**Факультативный курс: «Защита компьютера и компьютерных сетей» для старших классов средней школы (возможно применение и в ВУЗе)**

**Разрабатывал курс: Бухонин Иван Игоревич Студент III курса Факультета Информационных Технологий, Специальности Информатика (образовательная) группа Ин(о)-10;**

**Руководила и правила: Старший преподаватель Кольева Наталья Станиславовна**

**ТЕМА: Антивирусные программы и их использование**

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания о видах компьютерных вирусов, путях их распространения, об антивирусных программах и способах их использования на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Понятие компьютерного вируса.
- Основные типы компьютерных вирусов.
- Действие программного вируса.
- Методы реализации антивирусной защиты.
- Способы антивирусной защиты.
- Виды антивирусных программ.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с антивирусной программой.

**Оснащение и методическое обеспечение урока:**

- компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (демонстрация учебного материала, опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа.

ПЛАН УРОКА

| Ход занятия | Методы работы | Содержание | Время |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по видам программного обеспечения. | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br><br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br><br>10 |
| 4. Этап применения знаний | 4 | Практическая работа с антивирусной программой. | 10 |
| 5. Этап проверки знаний | 4 | Тестирование (электронный тест). | 7 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

**Компьютерные вирусы**

**Компьютерный вирус** – это программный код, встроенный в другую программу, или в документ, или в определенные области носителя данных и предназначенный для несанкционированных действий на компьютере.

**1. Основные типы компьютерных вирусов:**

| **Программные** | **Загрузочные** | **Макровирусы** |
|---|---|---|
| **Это блоки программного кода, внедренные внутрь других прикладных программ.** Вирусный код запускается при запуске программы. | **Поражают системные области магнитных носителей (гибких и жестких дисков).** Заражение происходит при загрузке ПК с | **Поражают документы, выполненные в некоторых прикладных программах (например, Word).** Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд |

зараженного носителя. (макросов).

**2. Этапы действия вируса:**

**Размножение** – вирусный код может воспроизводить себя в теле других программ.

**Вирусная атака** – после создания достаточного числа копий программный вирус начинает осуществлять разрушение: нарушение работы программ и ОС, удаление информации на жестком диске, самые разрушительные вирусы вызывают форматирование жесткого диска. Некоторые вирусы могут уничтожать данные, в этом случае требуется замена микросхемы (хотя считается, что никакой вирус не в состоянии вывести из строя аппаратное обеспечение ПК).

**3. Защита от компьютерных вирусов**

Существуют три рубежа защиты:

- предотвращение поступления вирусов;
- предотвращение вирусной атаки, если вирус поступил на ПК;
- предотвращение разрушительных последствий, если атака произошла.

**4. Методы реализации защиты**

- Программные
- Аппаратные
- Организационные

**5. Средства антивирусной защиты:**

- **Основное средство** – резервное копирование наиболее ценных данных. В случае утраты информации жесткие диски форматируют, устанавливают ОС с дистрибутивного CD-диска и все необходимые программы, а данные – с резервного носителя (который должен храниться отдельно от ПК). Все регистрационные и парольные данные для доступа в Интернет рекомендуется хранить не на ПК, а в служебном дневнике в сейфе.
- **Вспомогательные средства** – это антивирусные программы и аппаратные средства.
- **Аппаратное средство:** отключение перемычки на материнской плате не позволит осуществить стирание микросхемы BIOS ни вирусу, ни злоумышленнику, ни неаккуратному пользователю.
- **Антивирусная программа** сравнивает коды программ с известными ей вирусами, которые хранятся в ее базе данных. Обновление базы – 2 раза в месяц (не реже 1 раза в 3 месяца).

**6. Антивирусные программы**

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные программы, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными. Антивирусная программа сравнивает коды программ с известными ей

вирусами, которые хранятся в ее базе данных. Обновление базы – 2 раза в месяц (не реже 1 раза в 3 месяца).

Вот некоторые из них:

- **Антивирус Dr.Web** — Антивирус, который предоставляет надежную защиту компьютера от различного вида вирусных угроз. Антивирус Dr.Web может проверить всю память Windows даже на зараженном компьютере и способен остановить вирусный процесс. Уникальная эвристическая технология, используемая в антивирусе Dr.Web, позволяет обнаруживать новые вирусы и модификации вирусов, описаний которых еще нет в вирусной базе.
- **Антивирус Касперского** — это решение для базовой защиты компьютера от вредоносных программ. Продукт обеспечивает защиту в режиме реального времени от основных информационных угроз — как известных, так и новых.
- **Avast! Free Antivirus, ESET NOD32 Antivirus, Avira Free Antivirus, и т.д.**

**Практическая работа**

**Антивирусная программа DrWeb**

1. Запустить программу (паучок в нижнем правом углу рабочего стола, в панели задач)
2. При подключении к сети интернет автоматически обновится, попробовать ручное обновление.
3. Ознакомиться с модулями программы.
4. Открыть сканер DrWeb и просканировать, например, диск D, то есть сделать выборочную проверку Локального диска D.
5. Запустить сканирование.
6. После окончания сканирования проанализировать результаты (вкладка Статистика).

**Вопросы на самоподготовку:**

1. Что такое компьютерный вирус?
2. Основные типы компьютерных вирусов.
3. Действие программного вируса (этапы).
4. Методы защиты.
5. Средства антивирусной защиты.
6. Примеры антивирусных программ.

**ТЕМА: Признаки заражения**

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания о признаках заражения системы и других ее компонентов компьютерными вирусами, об антивирусных программах и способах их использования на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Понятие компьютерного вируса.
- Основные типы компьютерных вирусов.
- Действие программного вируса.
- Методы реализации антивирусной защиты.
- Способы антивирусной защиты.
- Виды антивирусных программ.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с антивирусной программой.

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- Программное обеспечение: электронная лекция, антивирусная программа (Доктор Веб и т.п.);
- опорный конспект,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа.

ПЛАН УРОКА

| Ход занятия | Методы работы | Содержание | Время |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |

| | | | |
|---|---|---|---|
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br><br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br><br>15 |
| 4. Этап применения знаний | 4 | Практическая работа с файлом «напроверку» работоспособности антивируса, составление краткой характеристики знакомого антивируса | 5 |
| 5. Этап проверки знаний | 4 | Тестирование (электронный тест). | 7 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

## Компьютерные вирусы

### Признаки заражения

Признаков, что на компьютере функционирует какая-либо вредоносная программа, может быть много, и здесь мы рассмотрим основные. Но стоит отметить, что само наличие признаков заражения – уже большая удача, поскольку, заподозрив неладное, можно начать экстренную проверку ПК на вирусы и внеочередную архивацию важных данных. Гораздо хуже, когда вредоносная программа вообще никак себя не проявляет, ибо в этом случае пользователь не подозревает о ее существовании вплоть до момента ее срабатывания, а порой так и остается в неведении. В такой ситуации владелец ПК не знает о том, что его персональные данные уже похищены, а персональные счета обналичены злоумышленниками. К счастью, идеально скрыть деятельность программы очень трудно и, так или иначе, догадаться о наличии вредоносного ПО в системе можно. Ниже перечислены признаки заражения компьютера, сгруппированные по области их проявления.

***Со стороны операционной системы:***

1. Компьютер часто зависает.

2. ОС загружается медленнее, чем раньше.

3. Заметно снижается быстродействие ПК, приложения работают медленнее, игры «притормаживают».

4. Периодически возникают критические системные ошибки (BSOD).

5. Изменяется внешний вид окон и системных сообщений.

6. Возникают разнообразные сообщения, внешне схожие с системными, но содержащие шутки или бессмысленные наборы символов.

7. В центре экрана появляются баннеры рекламного или порнографического содержания, которые нельзя убрать. Зачастую баннер загораживает всю рабочую область монитора.

8. Операционная система перестает загружаться.

9. Невозможно загрузить Windows в безопасном режиме.

10. Невозможно открыть диск или какую-либо папку.

11. Изменились настройки рабочего стола, и вернуть их в прежнее состояние вручную не удается. Например, изменилось разрешение или цветовая гамма.

12. Появились неизвестные значки в области уведомлений.

13. Невозможно создать точку восстановления системы или архивировать данные с помощью встроенных средств резервного копирования.

14. Перестают запускаться системные утилиты, или выдается сообщение о нехватке прав для их запуска.

***Со стороны аппаратной части и периферии:***

1. Компьютер внезапно перезагружается, хотя скачков напряжения и команд на перезагрузку не было.

2. Встроенный динамик или колонки компьютера воспроизводят мелодии или странные звуки.

3. DVD-привод открывается и закрывается без запроса пользователя.

4. Клавиши на клавиатуре перестают соответствовать обычно производимым им действиям. Например, клавиша Пробел функционирует как Esc.

5. Индикатор жесткого диска горит, даже когда вы не выполняете на ПК никаких действий.

6. Резко сокращается количество свободного места на дисках.

7. Резко сокращается объем доступной оперативной памяти.

8. Принтер стал недоступным, или невозможно напечатать документы.

***Со стороны почты и Интернета:***

1. Проявляется сетевая активность, инициируемая процессами или приложениями, которые вы не запускали.

2. Брандмауэр сообщает о попытке проявить сетевую активность приложениями, которые вы не устанавливали.

3. Часто обрывается связь или существенно замедляется работа Интернет-соединений.

4. Электронные письма возвращаются с сообщением о невозможности доставки их адресату (обычно в строке Отправитель там значится Mailer-Daemon или Mail Delivery System, это может быть связано с блокированием инфицированного сообщения почтовыми серверами).

***Со стороны браузера:***

1. Перестают открываться все или некоторые интернет-сайты (как правило, первыми блокируются сайты обновления Windows и ресурсы по информационной безопасности).

2. Изменяются настройки браузера (зачастую обнуляются опции безопасности и подменяется домашняя страница). В окне браузера появляются посторонние элементы.

***Со стороны приложений:***

1. Папки или файлы изменяются без участия пользователя.

2. Перестает обновляться антивирус.

3. Отключаются или начинают работать с ошибками антивирус или брандмауэр.

4. Без участия пользователя запускаются или закрываются приложения.

5. В списке активных процессов появляются неизвестные процессы с непонятными названиями.

Если вы обнаружили что-либо из вышеперечисленного на своем ПК, это еще не гарантия, что компьютер инфицирован, поскольку проблемы могут быть вызваны множеством других факторов. В этом случае необходимо действовать в *двух направлениях*:

Установить антивирус, если это не было сделано ранее, для уже имеющегося, скачать последние обновления. После этого выполнить полную проверку компьютера на вирусы.

Исправить ошибки в установленном ПО и системные сбои – «замусоренный» реестр может быть виновником очень большого числа проблем. Проверьте работоспособность тех узлов, которые вызывают сбои, скачайте последние версии всех используемых программ, установите все обновления для своей версии Windows.

Проверить работоспособность аппаратной части ПК – неисправность модулей оперативной памяти, жесткого диска и других компонентов может непредсказуемо влиять на поведение системы.

**Практическая работа**

**Проверка работоспособности Антивируса**

1) Скопировать .rar файл с вирусным устройством.

2) Запустить посмотреть на реакцию антивируса, на все компьютеры

3) Сохранить, напимер, на флешку повторить дома (или при возможности на электронную почту).

4) Составить короткую характеристику, используя ресурсы Интернет на один из антивирусов.

**Вопросы на самоподготовку:**

Какие вы знаете признаки заражения

1) Со стороны операционной системы?
2) Со стороны аппаратной части и периферии?
3) Со стороны почты и Интернета?
4) Со стороны браузера?
5) Со стороны приложений?

## ТЕМА: Способы проникновения вредоносного ПО на компьютер

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Понятие компьютерного вируса.
- Основные типы компьютерных вирусов.
- Действие программного вируса.
- Способы удаления вируса.
- Всесторонние признаки заражения системы.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с антивирусной программой.

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа.

ПЛАН УРОКА

| Ход занятия | Методы работы | Содержание | Время |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу. Работа с электронной лекцией. | 7<br>10 |
| 4. Этап применения знаний | 4 | Практическая работа по Реализация динамики вируса в рамках текущей локальной сети | 10 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 7 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |

| | | | |
|---|---|---|---|
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

**Основные сведения о вредоносном ПО**

**Пути проникновения вредоносного ПО на компьютер**

Обычно под термином «зараженный компьютер» понимают ПК, на котором есть один или несколько вредоносных объектов. На самом деле заражены всего несколько файлов, а с остальной «здоровой» частью в принципе можно продолжать спокойно работать. Итак, представим, что ваш компьютер кристально чист, то есть его жесткие диски не содержат ничего, кроме установленной еще до покупки операционной системы. Но как только вы начинаете устанавливать скачанные из Интернета программы, записывать музыку, фильмы, работать с дисками, открываются каналы для доступа вредоносного ПО на ваш компьютер. Ниже перечислены пути, используемые вирусами для проникновения на ПК.

