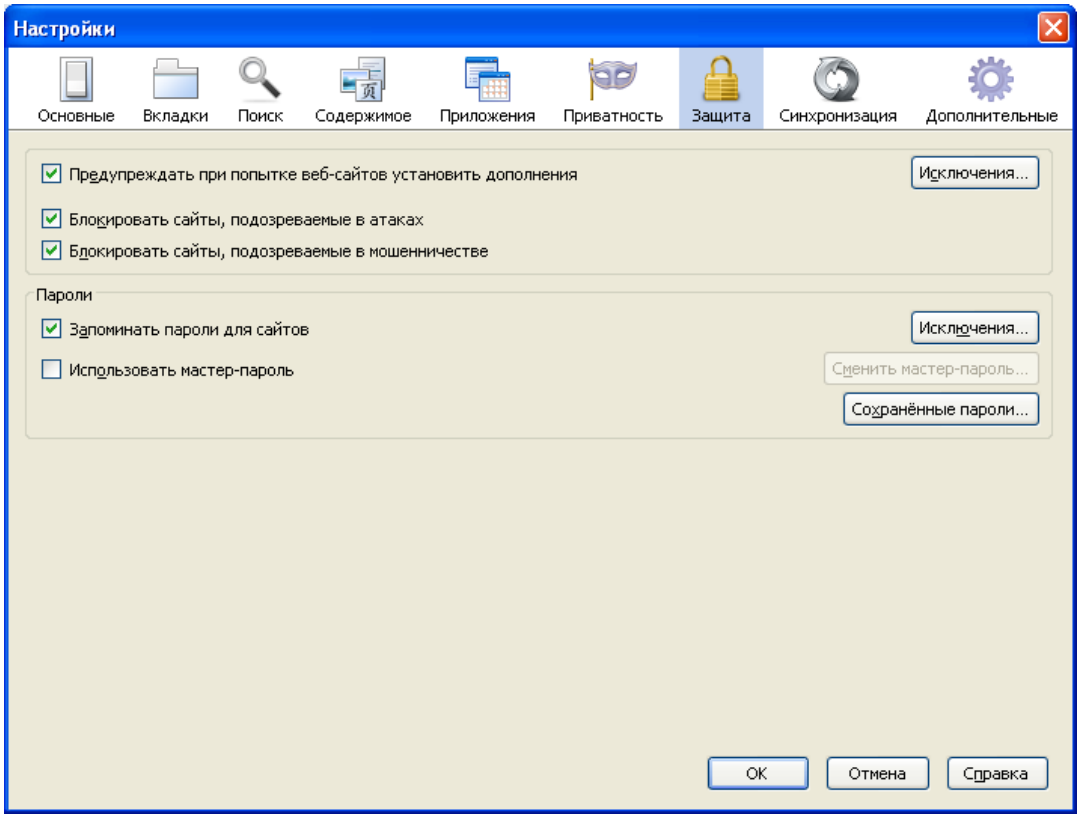
**Деятельность учителя** (пояснения при просмотре презентации): Вредоносное ПО предназначено для несанкционированного использования ресурсов ПК, для нейтрализации средств защиты или несанкционированного доступа к данным для их копирования, изменения, подмены или уничтожения.

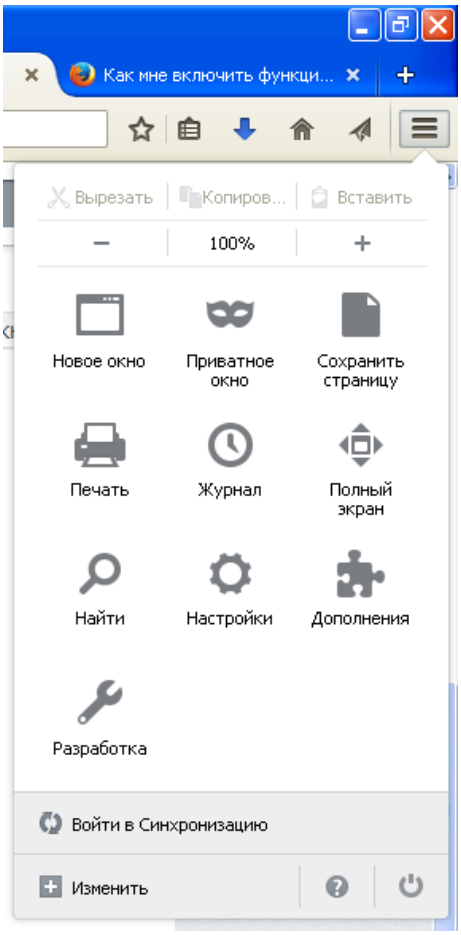
Вредоносное ПО, в том числе вирусы, нарушает конфиденциальность, целостность и доступность информации. Значительная часть вирусов распространяется через сетевые технологии (сетевые, пакетные, почтовые черви и др.). Их легко «подхватить», работая в Интернете. Конечно, необходимо выполнять пра-

