

КОМПЬЮТЕРНЫЙ ПРАКТИКУМ

 Ю. М. ПЕНКИН, проф., зав кафедрой фармакоинформатики НФаУ, г. Харьков, В. А. ЖУК, доц.,
Л. Ю. БЕЛОГОРЦЕВА, асс.

Современная практика Интернет-технологий, к сожалению, вынуждает пользователей обращаться к проблеме борьбы с компьютерными вирусами. Этой проблеме и посвящены задания данного компьютерного практикума.

**Задание 1.
Ознакомиться с классификацией
компьютерных вирусов.
Классификация компьютерных вирусов:**

Компьютерные вирусы	Краткая характеристика
Загрузочные вирусы	Воздействуют на загрузочный (boot) сектор флоппи-диска и boot-сектор или Master Boot Record (MBR) винчестера. Вирус «вынуждает» систему при ее перезапуске отдать управление коду загрузчика, а не оригинальному коду загрузки
Файловые вирусы	Воздействуют на файловую систему какой-либо или каких-либо ОС. Вирус заражает файлы, которые содержат исходные тексты программ, библиотечные или объектные модули
Файльово-загрузочные вирусы	Комбинированные вирусы, объединяющие свойства файловых и загрузочных. Основное разрушительное действие — шифрование секторов винчестера. При каждом запуске вирус шифрует очередную порцию секторов
Сетевые вирусы	Используют возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или «подтолкнуть» пользователя к запуску зараженного файла. Проникают в память компьютера из компьютерной сети, определяют сетевые адреса других компьютеров и рассылают по этим адресам свои копии
Макро-вирусы	Являются отдельными программами на макро-языках программирования, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для заражения вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие
Резидентные вирусы	Вирусы, обладающие способностью распространять свои копии в системной памяти (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов). Многие резидентные вирусы заражают диск повторно после того, как он отформатирован
Нерезидентные вирусы	Вирусы активны непродолжительное время — только в момент запуска зараженной программы. Поэтому опасны только во время выполнения инфицированной программы

**Задание 2.
Установка антивирусной программы на рабочем столе ПК.
Следует ознакомиться с процедурой установки антивирусной программы
на примере «Антивируса Касперского 6.0»**

Последовательность действий для выполнения задания:

- на рабочем столе ПК выберите ярлык Internet Explorer и откройте его;



- найдите сервер **Антивирусы**, для чего в адресной строке укажите <http://www.novirus.com.ua> и нажмите клавишу Enter;



- после загрузки home-страницы изучите ресурсы антивирусных программ (главная, антивирусы, Касперский, NOD32, Dr. Web и т.д.);
 - в МЕНЮ, активизировав «Касперский», изучите характеристику программы, условия установки;



- изучите более подробную информацию, активизировав «Подробнее»;



- изучите результаты поиска, ознакомьтесь с описанием характеристики программы;
 - для начала копирования программы активизируйте «скачать».

Комментарий. При копировании программы по умолчанию устанавливается на рабочий стол ПК.

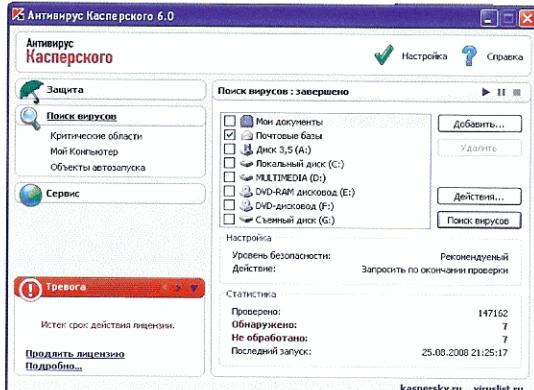
Задание 3.

Знакомство с работой антивирусной программы «Антивирус Касперского 6.0»

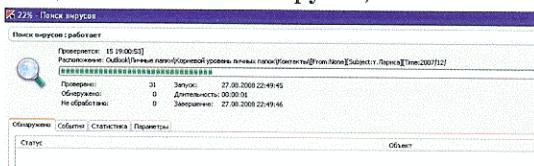
Следует ознакомиться с процедурой поиска вирусов на примере E-mail почты, при помощи программы «Антивирус Касперского 6.0»

Последовательность действия для выполнения задания:

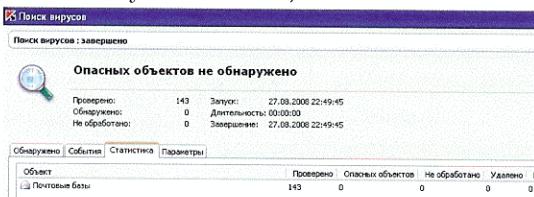
- на рабочем столе ПК выберите ярлык , откройте его;



- изучите открытое окно ресурса;
 - с помощью курсора выделите строку «**Почтовые базы**», нажмите **Поиск вирусов**;



- после окончания работы программы ознакомьтесь с данными (проверено, обнаружено и т.д.), при обнаружении программа автоматически «лечит» поврежденные файлы;
 - для более подробной характеристики активизируйте кнопку **Статистика**;



- по заданному алгоритму проверьте на наличие вируса съемный диск.

Комментарий. Если правильно выбирать антивирусное программное обеспечение и регулярно обновлять его, можно избежать заражения ПК вирусом и соответственно всех его последствий.