***Система автозапуска.*** Достаточно просто сделать так, чтобы при вставке флеш-карты в компьютер автоматически запускалась определенная программа. Автозапуск есть практически на всех компакт-дисках, а все версии Windows, начиная с XP, сами начинают анализировать содержимое флешки или диска, чтобы запустить подходящую программу для работы с ними. Если все в порядке, то системный автозапуск выдаст вам окошко с выбором вариантов дальнейших действий. Если же на сменном носителе содержится вирус, то есть вероятность, что первым попадет в оперативную память именно он (при отсутствии на ПК резидентного антивируса или при отсутствии в его базе соответствующих сигнатур). Этот путь –проникновения один из самых распространенных на сегодняшний день.

***Локальная сеть***. Если ваш компьютер подключен к какой-либо локальной сети, то невнимательность отдельных пользователей может поставить под угрозу безопасность всех ПК в сети, став источником распространения вредоносного ПО. Компьютерные черви очень легко распространяются по локальным сетям, где политика безопасности достаточно мягкая, и пользователи имеют много прав и разрешений по доступу на другие компьютеры сети. Кроме этого, размножению вирусов способствуют и ошибки в Windows, еще не устраненные Microsoft. Стоит отметить, что именно стремительное распространение вирусов по локальным сетям чаще всего становилось причиной глобальных вирусных эпидемий. Одной из последних можно считать эпидемию вируса Win32.HLLW.Shadow.based, который использовал уязвимости в ОС Windows.

***Интернет***. Многие сайты, независимо от содержимого, могут быть инфицированы вирусами или вредоносными скриптами. Пиратские

дистрибутивы программ тоже с высокой долей вероятности могут быть носителями вирусов или троянцев. Конечно, поймать вирус можно и на чьем-либо официальном сайте (от огрехов никто не застрахован, и специалисты по безопасности тоже люди, и тоже ошибаются), но шанс заразиться намного выше именно на ресурсах с «халявой» или материалами другого содержания. Сюда же можно отнести инфицированные сообщения электронной почты – многие крупные эпидемии развивались именно посредством обмена пораженными письмами.

***Уязвимости в установленном ПО***. По данным исследований, проведенных специалистами по информационной безопасности, ПК, на котором работают программы с известными уязвимостями, при отсутствии защитных систем может быть заражен в течение 3-5 минут.

***Сам пользователь***. Очень часто невнимательность и излишняя доверчивость могут привести к тому, что вы сами установите на компьютер все необходимое злоумышленнику вредоносное ПО. Этот метод распространения вирусов (и метод интернет-мошенничества) называется социальная инженерия – хакер лично общается с пользователем, и с помощью разнообразных уловок добивается, чтобы жертва установила на свой компьютер какую-либо программу, открыла файл, посетила сайт и т.д. Если вы будете осмотрительны и не слишком доверчивы, то эта угроза не столь опасна.

**Практическая работа**

Реализация динамики вируса в рамках текущей локальной сети.

1) Скинуть 1 вирус более безобидный естественно.

2) Попробовать удалить его без помощи посторонних средств используя только текущий антивирус.

3) Узнать имя и тип вируса изучить динамику и возможность распространения.

**Вопросы на самоподготовку**

**Пути проникновения вредоносного ПО на компьютер**

1) Как происходит процесс заражения **при вставке флеш-карты?**

2) Как происходит процесс заражения **по локальной сети?**

3) Как происходит процесс заражения с использованием **уязвимостей в установленном ПО**?

4) Как происходит процесс заражения **“Благодаря” пользователю?**

**ТЕМА: Основные Анализ активных заражений и лечение инфицированных систем**

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Понятие компьютерного вируса.
- Основные типы компьютерных вирусов.
- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с антивирусной программой.

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |

| | | | |
|---|---|---|---|
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br><br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br><br>10 |
| 4. Этап применения знаний | 4 | Практическая работа проверка папок где возможно размещены вирусы | 10 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 7 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

## Анализ активных заражений и лечение инфицированных систем

### Какие объекты могут подвергнуться заражению?

Многие пользователи, когда-либо серьезно пострадавшие от вредоносного ПО, начинают излишне бояться вирусов и с опаской относиться буквально ко всем получаемым данным.

С одной стороны, эти опасения не беспочвенны, но когда речь идет о работе с файлами, можно точно сказать, какие из них могут быть инфицированы, а какие нет. Итак, какие же именно файлы могут содержать в себе вирусный код?

***Исполняемые файлы программ***. Любой файл, который, будучи запущенным, получает возможность частичного контроля над компьютером, может быть опасен – внедренный в него вирусный код при запуске также получит возможность действовать. Это все файлы с расширениями .exe, .com, .bat, .msi, .lnk, .cmd, .scr. Также возможна ситуация, когда вредоносный исполняемый файл маскируется под файл другого типа с помощью ложного расширения. Отображение расширений может быть отключено в настройках системы, и в таком случае открывая, как можно судить по пиктограмме, avi или jpg файл, вызапускаете троянца или шпионскую программу. Иногда можно встретить даже файлы, имеющие такое имя: "Имя_файла.jpg.exe".

***Загрузочные сектора носителей информации***. Это нельзя назвать файлами, но стоит помнить, что вирус может быть и там.

Приложения, написанные на Flash. Небольшие игры и программы, имеющие расширение .swf, также могут быть заражены.

Файлы скриптов и скрипты на веб-страницах. Файлы с расширением .js или .vbs – это скрипты на языке Java или Visual Basic. Обычно они используются на веб-страницах, к примеру, для регистрации пользователей или при входе их на определенный сайт под своей учетной записью. Но эти же скрипты могут содержать и вирусный код, который, получив доступ к браузеру, может существенно помешать работе, установив на рабочий стол или прямо в браузер баннер, отключить который невозможно. В принципе, эти файлы тоже можно отнести к исполняемым, но без специальной программы работать они не смогут.

Документы MS Office. Документы, созданные в программах этого пакета, – основное и единственное место обитания макровирусов. Этот пункт можно считать несущественным, поскольку отключение макросов в документе (Word и Excel сразу выдают запрос на запрет или разрешение макросов) многократно снижает вероятность активации вируса и дальнейшего заражения. Стоит отметить, что в среде MS Office 2007 и новее вирусов замечено не было, но если вы используете более старые версии, следует соблюдать осторожность.

***Документы PDF***. Используя уязвимости программного обеспечения Adobe, некоторые вирусы способны встраивать себя в pdf-документы и при их открытии инфицировать ПК. Чаще всего такие вирусы блокируют сетевой экран и загружают из Интернета «основной» вирус, который и поражает систему и распространяется по сети. Уже несколько лет эти вирусы имеют широкое распространение, во многом за счет того, что файлы данного формата являются основой обмена документами в Интернете.

Медиа файлы. Существует несколько видов троянцев, способных поражать аудио- и видеофайлы. Этот вид угроз не получил большого распространения, но опасными могут быть уязвимости в медиапрогрывателях, которые встречаются часто и могут быть использованы злоумышленниками.

Все остальные объекты на компьютере можно считать относительно безопасными – txt-файлы, архивы, если в них нет исполняемых файлов, изображения и файлы данных различных программ, и т.д.

Папки размещения вредоносных файлов

Попадая на компьютер, вирусу необходимо в первую очередь куда-либо сохранить свои файлы, откуда он потом будет запускаться и действовать. Чаще всего вирусы размещают себя в следующих местах:

В корневых папках дисков, чаще всего – C:\

В профиле пользователей ПК (C:\Documents and Settings\ в Windows XP и C:\Users\ в Windows Vista и Windows 7)

Во временных папках (C:\Windows\Temp, C:\Documents and Settings\Temp, C:\Users\Temp)

В папке операционной системы (как правило, C:\WINDOWS\) и вложенных в нее папках (чаще C:\WINDOWS\system\, C:\WINDOWS\system32\, C:\WINDOWS\system32\drivers\, C:\WINDOWS\Temp).

**Практическая работа**

**Проверка папок где возможно размещены вирусы.**

*1) Открыть проводник и пройти по этим папкам*

Создаем заведомо на разных компьютерах в разных папках файлы. «Если нашел то молодец». Вкладываем в .txt формат код следующего содержания

X5O!P
%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
$H+H*

Приложение 1.

1) C:\

2) C:\Documents and Settings\ или C:\Users\

3) C:\Windows\Temp, C:\Documents and Settings\Temp, C:\Users\Temp

4) C:\WINDOWS\system\, C:\WINDOWS\system32\,
C:\WINDOWS\system32\drivers\, C:\WINDOWS\Temp

*2) Попробовать удалить его без помощи посторонних средств используя только текущий антивирус.*

*3) Узнать имя и тип вируса изучить динамику и возможность распространения.*

**Вопросы на самоподготовку**

*Какие объекты могут подвергнуться заражению?*

1) Каковы признаки заражения Документов MS Office?
2) Каковы признаки заражения Медиафайлов?
3) Каковы признаки заражения Документов PDF?
4) Где находятся папки размещения вредоносных файлов?
5) Вопрос-анализ «на дом». В каких папках вы еще находили вирусы?

## ТЕМА: Настройка ПК и приложений для обеспечения защиты вирусов и Интернет-угроз

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.

- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Понятие компьютерного вируса.
- Основные типы компьютерных вирусов.
- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с антивирусной программой.
- Работать с проводником и браузером (IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| Ход занятия | Методы работы | Содержание | Время |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |

| | | | |
|---|---|---|---|
| 3. Этап введения новых знаний | 1, 2<br><br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br><br>10 |
| 4. Этап применения знаний | 4 | Практическая работа при помощи ресурсов интернет найти определения таким понятиям | 10 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 7 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

**Анализ активных заражений и лечение инфицированных систем**

**Настройка ПК и приложений для обеспечения защиты от вирусов и интернет-угроз.**

Одной из важнейших (если не самой важной!) составляющих компьютерной безопасности является не качество установленного антивируса и даже не сам факт его наличия в системе, а банальная осведомленность и аккуратность пользователя. Известно, что любой человеческий вирус легче предупредить профилактическими мерами, нежели лечить уже проявившуюся после инкубационного периода заразу. То же самое можно сказать о компьютерных вирусах – если пользователь не соблюдает правила компьютерной «гигиены», то рано или поздно он попадет с ситуацию, где антивирус окажется бессилен. Ниже приведен перечень основных действий пользователя, выполнение которых обеспечивает системе достаточно высокий уровень вирусной безопасности (разумеется, эти методы не исключают установку антивируса).

***Настройка Windows***

Достоверно известно, что наибольший урон и глобальные эпидемии были вызваны сетевыми червями, которые эксплуатировали те или иные уязвимости в Windows. По сей день продукт от Microsoft остается наиболее распространенной ОС, используемой в офисах и на домашних ПК. Ниже мы рассмотрим ряд действий, позволяющих если не устранить, то существенно

минимизировать возможности вирусных атак, использующих системные ошибки.

1. Работа с ограниченными правами пользователя. Чаще всего домашний или офисный ПК имеет единственного системного пользователя, имеющего права администратора.

В то же время стоит помнить, что все программы, запускаемые пользователем, имеют тот же максимум прав, что и он сам. Таким образом, работая с правами администратора, вы открываете вирусам многие двери.

Чтобы избежать многих проблем, достаточно создать на компьютере учетную запись с ограниченными правами и использовать при работе именно ее, переключаясь на пользователя Администратор (проще всего так и назвать полноправную запись) только для установки новых программ или внесения изменений в системные настройки.

Чтобы создать новую учетную запись, нажмите Пуск → Панель управления → Учетные записи пользователей. Выберите Создание учетной записи, в открывшемся окне введите имя для этой записи (например, Работник) и нажмите Далее. В следующем окне отметьте флажком Ограниченная запись и выберите Создать учетную запись. Теперь при загрузке Windows на экране будет появляться меню выбора пользователя. Постоянно работая с ограниченной записью, вы существенно сократите возможности вирусов по поражению вашей системы и размножению в ней.

Примечание. Существует учетная запись с именем Гость, с помощью которой можно зайти в Windows, не имея собственной учетной записи. Удалить эту запись нельзя, но ее необходимо Отключить. Использование UAC. В среде Windows Vista и Windows 7 по умолчанию включен UAC (User Account Control – Контроль учетных записей), который требует подтверждения на выполнение любых значительных действий в системе. Желая избавиться от постоянных запросов, пользователи отключают UAC, но с точки зрения безопасности делать это категорически не рекомендуется! Подробнее об этой функции можно прочитать, например, здесь: http://www.java.com/ru/download/faq/uac.xml.

2. Регулярное обновление Windows. Постоянно поддерживая ОС в актуальном состоянии, вы избежите атак, осуществляемых через известные уязвимости. Самый простой вариант для реализации этого пункта – включить Автоматическое обновление. К сожалению, большая часть используемых у нас в стране копий Windows – пиратские и, следовательно, не могут обновляться автоматически. В такой ситуации можно устанавливать обновления, вручную скачав их с сайта компании Microsoft. Но наилучшим решением будет приобрести лицензионную копию Windows, что позволит не только получать все обновления автоматически, но и даст круглосуточный доступ к службе технической поддержки. Для проверки наличия еще не установленных обновлений можно использовать утилиту Microsoft Baseline Security Analyzer, скачать которую можно по ссылке: http://technet.microsoft.com/en-us/security/cc184924.

3. Отключение наиболее уязвимых компонентов системы. Такие компоненты, как Удаленный помощник, Удаленный реестр и им подобные, рекомендуется отключать, если вы их не используете.