вила безопасной работы и применять антивирусное ПО, но вредоносное ПО постоянно совершенствуется, и, кроме того, нельзя исключить случайных ошибок в работе (например, можно случайно перейти по вредоносной ссылке).

Поэтому не следует пренебрегать возможностью защиты браузера, с которым вы постоянно работаете. Для этого существует система настроек безопасности (на примере Firefox).

Браузер может предотвратить установку дополнений для браузера (Настройки – Защита). Там же можно установить блокирование сайтов, подозреваемых в атаках и мошеннических действиях (например, фишинге):





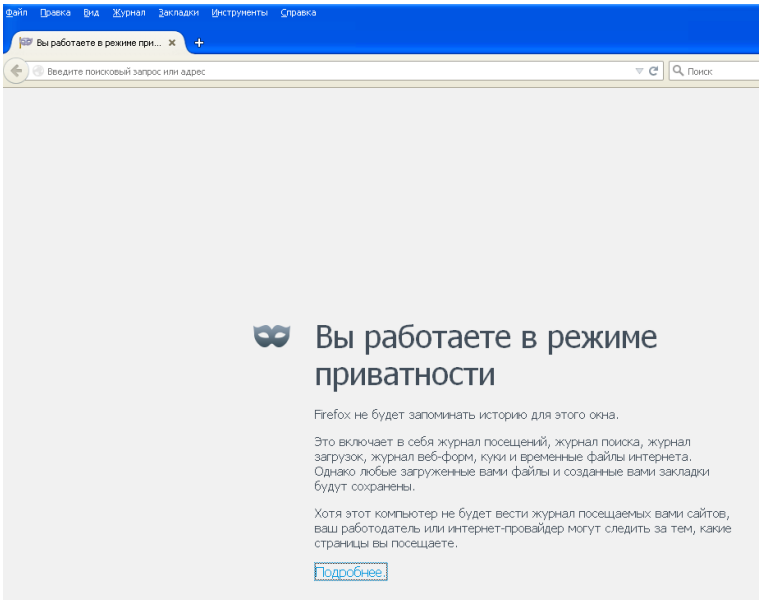

Можно также задать правила управления паролями. Для упрощения входа на сайты, требующие пароли, Firefox может эти пароли сохранять. Но можно и отключить эту возможность, сняв флажок «Запоминать пароли для сайтов».

Если задать опцию «Использовать мастер-пароль», браузер защитит личную информацию пользователя (например, сохранённые пароли и сертификаты) с помощью их шифрования. После этого доступ к сохранённым данным будет возможен только по паролю.

Пароли можно удалять через кнопку «Сохраненные пароли».

Если вам не хотелось бы, чтобы посторонние узнали историю ваших посещений, которая сохраняется браузером, можно пользоваться возможностями режима приватного просмотра. Для этого в меню надо выбрать Приватное окно:

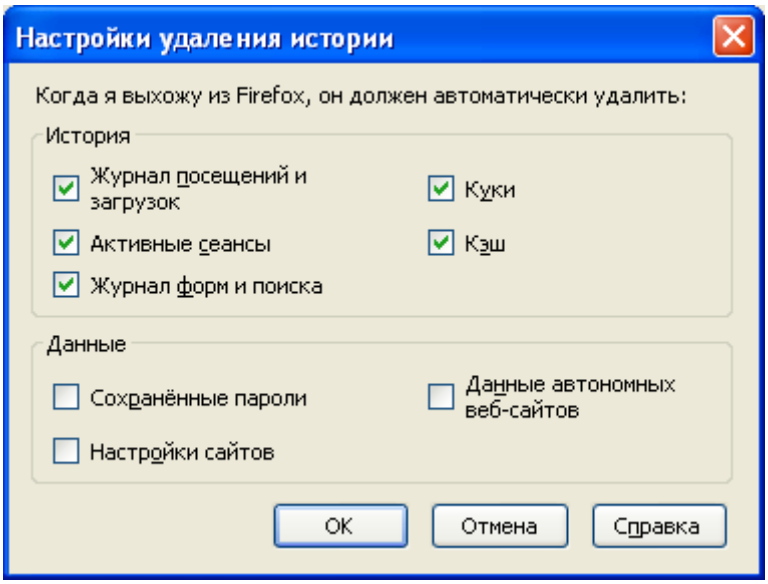
Тогда откроется новое окно с характеристиками приватного просмотра:



Куки (cookie) – это информация, оставляемая веб-сайтом на компьютере пользователя. Куки способны хранить данные для аутентификации пользователя, персональные данные (если они представлены самим пользователем), сведения о предпочтениях пользователя (используются веб-сервером для улучшения обслуживания), статистическую информацию и т.д. Браузер при обращении к сайту пересылает куки веб-серверу в составе HTTP-запроса. Куки дают определенные удобства при постоянной работе с одними и теми же ресурсами (например, чтобы не вводить постоянно имя и пароль). Куки требуются не всем сайтам, обычно они нужны сайтам с ограничением доступа. Существуют куки от сторонних сайтов, присылаемые тогда, когда на текущем сайте находятся ссылки на другие ресурсы (например, в виде кнопок «понравилось»). Такие сторонние куки могут использоваться рекламодателями.

Сами по себе куки безопасны, но могут служить источником информации о пользователе.

Большинство браузеров позволяет отключать куки (изначально они включены). Например, в Firefox их можно отключить по Инструменты – Настройки – Приватность – Принимать куки с сайтов:




Можно задать разный период хранения куки:

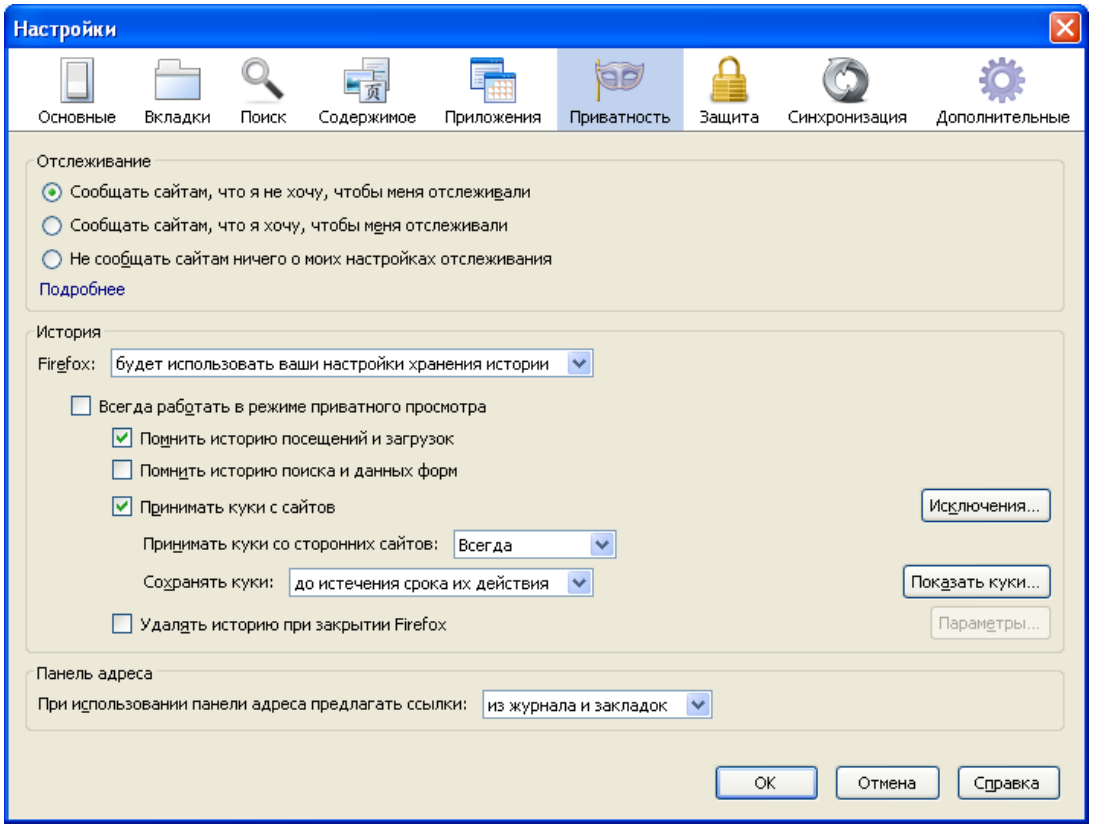
1. до истечения срока их действия

2. до закрытия браузера
3. каждый раз, когда сайт будет присылать куки, браузер будет спрашивать, сохранять ли их

Можно запретить принимать куки со сторонних сайтов.

