

Лабораторная работа 2

Проверка компьютерной системы на наличие вирусного заражения. Использование антивирусного пакета для очистки системы от вирусов

Целью настоящей лабораторной работы является приобретение практических навыков по профилактическому обследованию системы, по обнаружению и уничтожению компьютерных вирусов. Необходимые средства и условия для проведения лабораторной работы

- Исследуемый персональный компьютер с операционной системой семейства Windows[®]
- Антивирусное программное средство Cureit[®], предварительно записанное в один из каталогов жёсткого диска исследуемого компьютера;

Внимание: перед началом работы обеспечьте физическое отключение исследуемого компьютера от локальной сети, для этого коммутационный кабель (патч-корд) данного компьютера отсоедините от соответствующей настенной розетки.

Задание параметров антивирусного исследования

Этап начинается с запуска программной утилиты Cureit[®]
- для этого с помощью Проводника найдите соответствующий файл и щёлкните его мышью. На экране должно появиться окно, в котором изготовители данного программного средства предлагают Вам участвовать в улучшении продукта. Соглашаемся, пометив это соответствующей «галкой».

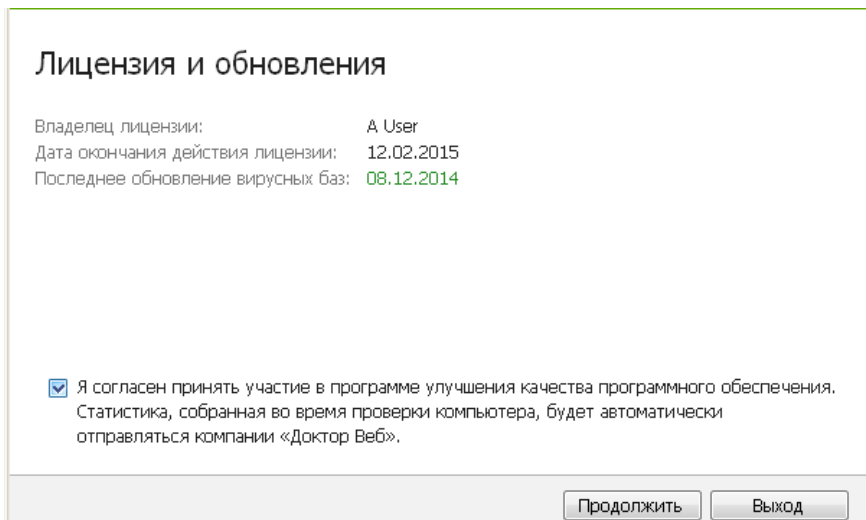
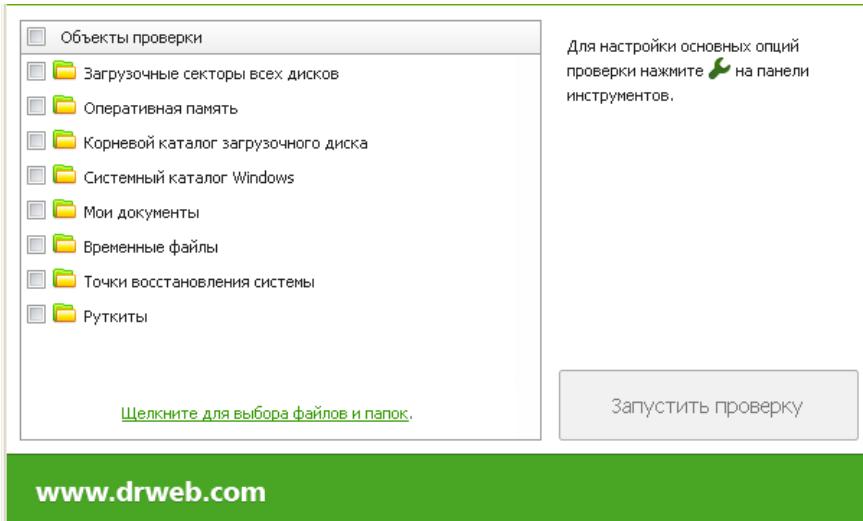