4. Использование программ сторонних разработчиков. В состав Windows входит множество компонентов, альтернативой которым являются продукты (в том числе бесплатные) сторонних разработчиков. Для обеспечения максимальной безопасности рекомендуется использовать следующее ПО сторонних производителей.

***Брандмауэр***. Брандмауэр является частью системы безопасности Windows, поэтому уязвимости в нем ищутся злоумышленниками в первую очередь. Чтобы обезопасить себя, установите брандмауэр другой фирмы или используйте комплексный антивирусный пакет (например, пакеты от Dr.Web: Dr.Web Security Space Pro или Антивирус Dr.Web Pro).

***Браузер***. Поскольку с его помощью пользователь работает в Интернете, браузер и ошибки в нем представляют наибольший интерес для хакеров. Использование бесплатных бразеров (например, Opera, Chrome или Firefox) значительно повышает уровень безопасности при работе в сети. Также можно использовать защитные плагины, например Noscript или ADBlock Plus для Firefox.

Почтовый клиент. Встроенный в Windows клиент Outlook Express и компонент пакета Microsoft Office Outlook являются первыми мишенями взломщиков, специализирующихся на различных почтовых диверсиях. Использование сторонних программ (например, Thunderbird или The Bat!) значительно снижает риск подвергнуться атаке через почтовый клиент.При желании заменить можно даже пакет Microsoft Office, например его бесплатным аналогом OpenOffice, который поддерживает все типы документов, созданных в MS Office.

Сама необходимость перехода на стороннее ПО вызвана тем, что широко распространенные продукты Microsoft имеют значительное количество уязвимостей, активно использующихся хакерами. Применяя для работы менее распространенные программы, вы существенно снизите риск пострадать от эксплойта в них.

**Практичекая работа**

**При помощи ресурсов Интернет найти определения таким понятиям**

1) Брандмауэр. Браузер. Почтовый клиент. Почтовый клиент. Автоматическое обновление. Дать определение по факту и своими словами.

2) Отключение наиболее уязвимых компонентов системы. Найти и назвать наиболее уязвимые компоненты системы.

3) Выполнить пункт 1.(Инструкция в пункте 1 данной лекции).

**Вопросы на самоподготовку**

1) Перечислить перечень основных действий пользователя, выполнение которых обеспечивает системе достаточно высокий уровень вирусной безопасности:

2) В чем состоит:

1. Работа с ограниченными правами пользователя.
2. Регулярное обновление Windows.
3. Отключение наиболее уязвимых компонентов системы.
4. Использование программ сторонних разработчиков.

**ТЕМА: Анализ активных заражений и лечение инфицированных систем**

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Понятие компьютерного вируса.
- Основные типы компьютерных вирусов.
- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с антивирусной программой.
- Работать с проводником и браузером(IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу. Работа с электронной лекцией. | 7<br>10 |
| 4. Этап применения знаний | 4 | Практическая работа определение признаков вируса по названию в диспетчере задач | 10 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 7 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на | |

| | | | |
|---|---|---|---|
| | | вопросы (устно). | |

**Анализ активных заражений и лечение инфицированных систем**

**Отключение автозапуска со съемных носителей**

Существует целый ряд вирусов, загружающихся в память ПК при установке в привод инфицированного диска или флеш-накопителя. Чтобы предотвратить активацию таких вирусов, необходимо запретить автозапуск со всех съемных носителей. В Windows версий Vista и 7 отключить автозапуск можно через соответствующее меню, а в Windows XP для этого необходимо внести ряд корректив в настройки групповой политики: Нажмите Пуск → Выполнить, в строке введите gpedit.msc → OK. В открывшемся окне выберите Политика Локальный компьютер → Административные шаблоны → Система → Отключить автозапуск. В диалоговом окне отметьте флажком пункт Включен, в выпадающем списке укажите Всех дисководах и нажмите Применить, затем OK.

*Примечание*. Многие антивирусные пакеты, например Антивирус Dr.Web, позволяют запретить автозапуск со съемных носителей. *Внимание*! К съемным носителям относятся не только флеш-карты и лазерные диски, но и вообще любые устройства, имеющие накопитель и использующие USB (или любой другой порт, например eSATA) для подключения к ПК! То есть можно передать вирус с одного компьютера на другой даже через фотоаппарат или mp3-плеер. Съемные жесткие диски, хоть и не считаются системой сменными носителями, представляют не меньшую угрозу, и в плане безопасности к ним требуется предельное внимание.

*Настройка установленного ПО*

Поддерживать установленное на компьютере программное обеспечение в актуальном состоянии не менее важно, чем обновлять ОС. Теоретически абсолютно любую ошибку в программе можно использовать для причинения вреда системе в целом. Будет это кратковременный сбой или серьезная порча данных - не важно, но возможность причинения ущерба есть. Чтобы этого избежать, важно следить за состоянием имеющегося ПО и своевременно скачивать обновления или новые версии.

Многие программы автоматически проверяют наличие обновления через Интернет. Отсюда вытекает простое правило: не следует отключать в настройках программ автоматическое обновление или, если его нет, уведомление о новых версиях.

Но многие программы не следят за собственной актуальностью, и в таком случае необходимо проявить активность пользователю. Например, воспользуйтесь утилитой Secunia Personal Software Inspector от компании Secuna. Скачать последнюю версию утилиты можно по адресу: http://secunia.com/vulnerability_scanning/personal. После инсталляции утилита сканирует установленное ПО, после чего просматривает сайты

соответствующих производителей и при необходимости позволяет в автоматическом режиме обновлять все установленные приложения.

Также стоит учесть, что количество вредоносного ПО, использующего уязвимости в продуктах Adobe, стабильно увеличивается. Чтобы противостоять этим угрозам, можно действовать по двум вариантам:

В настройках Adobe Reader отключить запуск объектов JavaScript (по умолчанию эта опция включена). Это не гарантия безопасности, но большая часть уязвимостей используется злоумышленниками с помощью скриптов.

Использовать альтернативные программы просмотра PDF-файлов (например, бесплатное приложение FoxIt Reader - http://www.foxitsoftware.com/downloads).

*Внимание*! Ни один программный продукт не требует столь частой актуализации, как антивирус. Новые вирусы пишутся постоянно, и вирусные базы обновляются с очень высокой частотой. Например, антивирус от компании «Доктор Веб» по умолчанию автоматически обновляется каждые полчаса! А антивирус «Касперского» по умолчанию через каждый час.

В то же время компьютер с антивирусом, базы которого последний раз обновлялись больше недели назад, можно считать абсолютно незащищенным. Поэтому старайтесь обновлять антивирус как можно чаще и ни в коем случае не отключайте автоматическое обновление!

*Настройка браузера*

Поскольку описать тонкости настройки всех существующих браузеров в рамках данного курса просто невозможно, здесь мы укажем ключевые параметры, от которых зависит защищенность браузера от вирусов и интернет-атак. Необходимо:

Блокировать незапрашиваемые всплывающие окна. Это нужно не только для избавления от части рекламы на сайтах, но и чтобы не допустить проникновения вредоносного ПО на жесткий диск.

Не сохранять пароли. Первое интернет-правило - ваш ПК не должен знать ваших паролей к интернет-ресурсам. В противном случае, при удачной атаке или вирусном заражении, все пароли попадут к хакеру. И если среди них будут почтовые или банковские данные - вы можете потерять многое.

Ограничить применение JavaScript.

Эта опция есть не во всех браузерах, но при ее наличии можно включить применение JavaScript, запретив ВСЕ дополнительные опции этого раздела (например, разрешение на изменение размеров окна, строки состояния и т. д.).

Включить антифишинговый фильтр.

Блокировать невидимые окна (отключить IFrame). Невидимые окна могут использоваться злоумышленниками для скрытого перенаправления пользователей на инфицированные сайты.

При работе с pdf-файлами сохранять их на диск, не открывая в браузере. Учитывая широкое распространение угроз для pdf-формата, безопаснее сохранять файлы этого типа на жесткий диск и открывать только после проверки антивирусом.

Как задать эти опции в вашем браузере, вы можете уточнить в его справочной системе.

**Практическая работа**

**Определение признаков вируса по названию в диспетчере задач.**

1) При помощи связки CTRL+ALT+DELETE вызвать диспетчер задач.
2) Выявить невредоносные процессы, то есть все непонятные процессы, которых не должно быть. Указать к чему они относятся.
3) При помощи браузера найти стандартный список для своей операционной системы в диспетчере задач.
4) Проанализировать получившиеся данные.
5) Дать ответ был ли вирус на компьютере. САМ ФАЙЛ!

**Вопросы на самоподготовку**

1) Как происходит отключение автозапуска со съемных носителей.
2) Каким образом происходит настройка установленного ПО.
3) Какие программы рекомендуются использовать при настройке установленного ПО.
4) Как правильно настроить браузер чтобы не заразить систему? Назовите несколько пунктов.

**ТЕМА: Общие правила безопасности при работе с Интернетом и почтой**

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Понятие компьютерного вируса.
- Основные типы компьютерных вирусов.
- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.

- Отключение автозапуска со съемных носителей.
- Настройка установленного ПО и браузера.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с антивирусной программой.
- Работать с проводником и браузером (IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br><br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br><br>10 |
| 4. Этап применения знаний | 4 | Практическая работа Рассмотрение примера спам сообщения содержащего ссылку на атаку типа социальная инженерия. | 10 |

| | | | |
|---|---|---|---|
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 7 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

**Анализ активных заражений и лечение инфицированных систем**

Общие правила безопасности при работе с Интернетом и почтой.

Поскольку большая часть вредоносного ПО распространяется через Интернет и, в частности, электронную почту, то особенно важно знать правила, позволяющие снизить риск заражения вирусом именно через эти источники:

1. Внимательно относиться к любым сообщениям, полученным от неизвестных людей.

Это относится как к сообщениям в IM-системах, так и к электронным письмам. В сообщении может содержаться не просто спам (к которому все уже привыкли), но и какие-либо вредоносные скрипты или ссылки. В идеале, неизвестные сообщения не стоит открывать вообще.

2. Не переходить по ссылкам в сообщениях из непроверенных источников. Где бы и какую бы ссылку вам ни предлагали, лучше ей не пользоваться. Вряд ли вы упустите что-то хорошее, зато точно не попадете на очередной фишинговый сайт или не скачаете вредоносный скрипт.

3. Не открывать и не скачивать вложения из писем от неизвестных адресатов. Если ссылка может вести на вредоносный сайт, то вложенный в письмо файл может сам оказаться троянцем, шпионом или вирусом. Вообще, переходить по ссылкам из писем можно только убедившись в подлинности адресата.

4. Не скачивать программы с непроверенных сайтов. Порталы с «халявным» ПО - любимое место обитания вирусописателей, вследствие чего большая часть свободно распространяемых через пиратские сайты программ инфицирована. Если вам потребовалось какое-либо приложение - загрузите его с официального сайта производителя - и честнее, и безопаснее.

5. Выбирать сложные пароли. Чем длиннее и сложнее ваш пароль -тем труднее злоумышленнику будет его взломать. Руководствуясь этим, старайтесь придумывать пароли, имеющие максимальную длину и содержащие как можно больше различных символов (строчные и заглавные буквы, цифры, допустимые спецсимволы).

6. Исключить повторение паролей. Необходимо, чтобы для каждого сетевого ресурса (страница в соц. сети, электронная почта, Интернет кошелек и т.д.) у вас был отдельный пароль. Это не позволит злоумышленникам, взломавшим один из ваших аккаунтов, получить доступ к остальным.

7. Не обращать внимания на мошеннические уловки. Если вы получили электронное письмо или мгновенное сообщение, якобы от администрации сервиса, в котором требуется подтвердить, например, активность аккаунта и сообщить свои логин и пароль, не обращайте внимания - это мошенничество. Никогда и никому не сообщайте свои учетные данные, даже если требование выглядит как официальный запрос от администрации ресурса (это обман)!

8. Не сообщать о себе в Интернете слишком много. Интернет - зона активного общения, где каждый человек может рассказать о себе все, что сочтет нужным. Разумеется, какой-то минимум данных о себе указать необходимо, но активно делиться с интернет-сообществом подробностями своей жизни не рекомендуется - зная о вас достаточно много, злоумышленники смогут использовать эти сведения, чтобы скомпрометировать вас или попытаться действовать от вашего имени.

9. Контрольные вопросы должны быть сложными. Пароль ко многим сетевым сервисам (например, к почте) можно восстановить с помощью Контрольного вопроса. Например, вы забыли пароль от почтового ящика. Через соответствующую ссылку на сайте вы запрашиваете новый пароль. Система выводит вам вопрос, который вы сами указали при регистрации и ответ на который (в идеале) известен только вам. В случае правильного ответа вы сразу можете ввести новый пароль и продолжить пользоваться сервисом. При выборе контрольного вопроса постарайтесь сделать так, чтобы никто, даже из ваших близких, не смог подобрать верный ответ на него. Указывать в качестве пары «вопрос-ответ» какие-либо очевидные вещи (например: «Сколько ног у человека?» «Две») тоже недопустимо.