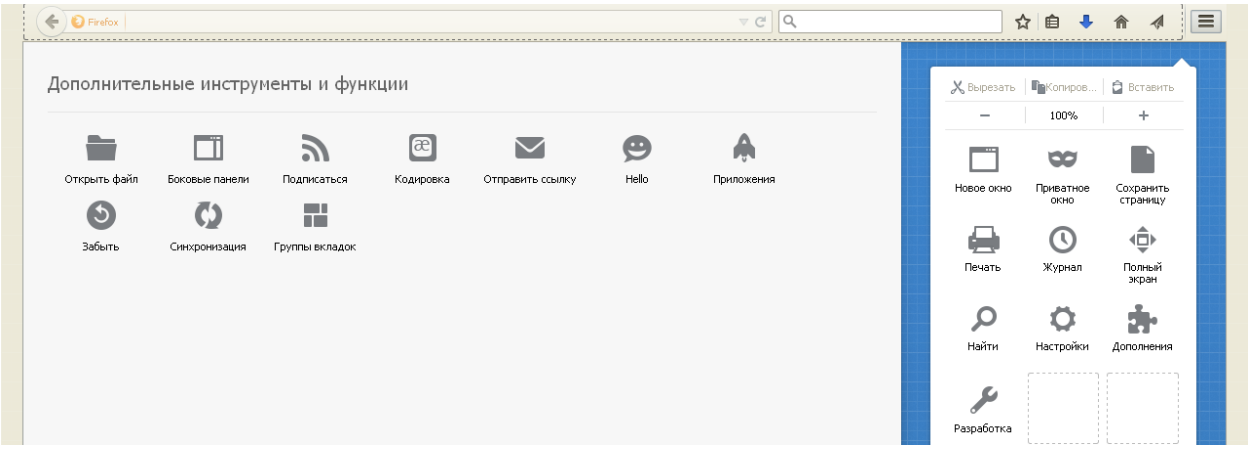
Установки отслеживания в этом же окне позволяют запретить или разрешить сайтам, которые вы посещаете, следить за вами. Эти сайты следят за вашими посещениями, предпочтениями, покупками, а затем могут продать все эти сведения, например, рекламодателям.

Установки История, помимо установок для куки, позволяют управлять журналами посещений и форм (т.е. форм, заполненных при работе через браузер). Если установить «Удалять историю при закрытии Firefox», то с помощью вкладки «Параметры» можно задать настройки удаления истории:



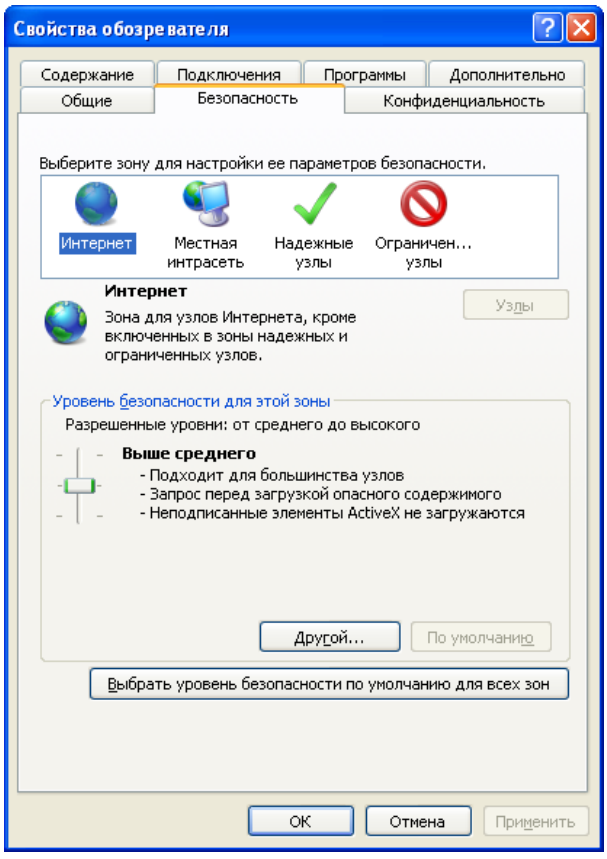

Очистить журнал посещений полностью или частично можно через Меню, пункт Журнал.