*Противодействие атакам типа «социальная инженерия» с помощью подручных средств*

Термин «социальная инженерия» объединяет в себе несколько видов интернет-угроз, общей чертой которых является тот факт, что внимательность жертвы играет решающую роль в успехе атаки. Уловок для пользователей может быть множество - фишинговые ссылки, ложные письма из банков или администрации каких-либо сетевых ресурсов и многое другое. Особенно стоит отметить, что различные виды социальной инженерии всегда направлены на одно и то же: получить личные данные пользователя, будь то пароли от веб-сервисов или конфиденциальная информация и банковские данные.

Чтобы справиться с мошенниками, использующими данный метод атаки, требуется не так много. Соблюдение простых правил из приведенного ниже списка помогает заметно снизить вероятность потери информации:

1. Если вы получили письмо с требованием сообщить или подтвердить ваш пароль от любого ресурса - удаляйте его, какие бы страшные угрозы в нем ни содержались (удаление аккаунта, обнуление счета и т.д.). Администрации сетевых ресурсов, а уж тем более банки НИКОГДА не запрашивают у пользователя какие-либо данные.

2. Если вы получили от своего знакомого письмо или сообщение странного содержания, например, похожее на спам или имеющее ссылки на какие-то ресурсы, - свяжитесь с респондентом любым другим способом (например, по телефону) и уточните, что и зачем он вам послал. Не исключено, что его аккаунт взломан и используется злоумышленниками.

3. Если какие-либо сторонние ресурсы предлагают перейти на страницу, где вам придется ввести свои данные (например, ссылка на сайт vkontakte.ru) - потратьте время, чтобы вручную ввести текст ссылки в окно браузера - это полностью исключит возможность попадания на фишинговый сайт (существует много методов маскировки истинных путей ссылок).

4. Прочитав в Интернете про «легкий» способ взломать какой-либо сайт, лучше не проверяйте описанный метод в действии. Хакеры никогда не афишируют, какие уязвимости им удалось найти, а сыграть на любопытстве пользователей, заставив тех сделать что-то нужное киберпреступникам, они могут.

5. Установите на ПК антивирусный пакет, содержащий веб-антивирус и антифишинг, - это намного обезопасит любые ваши действия в сети. (Хорошим примером может служить пакет Dr.Web Security Space Pro).

**Практическая работа**

**Рассмотрение примера спам сообщения содержащего ссылку на атаку типа социальная инженерия.**

1) Подробно ознакомится с содержанием лекции.

2) Зайти на свою электронную почту посмотреть (отправлено сообщение?).

3) Незамедлительно начать действовать, без паники задавая вопросы если что-то не понятно.

4) Особо любопытным по ссылке перейти, предварительно проверив антивирус на работоспособность.

Примерный текст сообщения: “Приветище! куда ты пропал, я подготовила офигительный сюрприз для тебя!
Это не купишь в твоем городе! Потом меня зацелуешь за находку!
Это новинка из Новой Зеландии http://55quowns.hotmail.ru”

P.S. в свою очередь, преподаватель должен проконтролировать удаление данного письма из ящика детей. На том же уроке!

**Вопросы на самоподготовку**

1) Общие правила безопасности при работе с Интернетом и почтой.

2) Расскажите о таком пункт как выбирать сложные пароли.

3) Что означает не сообщать о себе в Интернете слишком много?

4) Как происходит противодействие атакам типа «социальная инженерия»?

5) Что нужно делать, если вы получили от своего знакомого письмо или сообщение странного содержания?

6) Вопрос для размышления. С какими типами вирусов социальной инженерии вы уже встречались? Отсылались ли вам письма на почту?

7) Вопрос на дом Посмотреть встроенную программу Windows REGEDIT.

**ТЕМА: резервное копирование данных**

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.
- Отключение автозапуска со съемных носителей.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с Regedit. (на непрофессиональном уровне)
- Работать с проводником и браузером(IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br>10 |
| 4. Этап применения знаний | 4 | Практическая работа Настройка установленного ПО | 15 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 2 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

**Анализ активных заражений и лечение инфицированных систем**

***Резервное копирование важных данных***

Большое количество резервных копий, хранящихся в разных местах, надежная гарантия того, что ценная информация не пропадет. Сколь бы внимательны вы ни были, как бы ни был надежен используемый антивирус - всегда найдется причина краха, которую никто не учитывал. Это может быть пожар, прорванные трубы или банальное ограбление - в таких ситуациях любые защитные меры, кроме резервного копирования, будут бесполезны.

Оптимальным можно считать хранение информации в трех не связанных друг с другом местах. Например, на рабочем и домашнем компьютерах, и на съемном жестком диске. Флешки, ввиду своей «нежности» и частого «хождения по рукам» не могут считаться полноправным резервным хранилищем. Обратите внимание, что две копии в разных папках одного жесткого диска - это все равно одно хранилище - при повреждении диска погибнет, вполне вероятно, все содержимое.

Приступая к сохранению информации, нужно ответить на три вопроса:

Какая информация требует резервирования? Сохранять имеет смысл только личные и рабочие данные - папки и документы, созданные или полученные пользователем. Базы данных, адресные книги, почтовые и фотоархивы - тоже необходимо внести в этот список. Сюда можно с некоторой натяжкой отнести собираемые в течение долгого времени музыкальные коллекции, если составлялись они по принципу «с миру по нитке».

Что НЕ следует сохранять: кинофильмы, дистрибутивы программ, скачанные из Интернета музыкальные коллекции. Подобная оценка данных исходит из того, что скачать фильм или дистрибутив из Интернета - дело считанных минут, а восстановить семейные фотографии в случае утраты будет просто невозможно. Аналогичные примеры можно привести и с другими типами данных. На каких носителях будет содержаться информация? Оптимумом для хранения архивных копий можно считать жесткие диски, причем не обязательно съемные. Объясняется это просто: лазерные диски не способны гарантировать качественное длительное хранение (хоть производители и заверяют обратное), а флешки часто используются для переноса информации, и при небрежном использовании легко сгорают. Кроме этого, при невысокой цене жесткие диски имеют просто огромный объем, иногда позволяющий не задумываться над первым вопросом.

Где будет храниться информация? Ответ на этот вопрос зависит от степени конфиденциальности данных. Например, те же семейные фотографии можно хранить дома, на работе и на съемном диске. Для архивирования же документооборота компании такой подход не применим - цена рабочих данных может быть слишком высокой, чтобы позволить им «уйти домой» к кому-либо из сотрудников, а уж о хранении их на переносном диске не может быть и речи. В таком случае имеет смысл хранить один жесткий диск с зашифрованными данными в сейфе. При уходе ответственного лица с работы жесткий диск снимается с компьютера и

кладется в сейф, а ключ сдается на вахту. Утром ключ берется с вахты, открывается сейф, диск устанавливается в ПК, вводится пароль для доступа к зашифрованному содержимому, и можно начинать работу. Описанная процедура является стандартом работы с секретной информацией по требованиям КНБ.

Сколько копий информации необходимо иметь? Вы можете выбрать оптимальный вариант и приобрести один или два дополнительных носителя, понадеяться на авось, ограничившись двумя копиями, или проявить крайнюю осторожность и изготовить пять копий. Исходя из ответа на этот вопрос, можно будет рассчитать затраты средств на резервные накопители и времени на сам процесс архивации.

Продумав детали, можно приступать к копированию. С точки зрения экономии дискового пространства и сохранения структуры данных, имеет смысл использовать специальные программы-архиваторы. Со стороны безопасности лучше переносить данные чистым копированием - нет сжатия, нет единого архива, повреждение которого сведет на нет все усилия.

Приложение .
Обзор программ резервного копирования данных:
http://www.ixbt.com/soft/backup-part1.shtml
http://www.ixbt.com/soft/backup-part2.shtml
http://www.ixbt.com/soft/backup-part3.shtml

**Вопросы на самоподготовку**

1) Резервное копирование важных данных
2) Какая информация требует резервирования?
3) Что НЕ следует сохранять?
4) Где будет храниться информация?

## ТЕМА: Обнаружение вредоносного ПО

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Действие программного вируса.

- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.
- Отключение автозапуска со съемных носителей.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с Regedit. (на непрофессиональном уровне)
- Работать с проводником и браузером(IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br>4 |
| 4. Этап применения знаний | 4 | Практическая работа Автозагрузка вирусов | 21 |

| | | | |
|---|---|---|---|
| | | | |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 2 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

**Обнаружение вредоносного ПО**

**Начальные этапы вирусной активности**

Чтобы начать активно действовать в системе, вирусу необходимо разместить себя на жестком диске (опционально) и в оперативной памяти (обязательно). По сути, существует три способа скрытого попадания вирусов в оперативную память: загрузка вируса одновременно с ОС при помощи различных методов автозапуска;

загрузка вредоносной части вируса из Интернета и/или «сборка» его в памяти заражаемого ПК; удаленный ручной запуск вируса на вашем ПК по сети (с помощью различных средств доступа).

*Автозагрузка вирусов*

Начнем с методов автоматической загрузки вирусов в оперативную память ПК.

Способов загрузить какое-либо приложение одновременно с ОС существует достаточно много, и здесь мы постараемся разобрать их все:

Запуск с помощью реестра

Ниже приведены ветви, добавление в которые ключа может инициировать запуск указанной программы. Например, файл C:\file.exe будет загружаться автоматически при старте Windows или при входе пользователя в систему, если ключ «FILE.EXE” со значением “C:\file.exe” находится в одной или нескольких ветвях реестра, перечисленных ниже: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce]

**Практическая работа Автозагрузка вирусов**

В этих ключах важны параметры "run" и "load" (приложения, указанные в первом ключе, загружаются после входа пользователя в систему, вторые -до).

Особенно стоит обратить внимание на программы, которые могут попасть в автозагрузку через групповую политику, поскольку они зачастую не отображаются в программе MSConfig и большинстве менеджеров автозагрузки.

Проверьте ветвь: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run] и при необходимости удалите оттуда все ключи.

Очень важное место, откуда могут запускаться программы, - это ветвь реестра Windows Logon: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Она содержит достаточно много ключей, но нам будут нужны только некоторые:

Shell - ключ задает перечень файлов, которые запускаются вместе с Windows. По умолчанию значение ключа Shell: "Explorer.exe" для Windows 2000\XP и "taskman, progman, wowexec" для Windows 98\NT. Все посторонние файлы, перечисленные здесь, можно удалять - с высокой долей вероятности это файлы вирусов.

Userinit - ключ присутствует только в версиях Windows новее Windows 98 (за исключением NT).

Он задает файлы, загружаемые при входе пользователя в систему. Значения по умолчанию: “userinit, nddeagnt.exe” для Windows NT и “X:\WINDOWS\system32\userinit.exe,” для Windows 2000\XP, где X — раздел установки ОС. Все посторонние файлы, перечисленные здесь, нужно отправлять на анализ в вирусную лабораторию — с высокой долей вероятности это файлы вирусов.

System - аналогично предыдущему, этот ключ присутствует только в NT-версиях Windows (NT\XP). Он задает перечень файлов, запускаемых как системные в момент инициализации ОС.

Значение по умолчанию: “lsass.exe, spoolss.exe” для Windows NT, и “lsass.exe” для Windows XP.

В среде Windows 2000 параметр не обрабатывается.

VmApplet - ключ, присутствующий только в Windows 2000\XP, отвечает за активацию приложений, позволяющих пользователю

корректировать системные параметры. Значение по умолчанию: «rundll32 shell32, Control_RunDLL «sysdm.cpl»».

Все описанные ключи определяют поведение процесса winlogon.exe в условиях его нормального функционирования. Если файл инфицирован или подменен вирусом с аналогичным функционалом, его поведение может резко отличаться от стандартного, но ключи реестра здесь уже, не причем.

Порядок обработки этих ключей следующий: загрузившись, процесс winlogon.exe запускает файл "Userinit.exe", отвечающий за старт программной оболочки. Userinit исполняет сценарии регистрации, настраивает сетевые соединения и запускает процесс "Explorer.exe".

Если в ключе Userinit прописаны и другие файлы — они также исполняются на этом этапе.

Если старт процесса Userinit почему-либо невозможен, winlogon начинает обработку файлов, указанных в ключе "Shell".

Таким образом, возможно запустить приложения еще до входа пользователя в Windows, если в реестре вместо "Userinit.exe" прописан "userinit.bat" и существует соответствующий пакетный файл со списком программ, которые необходимо выполнить.

Запуск через назначенные задания

Все может быть очень просто - вирус не модифицирует ключи реестра, а просто добавляет в планировщик задание на загрузку себя в память после завершения загрузки Windows.

Узнать, какие программы запускаются по расписанию, можно, посмотрев содержимое папки C:\Windows\Tasks.

Запуск через папку Автозагрузка

Добавить сюда ярлык еще проще, чем прописать новое задание. Проверить содержимое папок автозагрузки нужно по двум адресам:

C:\Documents and Settings\All Users\Главное меню\Программы\Автозагрузка - из этой папки запускаются программы, установленные для всех пользователей.

C:\Documents and Settings\Имя_Пользователя\Главное меню\Программы\Автозагрузка - отсюда запускаются программы, установленные только для конкретного пользователя.

Важным фактором является то, что через ключи реестра можно сменить папку, которая будет обрабатываться ОС как источник ярлыков для автозагрузки. Проще говоря, абсолютно любую папку на компьютере можно задать в качестве папки автоматической загрузки.

За это отвечают два ключа: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders] - ключ "Common Startup"="%ALLUSERSPROFILE%\Главное меню\Программы\Автозагрузка" — общая для всех пользователей папка автозагрузки. Изменив это значение, можем указать другую папку (например, C:\Кучавирусов).

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders] - ключ "Startup"="%USERPROFILE%\Главное меню\Программы\Автозагрузка" - автозагрузка для текущего пользователя.

Примечание. Обработку папки Автозагрузка можно отменить вручную. Для этого во время загрузки Windows необходимо зажать клавишу Shift.

***Примечание. Вирусная активность по отношению к папке автозагрузки может проявляться также в подмене ярлыков. Например, в папке хранится ярлык для какой-либо установленной программы, но указывает он совершено не на тот файл, что значится в названии. Или же ярлык ссылается на командный файл, который запускает не только то, что значится в названии, но и исполняемый файл вируса или троянца.***

**Вопросы на самоподготовку**

1) Начальные этапы вирусной активности, расскажите о них, поделитесь своими соображениями на эту тему.

2) Автозагрузка вирусов запуск с помощью реестра.

3) Подробно опишите с помощью конспекта в тетради процесс автозагрузки вирусов.

4) Как осуществить прописывание какой либо программы в автозагрузке?

**ТЕМА: Начальная вирусная активность**

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.
- Отключение автозапуска со съемных носителей.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с Regedit. (на непрофессиональном уровне)
- Работать с проводником и браузером(IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br>4 |
| 4. Этап применения знаний | 4 | Практическая работа **точки начальной вирусной активности** | 21 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 2 |
| **III. Заключительная часть** | | | **5** |

| | | | |
|---|---|---|---|
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

**Обнаружение вредоносного ПО**

**Точки начальной вирусной активности**

Тем или иным способом загрузившись в память ПК, вирус может сразу начать свою разрушительную деятельность, а может сначала позаботиться о собственной безопасности и доступе к нужным ему функциям ОС, которые обычно бывают защищены. Ниже перечислены точки, через которые вирус начинает действовать, уже будучи активированным и загруженным в память.

*Ключи реестра*

Разбор начальной вирусной активности мы начнем с реестра. Зачастую именно его ключи подвергаются модификациям, чтобы позволить вирусу обходить систему безопасности ПК или загружать вредоносный код при старте Windows. Для работы с реестром используется программа Regedit (Пуск → Выполнить → regedit, OK). Нас будут интересовать ключи и соответствующие им значения различных ветвей реестра следующего типа:

Ключи параметров безопасности. Они находятся в следующих ветках:

\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ (любой куст)

\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ (любой куст)

HKLM\SYSTEM\ControlSet00x\Services\SharedAccess\Parameters\FirewallPolicy\ (x - цифры 1–9)

К этой группе относятся ключи, задающие настройки безопасности интернет-соединений, групповых политик и параметры работы брандмауэра.

Ключи регистрации системных служб и драйверов:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00x\Services (x - цифры 1-9)

Они управляют регистрацией и запуском системных служб и драйверов. Стоит отметить, что внесение в эти ключи вредоносных драйверов значительно затрудняет восстановление системы и очистку ее от вирусов, при этом значительно расширяя возможности самого вредоносного ПО.

Ключи настроек операционной системы и приложений. К ключам этой группы относятся очень многие ветви реестра, в частности все, что перечислены в этой книге. Они могут использоваться вредоносными программами двояко: чтобы нарушить работу ОС и приложений, либо чтобы

украсть персональные данные пользователя из различных программ (особенно опасно здесь запоминание различных паролей браузером).

*Сетевые компоненты Windows*

Сюда относятся все элементы системы, которые отвечают за функционирование компьютера как одной из составляющих сети. Изначально все, описанное ниже, создавалось исключительно для обеспечения или оптимизации работы сети, но вирусы могут использовать многие из этих возможностей для своих целей. Чаще всего деятельность вредоносной программы проявляется одним из перечисленных ниже способов.

Открытые сетевые порты. Каждый компьютер имеет один физический провод, соединяющий его с Интернетом или локальной сетью. Но ведь этот провод используется всеми программами, требующими доступ к сети. Чтобы использовать единое соединение могли все приложения, в протоколах TCP и UDP было введено понятие Сетевой порт - виртуальная точка подключения, которых может быть создано до 65535, и каждая из которых нумеруется от 0 до 65535. Соответственно, каждой программе выделяется один или несколько портов для взаимодействия с сетью. Контролем безопасности портов занимается брандмауэр.

Каждый сетевой порт характеризуется одним из состояний:

SYN_SENT (соединение устанавливается)

ESTABLISHED (соединение установлено)

TIME_WAIT или CLOSE_WAIT (соединение закрывается)

LISTENING (готов к приему соединений)

В то же время для многих программ, сканирующих порты (к ним относятся некоторые легальные, например, брандмауэр, и нелегальные - снифферы), любой порт может иметь состояние Открыт, Закрыт или Скрыт. Открытый порт готов принять подключение, Закрытый - нет, а Скрытый порт не виден из сети, поэтому его состояние определить невозможно. Основной интерес с точки зрения взломщика представляют именно Скрытые порты, поскольку атака на закрытые невозможна, а открытые контролируются брандмауэром.

Проверить состояние портов на ПК можно с помощью системной утилиты Netstat. Для работы с ней откройте Командную строку (Пуск –> Все программы → Стандартные → Командная строка), введите netstat, задайте необходимые параметры и нажмите клавишу Enter. Для просмотра допустимых параметров введите netstat /?.

Далее приведена ссылка на список портов, зарегистрированных за различными программами и службами. Зная, какое ПО установлено на компьютере пользователя, можно попытаться соединиться с его ПК, используя порты, которые открываются соответствующими программами и имеют статус LISTENING, то есть готовы к приему входящих соединений. Кроме этого, можно использовать какое-либо вредоносное ПО, чтобы создать несколько портов с состоя-нием LISTENING, что значительно облегчит взломщику соединение с компьютером жертвы.

Полный список общеизвестных и зарегистрированных портов можно прочитать здесь: http://ru.wikipedia.org/wiki/Список_портов_TCP_и_UDP.

**Практика точки начальной вирусной активности**

Проделать вышесказанное на текущем компьютере и дома

**Вопросы на самоподготовку**

1) Назовите точки начальной вирусной активности.

2) Ключи точек начальной вирусной активности

3) Каждый сетевой порт характеризуется одним из состояний назовите их.

## ТЕМА: Обнаружение вредоносного ПО

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.
- Отключение автозапуска со съемных носителей.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с Regedit. (на непрофессиональном уровне)
- Работать с проводником и браузером(IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;

- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br>4 |
| 4. Этап применения знаний | 4 | Практическая работа **точки начальной вирусной активности 2** | 21 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 2 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

**Обнаружение вредоносного ПО**

Встроенные утилиты удаленного администрирования. В Windows присутствует несколько инструментов, позволяющих удаленно управлять компьютером. Изначально эти программы создавались для облегчения взаимодействия пользователей, но их (вернее, ошибки в них) очень быстро освоили злоумышленники. Перечень компонентов, обеспечивающих непосредственный удаленный доступ, и которые необходимо отключить:

*Удаленный реестр*. Отключение: выберите Пуск → Настройка → Панель управления → Администрирование → Службы. Найдите службу Удаленный реестр и, дважды нажав на нее левой кнопкой мыши, выберите Тип запуска → Отключено.

*Удаленный помощник*. Отключение: выберите Пуск → Выполнить → gpedit.msc, OK. В открывшейся консоли перейдите: Политика "Локальный компьютер" → Конфигурация компьютера → Административные шаблоны → Система → Удаленный помощник. В правом окне консоли для параметра Запрошенная удаленная помощь задайте Отключен, нажмите Применить, а затем OK. По умолчанию значение этого параметра Не задано, что на самом деле позволяет запускать удаленного помощника.

*Удаленный рабочий стол*. Отключение: выберите Пуск → Выполнить → gpedit.msc, OK. В открывшейся консоли перейдите Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Службы терминалов. В правом окне консоли для параметра Разрешать удаленное подключение с использованием служб терминалов задайте Отключен, нажмите Применить, а затем OK.

*Браузеры*

В настоящее время браузер стал не просто средством просмотра html-страниц, а «всем и сразу», вплоть до игровой станции, за счет поддержки огромного количества скриптов, и медиастудии, что обусловлено поддержкой различных плагинов для работы с аудио и видеоинформацией.

*Плагины и скрипты* - самая уязвимая часть браузера, ибо применить их возможно не только на благо пользователя и для его удобства, но и ему же во вред. В частности, вредоносное ПО может использовать возможности вашего браузера поддерживать следующие элементы веб-страниц:

*Скрипты*. Это небольшие элементы кода, написанные на языке JavaScript ли VisualBasic. Вредоносные скрипты, как правило, скрыто загружают вирусы на ПК, занимаются непосредственной «сборкой» вредоносной программы на пораженном компьютере, или производят несанкционированное перенаправление на посторонние сайты (в основном инфицированные).

Невидимые окна (inline frame, сокращенно IFRAME). Iframe - это обычный html-тег, создающий невидимое окно, которое нельзя закрыть обычными способами. С его помощью отображается баннерная реклама, а если речь идет о вредоносном использовании тега - он позволяет переадресовывать пользователя на посторонний инфицированный сайт за

счет скрипта, внесенного внутрь этого тега. Отключить обработку тега iframe в различных браузерах можно следующими способами:

*Opera* (http://ru.opera.com). В главном меню нажмите Инструменты → Общие настройки, в появившемся окне перейдите на вкладку Расширенные и в левой части выберите Содержимое. Затем нажмите Настроить стили и в открывшемся окне снимите флажок с пункта Включить inline-фреймы, после чего нажмите OK.

*Internet Explorer*. В главном меню нажмите Сервис → Свойства обозревателя, в открывшемся окне перейдите на вкладку Безопасность и, выбрав зону Интернет, нажмите кнопку Другой. Откроется окно параметров безопасности. В нем необходимо найти пункт Запуск программ и файлов в окне IFRAME и установить соответствующие ему флажок напротив Отключить. После нажатия OK необходимо перезапустить браузер, чтобы изменения вступили в силу.

Firefox (http://www.mozilla.com/ru/firefox). В этом браузере для прекращения обработки IFRAME будет удобно использовать дополнение Noscript (https://addons.mozilla.org/ru/firefox/addon/noscript).

Элементы ActiveX. Если элементы управления ActiveX разрешены, они могут устанавливаться на компьютер прямиком с сайта, что обеспечивает более широкое взаимодействие ПК с веб-ресурсом. Соответственно, если элемент вредоносный, он может нанести немалый ущерб компьютеру, на который будет инсталлирован. Если в элементах ActiveX нет необходимости (чаще всего они используются в браузерных играх), их также можно отключить.

Плагины сторонних разработчиков. По частоте проявления это второй после скриптов вид браузерной угрозы. Легальные плагины добросовестных авторов могут существенно облегчить и улучшить работу с браузером, но порой вдобавок к плагину пользователь устанавливает какой-либо шпионский модуль или троянскую программу. Основная опасность в ситуации, когда вредоносное ПО попало в обозреватель Интернета, - это потеря брандмауэром контроля над сетью. Обычно браузер имеет полный доступ к сети, а через него и плагин-троянец или шпион получают возможность пользоваться сетевыми соединениями практически без ограничений. Поэтому оптимальным будет не рисковать и не устанавливать никаких надстроек в браузер или пользоваться только фирменными надстройками с сайтов разработчиков.

**Практика точки начальной вирусной активности 2**

Проделать вышесказанное на текущем компьютере и дома

**Вопросы на самоподготовку**

1) Назовите Встроенные утилиты удаленного администрирования.
2) Браузеры, Плагины и скрипты.

3) Элементы ActiveX.

**ТЕМА: Методы обнаружения вредоносных файлов**

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.
- Отключение автозапуска со съемных носителей.

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с проводником и браузером(IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br>4 |
| 4. Этап применения знаний | 4 | Практическая работа **проверить файл svhost.exe и местоположение системных файлов** | 21 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 2 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

## Обнаружение вредоносного ПО

## Методы маскировки вредоносных файлов

Если вирус легко обнаружить - это плохой вирус. К сожалению, вредоносное ПО стараются делать на совесть во всем, в том числе, старательно прорабатывая механизм маскировки. Существует два принципиальных метода скрытия вируса в системе:

Автоматическая маскировка - руткит-технологии (от англ. Root kit - загрузочный пакет) и подмена системных файлов. Ручная маскировка - сюда относятся все приемы «ручного» скрытия вируса в системе. Рассмотрим эти методы подробнее.

*Автоматическая маскировка*

1. Руткит-технологии

Суть этого метода маскировки в том, что вредоносная программа перехватывает запросы операционной системы и подменяет их. Так, она может, например, «подставлять» антивирусной программе правильные данные о проверяемых файлах, в то время когда эти файлы уже безнадежно испорчены. Разумеется, это возможно только в случае, когда антивирус не имеет антируткит-функции.