Доступ к дополнительным возможностям по управлению безопасностью можно получить через Меню – Изменить (+):

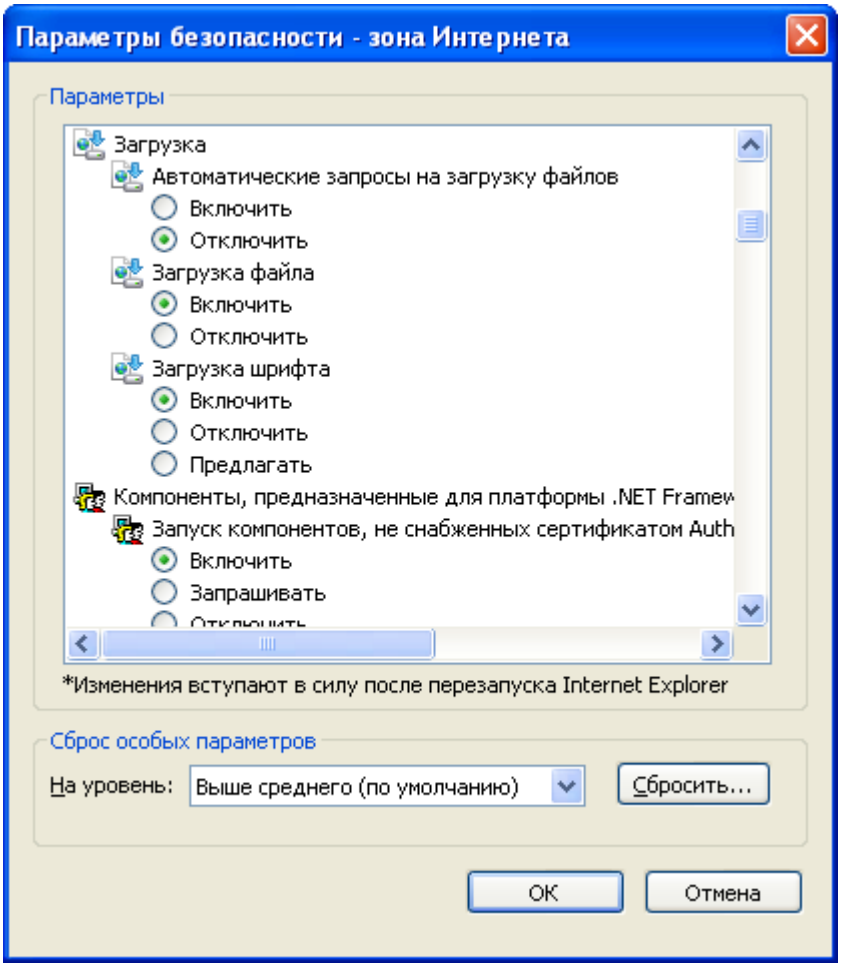



Если, например, перетащить кнопку Забыть из панели «Дополнительные инструменты» на панель инструментов и выйти из настроек, то эта кнопка появится там и ее можно будет использовать для того, чтобы удалить историю посещений и куки за указанный период.

В Internet Explorer Сервис – Свойства обозревателя – Безопасность можно управлять уровнем безопасности с помощью ползунка (от среднего до высокого)




Кнопка «Другой» позволяет устанавливать каждый параметр отдельно:




В каждом браузере имеются свои настройки безопасности. Их обязательно нужно изучить и использовать.

При работе в интернете, помимо уже известных правил безопасной работы, рекомендуется выполнять следующие требования:

1. Своевременно обновляйте браузеры (лучше всего автоматически)
2. Устанавливайте необходимые настройки безопасности браузера
3. Не разрешайте браузеру сохранять пароли
4. При работе в браузере за чужим ПК пользуйтесь режимом приватного просмотра

3) **Практическая работа**

**Деятельность учителя**: Найдите в справке браузера информацию о настройках безопасности. Узнайте, как протестировать защиту от фишингового сайта в Firefox.

**Деятельность учащихся**: поиск и анализ информации в соответствии с заданием

4) **Закрепление изученного материала**

Опрос:

1) назовите основные пути распространения вредоносного ПО

2) назовите известные вам браузеры

3) перечислите основные установки безопасности браузера

Информация о домашнем задании

Сегодня мы рассмотрели основные настройки безопасности браузера. Необходимо постоянно следить за всеми настройками безопасности вашего компьютера. Дома проверьте установки безопасности вашего браузера. Составьте отчет о проделанной работе со скриншотами.