Руткиты делятся на два вида по принципу действия:

изменяющие алгоритмы выполнения системных функций (Modify execution path),

изменяющие системные структуры данных (Direct kernel object manipulation), и на два типа по уровню воздействия: уровня пользователя (user-mode), уровня ядра (kernel-mode).

Руткит - полноценный компонент вируса, но сам он ничего, кроме как скрывать деятельность вредоносной части вируса, не может.

2. Подмена системных файлов

Зачастую вирус не только поражает какие-либо данные, но сперва подменяет собой системные файлы. То есть в зараженной ОС часть важных файлов представляют собой вирусы, способные выполнять базовые функции системных элементов. Такое встречается достаточно редко, поскольку требует от вирусописателя хороших навыков в программировании. Чтобы выявить подмену, можно проверить действительность цифровой подписи файла или его контрольную сумму (md5) файла. Работа с контрольными суммами и цифровыми подписями описана далее.

*Ручная маскировка*

Эти методы не столь эффективны, как руткит-технология, зато технически несравнимо проще, что и сделало их столь популярными. Рассчитана эта маскировка, прежде всего, на невнимательных системных администраторов и пользователей, имеющих слабое представление о компьютерной безопасности. Вот основные средства подобной системы скрытия: Маскировка вредоносного ПО под файлы операционной системы. Здесь существуют два основных варианта:

1. Вирусу дается имя одного из системных файлов, но размещается он в другой папке, нежели настоящий системный файл. Чаще всего мишенями подлога становятся файлы svchost.exe, winlogon.exe, lsass.exe и другие. В таблице приведено стандартное расположение системных файлов Windows, наиболее часто подделываемых злоумышленниками. Если эти файлы встречаются в других папках (в том числе системных) - это вирусы. Файл Расположение

Svchost.exe C:\WINDOWS\system32
Winlogon.exe C:\WINDOWS\system32
lsass.exe C:\WINDOWS\system32
userinit.exe C:\WINDOWS\system32
ipconfig.exe C:\WINDOWS\system32

mmc.exe C:\WINDOWS\system32
services.exe C:\WINDOWS\system32
shutdown.exe C:\WINDOWS\system32
winspool.exe C:\WINDOWS\system32
tcpip.sys C:\WINDOWS\system32\drivers
explorer.exe C:\WINDOWS
TASKMAN.EXE C:\WINDOWS

2. Имя вируса или троянца делают визуально похожим на имя системного файла. Этого добиваются двумя методами: добавляют или убирают один-два символа или используют букв в различных национальных кодировках (например, добавляются русские или немецкие буквы, схожие внешне с латинскими). Уже несколько лет вирусы чаще всего маскируются под файл svchost.exe. Создан даже своеобразный «топ» подделок:

1. svchost.exe (вместо английской «c» используется русская «c»)
2. svchost.exe (вместо английской “o” используется русская “o”)
3. svcchost.exe (2 “c”)
4. svhost.exe (пропущено “c”)
5. svch0st.exe (вместо “o” используется ноль)
6. svchos1.exe (вместо “t” используется единица)
7. svchosl.exe (вместо “t” используется “l”)
8. svchosts.exe (в конец добавлено “s”)
9. svchoste.exe (в конец добавлено “e”)
10. svchostt.exe (две “t” на конце)
11. svchost32.exe (в конец добавлено “32”)
12. svchosts32.exe (в конец добавлено “s32”)
13. svchosthlp.exe (в конец добавлено “hlp”)
14. svdhost32.exe (вместо “c” используется “d” + в конец добавлено “32”)
15. svshost.exe (вместо “c” используется “s”)
16. svehost.exe (вместо “c” используется “e”)
17. svrhost.exe (вместо “c” используется “r”)
18. svchest.exe (вместо “o” используется “e”)
19. svschost.exe (после “v” добавлено лишнее “s”)
20. svcshost.exe (после “c” добавлено лишнее “s”)
21. svxhost.exe (вместо “c” используется “x”)
22. syshost.exe (вместо “vc” используется “ys”)
23. svchoes.exe (вместо “st” используется “es”)
24. svhostes.exe (пропущено “c” + в конец добавлено “es”)
25. ssvvcchhoosst.exe (все символы имени продублированы)

Почему svchost.exe? Дело в том, что этот файл является основным для запуска всех системных служб, которые стартуют из динамически загружаемых библиотек (.dll), то есть в памяти всегда находится несколько процессов с этим названием, что позволяет достаточно легко замаскировать вирус среди них (в то же время у каждого запущенного через svchost

процесса свой идентификатор). Поэтому к данному файлу нужно относиться наиболее внимательно, но и с другими тоже расслабляться не стоит.

**Практика проверить файл svhost.exe и местоположение системных файлов**

Проделать вышесказанное на текущем компьютере и дома

**Вопросы на самоподготовку**

1) Существует два принципиальных метода скрытия вируса в системе, расскажите о них.

2) Расскажите, что вы знаете о руткит-технологии.

3) Расскажите, что вы знаете о подмене системных файлов.

4) В чем заключается ручная маскировка?

5) Почему svchost.exe?

## ТЕМА: Способы обнаружения вредоносного ПО

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.
- Методы маскировки вредоносных файлов

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с MSConfig. (на непрофессиональном уровне)
- Работать с проводником и браузером(IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 7<br>4 |
| 4. Этап применения знаний | 4 | Практическая работа **Борьба с Autoruns с помощью системной утилиты MSConfig** | 21 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 2 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о | | *Задание на самоподготовку:* | |

| | | | |
|---|---|---|---|
| задании на самоподготовку | | конспект, ответить на вопросы (устно). | |

**Обнаружение вредоносного ПО**

1. Иногда вредоносное ПО мимикрирует не под системные файлы, а под наиболее распространенные драйвера. Например, под драйвера производителей видеоадаптеров - Nvidia и ATI Radeon. Чтобы вычислить такие вирусы, достаточно посмотреть список служебных файлов на сайте производителя оборудования.

2. Кроме «фокусов» с именем, злоумышленники могут также подделать цифровую подпись или описание файла.

Для просмотра описания файла достаточно навести на него курсор мыши. Если какой-то системный файл находится не на своем месте, но описание гласит, что это компонент Windows, - достаточно посмотреть в сети, действительно ли файл с таким именем является указанным в его описании компонентом, или информация фальшивая.

Есть три действенных метода «демаскировки» подозрительных файлов:

Если вы не уверены, что имя не содержит национальных символов, нажмите правой кнопкой мыши на файл. Выберите в открывшемся меню пункт Переименовать, после чего вставьте скопированное в буфер обмена имя в любой текстовый редактор с функцией проверки орфографии. Если имя написано на разных языках, «неправильная» буква будет выделена. Проверьте цифровую подпись файла. Для этого нужно нажать на файл правой кнопкой мыши и в контекстном меню выбрать Свойства, затем в открывшемся окне перейти на вкладку Цифровые подписи и посмотреть Сведения. Если в окне сведений значится Эта цифровая подпись действительна, то все в порядке. В противном случае файл, вероятнее всего, изменен или подменен.

Если вы подозреваете, что подпись файла фальшива, или файл не тот, которым пытается притвориться, - можно проверить его контрольную сумму (md5). Для получения контрольной суммы воспользуйтесь программой Hash или ссылкой http://forum.drweb.com/hash. При переходе по ссылке укажите нужный файл с помощью кнопки Обзор, после чего нажмите Compute. Когда анализ завершится, вам будет выдана вся информация о файле, в том числе md5. После этого можно сравнить результат с данными на официальном сайте производителя файла и определить, настоящий он или фальшивый. Для проверки md5 конкретного файла достаточно ввести его контрольную сумму в форму на сайте: http://fileadvisor.bit9.com/services/search.aspx.

Борьба с Autoruns с помощью системной утилиты MSConfig

В ОС Windows есть очень простая и в то же время удобная утилита для работы с системными файлами и настройками. Она называется MSConfig (запуск: Пуск → Выполнить → MSConfig, OK) и является по сути интерфейсом для просмотра и редактирования ini-файлов. Она может

значительно ускорить процесс поиска загрузочных вирусов. Работать с этой утилитой мы будем по той причине, что через нее можно очень легко отключить автозапуск приложений из системных файлов. Вот какие вкладки программы нам будут интересны:

*Вкладка Общие*

Здесь можно задать вариант загрузки системы, причем система будет загружаться с указанными параметрами до тех пор, пока они не будут вновь изменены. Варианты запуска:

Обычный запуск - в этом режиме обрабатываются все ключи автозапуска, папка Автозагрузки, а также запускаются все стандартные драйвера и службы. Установлен по умолчанию, и в отсутствии проблем включать другой режим не рекомендуется.

Диагностический запуск - загружаются только необходимые драйвера и службы. Использовать не рекомендуется - определить источник ошибки будет трудно, поскольку отключается множество драйверов и служб.

Выборочный запуск - позволяет указать, какие системные файлы конфигурации обрабатывать. Отключая по очереди пункты этого меню, можно вычислить, что является причиной сбоев и ошибок и, возможно, примерно определить место расположения поразившего систему вируса.

*Вкладка WIN.INI*

На этой вкладке в структурированном виде представлено содержимое файла Win.ini (расположен: C:\Windows). Изначально в нем нет строк автозапуска, но они могут быть добавлены туда вирусом и, следовательно, обрабатываться системой. Обратить внимание следует на строки "load" и "run", и соответствующие им значения — имена загружаемых файлов. Для отключения запуска через эти параметры достаточно выделить строку в окне MSConfig и нажать Отключить или просто убрать флажок с соответствующей строки.

Вкладка SYSTEM.INI

Здесь в аналогичном предыдущему файлу формате представлен System.ini (расположен: C:\Windows). Нам будет важен параметр "Shell" раздела "boot", по умолчанию отсутствующий, но который при необходимости может быть создан (вирусом в том числе). Если в этом параметре есть что-то, кроме "Explorer.exe", то, скорее всего, это указание на автозапуск вредоносного ПО. Отключив обработку этого параметра можно заблокировать старт вирусов из данного системного файла.

Вкладка Автозагрузка

На этой вкладке перечислены все программы, запускаемые из различных веток реестра ключами "run" и "load". В графе Расположение указано, из какого именно ключа реестра запускается указанный файл. Если здесь обнаружилось какое-либо нелегально запускаемое приложение, его запуск можно отключить, сняв соответствующий флажок, но удалить запись нельзя. Для удаления ключа автозапуска воспользуйтесь редактором реестра Regedit. Второе средством для борьбы с autorun-вирусами - редактор системного реестра Regedit, который уже неоднократно упоминался выше.

Работать с ним не сложно, в случае возникновения вопросов воспользуйтесь встроенной справкой по редактору (Пуск → Выполнить → regedit, OK. Затем выбрать пункт меню Справка → Вызов справки).

**Практика Борьба с Autoruns с помощью системной утилиты MSConfig**

**Проделать вышесказанное на текущем компьютере и дома**

**Вопросы на самоподготовку**

1) Есть три действенных метода «демаскировки» подозрительных файлов, расскажите о них.

2) Расскажите, борьба с Autoruns с помощью системной утилиты MSConfig.

3) Расскажите, о 4 существующих вкладках.

4) Вопрос для размышления на дом: почему в MSCONFIG бывает больше 4х вкладок и за что они отвечают.

**ТЕМА: Борьба с вредоносном ПО с помощью Антивируса Dr.Web**

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.
- Методы маскировки вредоносных файлов

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с проводником и браузером (IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 12<br>9 |
| 4. Этап применения знаний | 4 | Практическая работа **борьба с вредоносным ПО с помощью Антивируса Dr.Web** | 10 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 4 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о | | *Задание на самоподготовку:* | |

| | | | |
|---|---|---|---|
| задании на самоподготовку | | конспект, ответить на вопросы (устно). | |

**Борьба с вредоносным ПО с помощью Антивируса Dr.Web**

На этом уроке мы рассмотрим использование антивируса Dr.Web, то есть ситуацию, когда пакет был установлен на компьютер, где ранее никакой защиты установлено не было. Второй вариант ситуации - когда антивирус установлен на инфицированный ПК с целью лечения вирусов и постоянной дальнейшей защиты (подробное описание установки можно прочитать по ссылке: *http://download.drweb.com/doc*, в разделе *Установка антивируса*).

Итак, антивирус установлен, и требуется проверить ПК на вирусы, и, при необходимости, устранить все найденные угрозы.

**Порядок работы с антивирусом**

Когда антивирус будет полностью подготовлен к работе (установлен, обновлен, после чего ПК потребуется перезагрузить), в области уведомлений появится фирменный логотип Dr.Web - зеленый паучок. Отсутствие на значке дополнительных элементов (значок красный или с восклицательным знаком) говорит о том, что все установленные компонента антивируса исправны и функционируют, а вирусные базы обновлены. Также паучок свидетельствует о том, что включена постоянная защита ПК от вирусов. В такой ситуации, при попытке какой-либо вредоносной программы активно проявить себя в системе, вирус будет обнаружен и обезврежен. Но неактивные вирусы, даже если они находятся в оперативно памяти, найдены не будут. Наша задача - полностью просканировать компьютер и устранить все опасные программы. Для ее решения нужно выполнить следующие шаги:

1. Нажмите правой кнопкой мыши на значок в области уведомлений и выберите *Сканер*.

2. Когда сканер запустится, выберите пункт *Быстрая проверка* и нажмите *Начать проверку*.

В этом режиме сканируется оперативная память и базовые компоненты системы. Если вирусы найдены - выполните действия, указанные в шаге 4.

3. Когда быстрая проверка завершится, можно задать новую проверку. В общем случае все установленные по умолчанию настройки подходят для работы, поэтому требуется только задать объект сканирования и запустить проверку. Поскольку мы подозреваем (или есть уверенность), что какие-либо файлы на ПК заражены, в окне сканера следует отметить флажком пункт *Полная проверка* и нажать кнопку с зеленой стрелкой (*Начать проверку*) под фирменным логотипом Dr.Web.

4. Если в ходе работы сканер обнаружит вирусы - от них необходимо избавиться. В нижней части окна программы будет выведен список зараженных объектов, которые можно с помощью соответствующих кнопок

*Вылечить*, *Переименовать*, *Переместить* или *Удалить*. Пораженные файлы рекомендуется попробовать вылечить, если лечение не удалось - удалить.

Если часть объектов невозможно вылечить, антивирус переместит их в карантин (они будут скопированы в папку карантина - C:\Program Files\DrWeb\infected!!!). Помещенные в карантин подозрительные объекты можно затем отправить в антивирусную лабораторию «Доктор Веб».

Примечание. Если вы обратитесь за помощью в техническую поддержку Dr.Web, у вас могут попросить лог работы антивируса. Для создания полного отчета воспользуйтесь утилитой Dr.Web SysInfo.

Примечание. Антивирусный сканер - это возможность «заставить» Dr.Web проверить нужный вам объект. Постоянную защиту ПК обеспечивает другой компонент - антивирусный сторож SpIDer Guard.

**Практика борьба с вредоносным ПО с помощью Антивируса Dr.Web**

**Проделать вышесказанное на текущем компьютере и дома**

**Вопросы на самоподготовку**

1) Объясните порядок работы с антивирусом.
2) Что нужно сделать, если в ходе работы сканер обнаружит вирусы?
3) Что делать, когда быстрая проверка завершится?
4) Какой компонент обеспечивает постоянную защиту ПК?

## ТЕМА: Лечение системы с помощью лечащей утилиты Dr.Web CureIt!

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.

- Методы маскировки вредоносных файлов

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с проводником и браузером (IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| **Ход занятия** | **Методы работы** | **Содержание** | **Время** |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | 39 | | |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу. Работа с электронной лекцией. | 17<br>4 |
| 4. Этап применения знаний | 4 | Практическая работа **борьба с вредоносным ПО с помощью Антивируса Dr.Web** | 10 |

| | | | |
|---|---|---|---|
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 4 |
| **III. Заключительная часть** | **5** | | |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

## Борьба с вредоносным ПО с помощью Антивируса Dr.Web

### Лечение системы с помощью лечащей утилиты Dr.Web CureIt!

Лечащая утилита Dr.Web CureIt! от «Доктор Веб» - первейшее антивирусное средство, с помощью которого необходимо попытаться исцелить ПК от вирусов. Dr.Web CureIt! не требует установки, может запускаться с флеш-накопителя и работает без конфликтов с установленными резидентными антивирусами.

В отличие от полноценного продукта Антивирус Dr.Web, Dr.Web CureIt! представляет собой сканер с набором вирусных баз, что делает его весьма мобильным, но не предоставляет пользователю постоянной резидентной защиты, поскольку сторож SpIDer Guard в пакет Dr.Web CureIt! не входит. Также программа не имеет планировщика и модуля обновления, но модуль самозащиты в утилите присутствует.

Dr.Web CureIt! невозможно обновить - перед использованием необходимо скачать актуальную версию программы с сайта «Доктор Веб» по ссылке: *http://www.freedrweb.com/cureit/?lng=ru*.

Важно заметить, что при каждом скачивании генерируется новый дистрибутив утилиты, поэтому, сохраняя Dr.Web CureIt! на жесткий диск, запомните, какое имя имеет файл. Название генерируется из случайной последовательности латинских букв и цифр, но пиктограмма файла - всегда фирменный знак Dr.Web.

### Порядок работы с утилитой Dr.Web CureIt!

Ниже мы пошагово разберем алгоритм работы с лечащей утилитой Dr.Web CureIt! на ПК, пораженном вирусами, но не полностью заблокированном (запустить Dr.Web CureIt! на пораженной системе возможно). Для работы нам понадобится только свежий дистрибутив Dr.Web CureIt!.

Итак:

1. Скачайте утилиту, запомнив имя и местоположение скачиваемого файла. Если доступ к сайту *http://www.freedrweb.com* заблокирован, скачайте утилиту с другого ПК и на флешке перенесите на свой компьютер.

2. Запустите скачанный файл.

3. Загрузившись, Dr.Web CureIt! временно заблокирует работу системы и выведет на экран информацию о режиме усиленной защиты. Если есть подозрение на присутствие в системе активных вирусов, рекомендуется нажать ОК и проверить ПК в защищенном режиме. Выходить из этого режима (кнопка *Отмена*) имеет смысл, только если проверка проводится с профилактическими целями в фоновом режиме.

4. Появится окно с краткой информацией о лицензировании. Можно ознакомиться с условиями покупки, выбрав *Да*, но если лечение требуется немедленно, и оно не противоречит лицензионному соглашению, нажмите *Нет.*

5. Откроется окно с двумя вариантами действий: Пуск Обновить Поскольку скачивается всегда последняя версия, нажмите *Пуск*.

Примечание. Если ваш дистрибутив был выпущен более суток назад, будет выведеноокно с предупреждением, что программу необходимо обновить.

Примечание. После проверки системы Dr.Web CureIt! рекомендуется удалить с жесткого диска, а при необходимости повторной проверки - скачать новую версию.

6. Dr.Web CureIt! предложит провести быструю проверку на вирусы. Нажатие кнопки *Нет* откроет предыдущее окно, поэтому необходимо выбрать *Да*. Начнется сканирование основных элементов системы. Если планируется выполнение полной проверки ПК, лучше не тратить время на быструю - нажатием кнопки с зеленым квадратом (*Остановить проверку*) сканирование можно прервать. Если утилита запущена для профилактики - дождитесь окончания проверки.

7. Во время работы программы может появиться зеленое окошко с предложением бесплатно попробовать полную версию антивируса Dr.Web. При работе в обычном режиме это можно сделать немедленно, перейдя по ссылке в окне. Если демоверсия не требуется, закройте диалоговое окно.

8. Когда быстрая проверка будет закончена или остановлена, вы увидите рабочее окно программы. В общем случае все установленные по умолчанию настройки подходят для работы, поэтому требуется только задать объект сканирования и запустить проверку. При подозрении, что ПК инфицирован, следует выбрать пункт *Полная проверка* и нажать кнопку с зеленой стрелкой (*Начать проверку*) под фирменным логотипом Dr.Web.

Примечание. Более подробно о программе Dr.Web CureIt! и ее настройках можно прочитать в меню *Помощь → Разделы помощи*.

9. Если в ходе работы Dr.Web CureIt! обнаружит вирусы - от них необходимо избавиться. В нижней части окна программы будет выведен список зараженных объектов, которые можно с помощью соответствующих кнопок *Вылечить*, *Переименовать*, *Переместить* или *Удалить*. Пораженные

файлы рекомендуется попробовать вылечить, если лечение не удалось - удалить. Если часть объектов невозможно ни вылечить, ни удалить, необходимо либо переместить файлы (они будут скопированы в папку карантина по адресу C:\DocumentsandSettings\Ваше_имя_пользователя\DoctorWeb\Quarantine), либо переименовать их. Переименование может потребоваться, чтобы при повторном запуске утилитасмогла удалить пораженные файлы, поскольку стереть объекты, в данный момент используемые системой, невозможно. Помещенные в карантин подозрительные объекты можно затем отправить в антивирусную лабораторию «Доктор Веб».

Примечание. Если вы обратитесь за помощью в техническую поддержку Dr.Web, у вас могут попросить лог работы программы Dr.Web CureIt! для анализа. Отчет утилиты (log-файл) находится в папке C:\Documents and Settings\Ваше_имя_пользователя\ DoctorWeb\ и называется CureIt.log.

Примечание. Если HOSTS файл был изменен, Dr.Web CureIt! выдаст соответствующее предупреждение с предложением восстановить его в исходное состояние. Если изменения в HOSTS вносились вами или системным администратором, необходимо нажать Нет, в противном случае нажатием кнопки Да приведите файл в порядок.

Примечание. Использование Dr.Web CureIt! - лишь разовая мера спасения, которую вы можете использовать в экстренной ситуации, но она не заменит полнофункционального антивируса. Чтобы всегда быть уверенным в безопасности своего ПК, используйте полный антивирусный пакет Dr.Web.

**Практика борьба с вредоносным ПО с помощью Антивируса Dr.Web**

Проделать вышесказанное на текущем компьютере и дома

**Вопросы на самоподготовку**

1) Лечащая утилита Dr.Web CureIt!, зачем она нужна?
2) Расскажите пошагово алгоритм работы с лечащей утилитой Dr.Web CureIt! на ПК
3) Если в ходе работы Dr.Web CureIt! обнаружит вирусы?

## ТЕМА: Лечение и восстановление системы с помощью Dr.WebLiveCD/USB

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.

- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.
- Методы маскировки вредоносных файлов

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с проводником и браузером (IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).
3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| Ход занятия | Методы работы | Содержание | Время |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, | 1 |

| | | | |
|---|---|---|---|
| | | мотивация учебной деятельности. | |
| 3. Этап введения новых знаний | 1, 2<br><br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу. Работа с электронной лекцией. | 19<br><br>2 |
| 4. Этап применения знаний | 4 | Практическая работа **создание загрузочной флешки Dr.Web LiveUSB/LiveCD** | 10 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 4 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

**Борьба с вредоносным ПО с помощью Антивируса Dr.Web**

**Лечение и восстановление системы с помощью Dr.WebLiveCD/USB**

Средства аварийного восстановления системы Dr.Web LiveCD и Dr.Web LiveUSB - это продукты компании «Доктор Веб», позволяющие загрузить ПК со сменного носителя (компакт-диска или флеш-накопителя). Загрузив компьютер, вы сможете провести антивирусную проверку с помощью интегрированного в состав пакета антивируса и удалить все вредоносные объекты из системы, а также извлечь критически необходимые данные. В нашем примере мы рассмотрим процесс работы с Dr.Web LiveCD, поскольку, не считая этапов загрузки, эти продукты функционируют одинаково.

Создание загрузочного носителя Dr.Web LiveCD. Для создания загрузочного компакт-диска скачайте iso-образ Dr.Web LiveCD по ссылке: http://download.geo.drweb.com/pub/drweb/livecd/drweb-livecd-600.iso. Затем с

помощью любой программы для прожига CD запишите образ на чистый компакт-диск. Например, если вы используете Nero Burning ROM, вам необходимо сделать следующее: Вставить чистый CD в привод (привод должен поддерживать функцию прожига).

В главном меню программы выбрать Файл → Открыть.

В открывшемся окне выберите сохраненный образ.

Нажать кнопку Прожиг и дождаться окончания процесса записи.

Примечание. Записать образ Dr.Web LiveCD можно только на CD-диск, DVD не подходит.

Dr.Web LiveUSB. Для создания загрузочной флеш-карты скачайте дистрибутив Dr.Web LiveUSB и запустите загруженный файл, предварительно присоединив к компьютеру флеш-накопитель. В открывшемся окне укажите, какую флешку нужно использовать (если их несколько), и требуется ли ее перед этим форматировать. Нажмите Создать Dr.Web LiveUSB и дождитесь окончания процесса. Когда создание будет завершено - нажмите Выход.

Загрузка со сменного носителя

В большинстве современных ПК и ноутбуков есть клавиша, которая позволяет выбрать загрузку с любого носителя, который имеется в компьютере. Как правило, эта клавиша F11. При ее нажатии появляется меню с выбором устройства загрузки. В более старых версиях BIOS устройство загрузки можно выбрать вручную. Для этого необходимо зайти в BIOS, при загрузке нажав кнопку Del или F2, затем открыть раздел загрузки Boot Settings (иногда просто Boot) и поменять последовательность загрузки. Для Dr.Web LiveCD первым пунктом необходимо поставить CD-ROM, для Dr.Web LiveUSB - USB или Removable device.

В начале загрузки с Live-устройства на экран будет выведено меню с вариантами запуска. Как правило, достаточно просто нажать клавишу Enter, так как вариант по умолчанию (Dr.Web LiveUSB (Default)) - самый простой и наглядный. С ним мы и будем работать.

Примечание. Иногда ПК может загрузиться с флеш-карты, только если в настройках BIOS она указана как первичный жесткий диск. В этом случае внесите необходимые коррективы в BIOS и перезагрузите компьютер.

Проверка системы

Когда загрузка будет завершена, вы увидите рабочий стол, схожий с рабочим столом Windows.

Автоматически запустится приложение Dr.Web Control Center для Linux. Для полной проверки ПК на вирусы необходимо выполнить следующие действия:

В программе Dr.Web Control Center для Linux откройте вкладку Сканер (Scanner).

В открывшемся окне в разделе Режим сканирования (Scan modes) выберите пункт Полное сканирование (Full Scan).

Нажмите кнопку Начать сканирование (Begin to scan).

Если во время сканирования будут обнаружены зараженные объекты, выделите их и укажите, какое действие сканер должен выполнить в списке Действия (Select objects from the list and apply a relevant action). Сначала файлы нужно попробовать Вылечить (Cure), если лечение невозможно, их нужно либо Удалить (Delete) либо Переместить в карантин (Move to quarantine).

Закончив работу, закройте сканер и перезагрузите ПК. Для перезагрузки нажмите на значок Dr.Web в левом нижнем углу экрана (на месте стандартной кнопки Пуск) и в открывшемся меню выберите пункт Перезагрузка (Restart). Внесите изменения в BIOS, чтобы ПК загружался с жесткого диска, и проверьте, восстановлено ли функционирование системы.

Если удаление вирусов не помогло вернуть компьютер в рабочее состояние, попробуйте исправить реестр.

Резервное копирование важных данных

Если есть необходимость извлечь с поврежденного ПК какие-либо важные файлы или папки, их можно скопировать на флеш-накопитель (его необходимо вставить ДО загрузки ПК).

Для копирования файлов сделайте следующее:

Запустите Midnight Commander с помощью ярлыка на рабочем столе. Интерфейс этой программы прост и интуитивно понятен, внешне он практически не отличается от известного большинству пользователей Norton Commander.

В окне программы перейдите в корневой каталог, нажав на символ перехода в родительский каталог «/..», в заголовке левого столбца появится значок «/».

Перейдите в каталог /WIN, в нем отображаются буквы жестких дисков вашего ПК. Откройте нужный диск (например: /D), а затем каталог, содержимое которого нужно скопировать на флешку.С помощью клавиши Tab перейдите в правую колонку файлового менеджера и описанным ранее способом откройте корневой каталог флеш-накопителя (например: /F).Вернитесь в левую колонку и с помощью клавиши F5 скопируйте нужный файл или папку на флеш-носитель. Аналогичным методом можно скопировать остальные файлы и папки.

Примечание. Описанным выше способом можно извлечь файлы реестра и, экспортировав их на другой ПК, исправить и восстановить в рабочее состояние, что позволит вернуть систему в рабочее состояние.

**Практика создание загрузочной флешки Dr.Web LiveUSB/ LiveCD**

Выполнить алгоритм и произвести попытку работы с компьютером. Проверить домашний компьютер с помощью этой флешки/диска.

**Вопросы на самоподготовку**

1) Порядок работы со средствами аварийного восстановления системы Dr.Web LiveCD и Dr.Web LiveUSB.

2) Для создания загрузочного компакт-диска скачайте iso-образ Dr.Web LiveCD.

3) Для создания загрузочной флеш-карты скачайте дистрибутив Dr.Web LiveUSB.

4) Резервное копирование важных данных.

**ТЕМА: Анализ системы с помощью утилиты Dr.Web SysInfo**

Урок формирования и совершенствования знаний

**Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания об основных, путях проникновения вредоносного ПО на компьютер, о вирусах и способах их устранения на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учеников.
- *Воспитательная:* воспитывать внимание, аккуратность, бережливое отношение к компьютерной технике и программному обеспечению.

**Ученики должны знать:**

- Действие программного вируса.
- Всесторонние признаки заражения системы.
- Пути проникновения вредоносного ПО на компьютер.
- Настройка ПК и приложений для обеспечения защиты от вирусов.
- Методы маскировки вредоносных файлов

**Ученики должны уметь:**

- Составлять конспект при работе с электронной лекцией.
- Отвечать на контрольные вопросы по теоретическому материалу.
- Работать с проводником и браузером (IE 8 или Firefox).

**Оснащение и методическое обеспечение урока:**

- Компьютерный класс;
- программное обеспечение: электронная лекция, программа Доктор Веб;
- опорный конспект, карточки с заданиями,
- доска, в том числе и интерактивная, мел, маркер.

**Методы работы:**

1. Словесный (беседа, электронная лекция, изложение материала).
2. Наглядный (опорный конспект).

3. Самостоятельная работа (работа с электронной лекцией).
4. Практическая работа. Закрепление пройденного материала.

ПЛАН УРОКА

| Ход занятия | Методы работы | Содержание | Время |
|---|---|---|---|
| **I. Организационная часть** | | Приветствие, готовность учеников и оборудования. | 1 |
| **II. Основная часть** | | | 39 |
| 1. Актуализация знаний | 1 | Фронтальный опрос по предыдущей теме | 4 |
| 2. Мотивация | 1 | Целеполагание, мотивация учебной деятельности. | 1 |
| 3. Этап введения новых знаний | 1, 2<br>2, 3 | Демонстрация преподавателем презентации, постановка задачи на работу с электронным конспектом и практическую работу.<br>Работа с электронной лекцией. | 10<br>4 |
| 4. Этап применения знаний | 4 | Практическая работа с **сервисной утилитой Dr.Web SysInfo** | 17 |
| 5. Этап проверки знаний | 4 | Опрос по пройденной теме | 4 |
| **III. Заключительная часть** | | | **5** |
| 1. Рефлексия. Подведение итогов | 1 | Подвести итоги, отметить наиболее отличившихся учеников, выставить оценки. | |
| 2. Этап информации о задании на самоподготовку | | *Задание на самоподготовку:* конспект, ответить на вопросы (устно). | |

## Борьба с вредоносным ПО с помощью Антивируса Dr.Web

## Анализ системы с помощью утилиты Dr.Web SysInfo

Сервисная утилита Dr.Web SysInfo - хороший инструмент для анализа состояния системы. По отчету, сформированному Dr.Web SysInfo, можно

досконально изучить происходящие на ПК процессы и выявить возможные причины нестабильной работы: конфликты оборудования, конфликты программ или вирусную активность.

Утилита полностью бесплатна, скачать ее можно по ссылке: *ftp://ftp.drweb.com/pub/drweb/tools/dwsysinfo.exe*. Для работы Dr.Web SysInfo не требуются никакие дополнительные компоненты, просто запустите скачанный файл (dwsysinfo.exe) и в открывшемся окне нажмите *сформировать отчет*.

Имя файла отчета может выглядеть, например, так: VD_v_300111_105015.zip. Где VD - имя компьютера, v - имя пользователя, 30 01 11 - дата создания отчета в формате дд мм гг, 10 50 15 - время создания отчета в формате чч мм сс. Расширение .zip говорит о том, что отчет сжат в архив ZIP-формата. Архив с отчетом сохраняется в папке C:\DocumentsandSettings\

Ваше_имя_пользователя\DoctorWeb. Когда создание архива завершено, программа выводит окно с информацией об имени и месте его расположения.

*Примечание. Настройки программы по умолчанию являются оптимальными. При необходимости можно изменить перечень включаемых в анализ элементов системы. Для этого после запуска программы нажмите* ***Параметры отчета****, отметьте флажками пункты, информация о которых требуется, и выберите* ***Сформировать отчет***.

Примечание. Кроме архива, программа создает log-файл, в который заносятся описания всех проблем, возникших в ходе работы (например, если какой-то файл не был найден или было отказано в доступе). Он называется SysInfoLog.txt и располагается в папке со сформированным отчетом.

**Анализ отчета Dr.Web SysInfo**

При задании сбора полной информации о системе (настроено по умолчанию) архив Dr.WebSysInfo будет содержать следующие файлы:

Applications.evt
DrWebInfo.xml
DrWebRegistryExport.xml
HOSTS
msinfo32report.nfo
System.evt
DoctorWeb.evt
SystemInfo.xml
SystemRegistryExport.xml

Файлы .xml открываются с помощью браузера, файл HOSTS - любым текстовым реактором, .nfo - системной утилитой *Сведения о системе*, .evt - программой *Event Log Explorer* (скачать trial-версию можно по ссылке: *http://www.eventlogxp.com/download/elex.zip*). Содержимое каждого файла мы рассмотрим отдельно:

***Applications.evt*** - журнал событий, созданных различными приложениями. Сюда входят информационные события (Information, например, отчет об успешных обновлениях), предупреждения (Warning, например, когда возникают какие-то конфликты или обнаружено несоответствие прав, что может привести к нарушению защиты) и ошибки (Error, например, «вылет» программы). Все события досконально описываются в графе Description.

***DrWebInfo.xml -*** в разделах этого файла содержится информация о функционирующих в системе компонентах Dr.Web:

*LaunchedModules* - здесь перечислены компоненты антивируса с их статусами. True - компонент активен, False - компонент отключен или недоступен по лицензии;

*LicenceFiles* - указывает на лицензионный файл;

*DirectoriesListing* - перечень файлов папки Dr.Web.

Если антивирус Dr.Web не установлен - в первом разделе везде будет значение False, в других местах не будет ничего.

***DrWebRegistryExport.xml -*** здесь перечислены ветки реестра, отвечающие за функционирование Dr.Web. По большей части эта информация для службы технической поддержки.

*Примечание. Файлы DrWebInfo.xml и DrWebRegistryExport.xml используются для диагностики неполадок в самом антивирусе и требуются в первую очередь для инженеров поддержки. При использовании утилиты для поиска следов вирусов они не используются.*

***HOSTS -*** копия системного HOSTS файла. Можно сразу проверить его и, при необходимости, удалить все лишнее из оригинального файла в системной папке.

***msinfo32report.nfo -*** это отчет, создаваемый системной утилитой *Сведения о системе* (вызов: *Пуск → Программы → Стандартные → Служебные → Сведения о системе*). Как пользоваться этой утилитой для диагностики системы поясняется в ее руководстве пользователя (*Справка → Вызов справки)*.

***System.evt*** *- системный журнал событий. Здесь можно отследить проблемы, возникающие у системных компонентов и служб. Формат данных аналогичен предыдущему файлу этого типа.*

***DoctorWeb.evt*** *- журнал событий, зарегистрированных антивирусом. Здесь отображаются все события, связанные с обнаружением подозрительных, инфицированных и непроверенных файлов, а также информация об изменении состояния компонентов (например, выключение/отключение SpIDer Gate и т. д.).*

***SystemInfo.xml*** *- в этот файл выводится сводка по всем параметрам системы. Он содержит следующие разделы:*

***SystemInfo*** *- сведения о компьютере. Сюда входят данные о компонентах системы: ОС, процессор, память, жесткие диски, перечень пользователей, права текущего пользователя, текущее местоположение, системные папки Windows и сетевые адаптеры.*

***AntivirusInfo*** *- данные об установленном антивирусе.*

***FireWall*** *- данные об установленном в системе брандмауэре. Если установлен только системный брандмауэр, раздел будет пустым.*

***ProcessesInfo*** *- информация по всем активным процессам. Самый крупный раздел файла.*

***Serviceinfo*** *- здесь перечислены запущенные системные службы.*

***DriversInfo*** *- информация об используемых системой драйверах.*

***BrowserInfo*** *- данные по установленному по умолчанию браузере.*

***InstalledApplications*** *- сведения обо всех установленных приложениях, в том числе обновлениям к продуктам Microsoft (Windows, Office и др.).*

***SystemRegistryExport.xml -*** *этот файл содержит экспорт наиболее важных веток реестра:*

*Раздел автозагрузки:*

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

*Раздел системных настроек:*

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services - системные сервисы
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule - планировщик
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot - безопасный режим
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application - журнал

*событий приложений*

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ PersistentRoutes - сетевые настройки
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment -переменные среды окружения

*Прочие параметры:*

*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion*

*Image File*

***Execution Options*** *- запрет на отображение перечисленных в данной ветке файлов. То есть программу можно запустить, но работать с ней станет невозможно. Например, при добавлении сюда параметра со значением "explorer.exe", вы не увидите рабочего стола.*

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon - параметры автозагрузчика.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Windows - раздел системных настроек Windows.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows*CurrentVersion\Policies\System - локальная политика безопасности.*

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer - политика ограничения запуска приложений (наличие там путей к антивирусу может привести к его неработоспособности).

*Раздел обработчика системных типов файлов:*

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile - EXE
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\cmdfile - CMD
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\piffile - PIF

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\batfile - BAT
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\comfile - COM
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\scrfile - SCR
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile - LNK

*Проанализировать результаты работы Dr.Web SysInfo вы можете самостоятельно, а можете отправить их в службу технической поддержки «Доктор Веб».*

**Практика использования сервисной утилитой Dr.Web SysInfo**

**Проделать вышесказанное на текущем компьютере и дома.**

**Вопросы на самоподготовку**

1) Что такое сервисная утилита Dr.Web SysInfo?

2) В какой папке сохраняется архив с отчетом Dr.Web SysInfo?

3) Кроме архива, программа создает log-файл в котором…

4) При задании сбора полной информации о системе (настроено по умолчанию) архив Dr.WebSysInfo будет содержать следующие файлы, перечислите их

5) SystemRegistryExport.xml - этот файл содержит экспорт наиболее важных веток **реестра**, перечислите несколько.