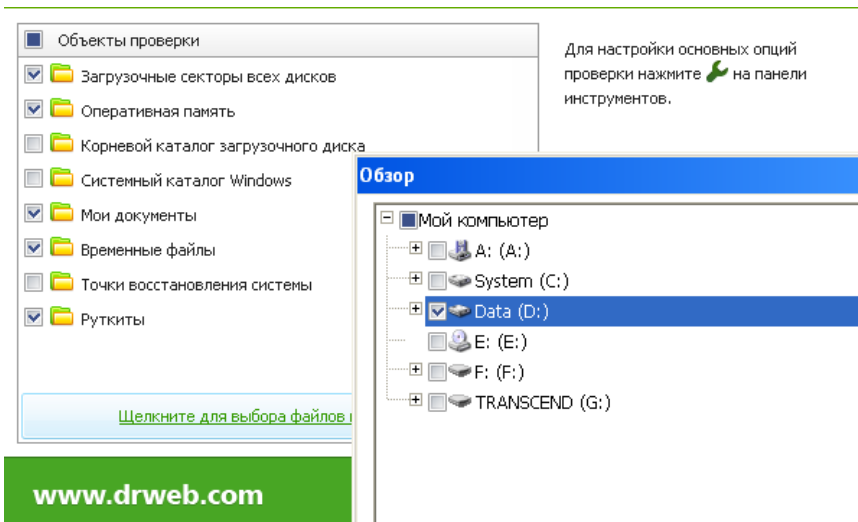
Рис.2_1

После этого должно появиться окно, где перечислены стандартные объекты предстоящего исследования компьютера на наличие вирусов, однако наряду с ними утилита позволяет Вам задать дополнительные пути поиска вирусов.



Воспользуйтесь этим шансом и щёлкните мышью по соответствующей строке внизу данного окна.

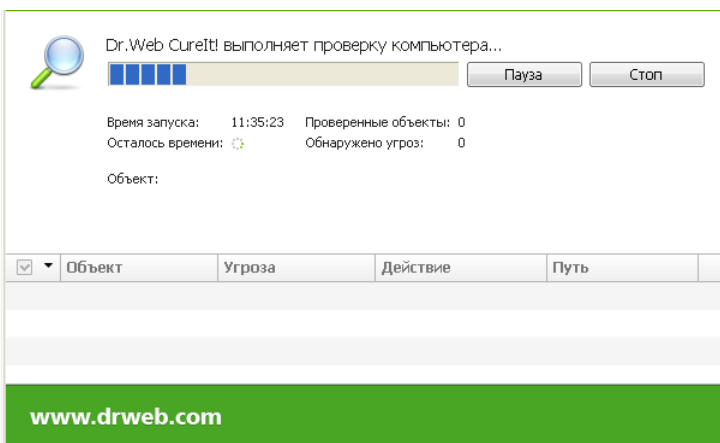
Рис.2_2



В возникшем окне «Обзор» укажите те дополнительные пути, которые планируете проверить: на рисунке отмечен путь Data (D:), а в левой части окна помечен ряд проверяемых стандартных объектов. По завершении этих действий щёлкните кнопку «Запустить проверку».

Рис.2_3

1. Поиск источников вирусов



Проверка и проверяемые файлы отображается в данном окне. При наличии вирусных угроз их источники последовательно высвечиваются в нижней части окна: в примере на Рис.2_5 антивирусная утилита обнаружила 7 таких источников.

Рис.2_4

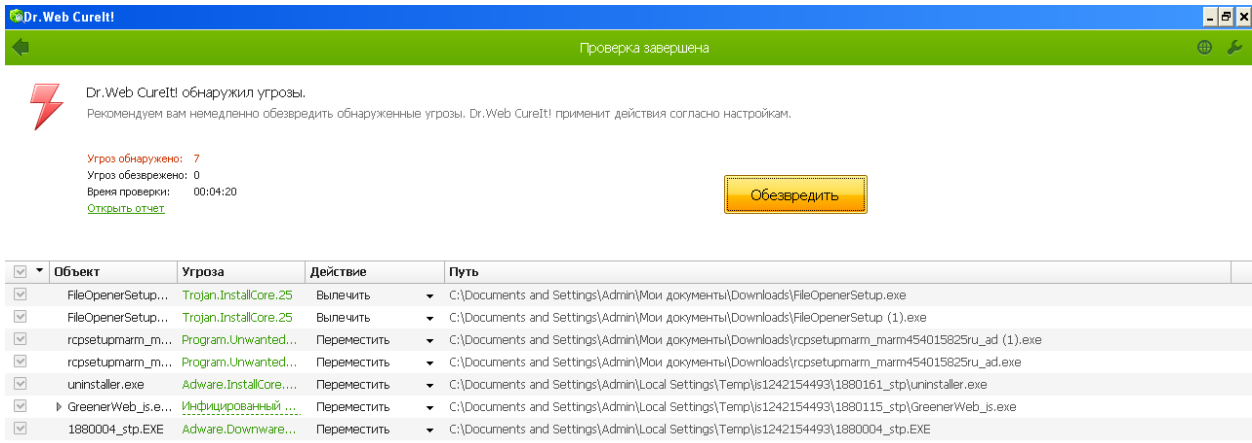


Рис.2_5

Внимательно присмотритесь к сообщениям утилиты – это не только сведения о наличии и месте нахождения вирусов, но и, что гораздо важнее - указания на связь вирусов с содержимым информации на диске, а также об ориентировочном времени заражения и источниках – программах заражения. Это позволяет избежать в будущем повторных вирусных угроз.

2. Уничтожение источников вирусов.

Нажмите кнопку «Обезвредить» и утилита начнёт уничтожать отмеченные источники вирусных угроз. На иллюстрации дано окно, которым завершается этот процесс.

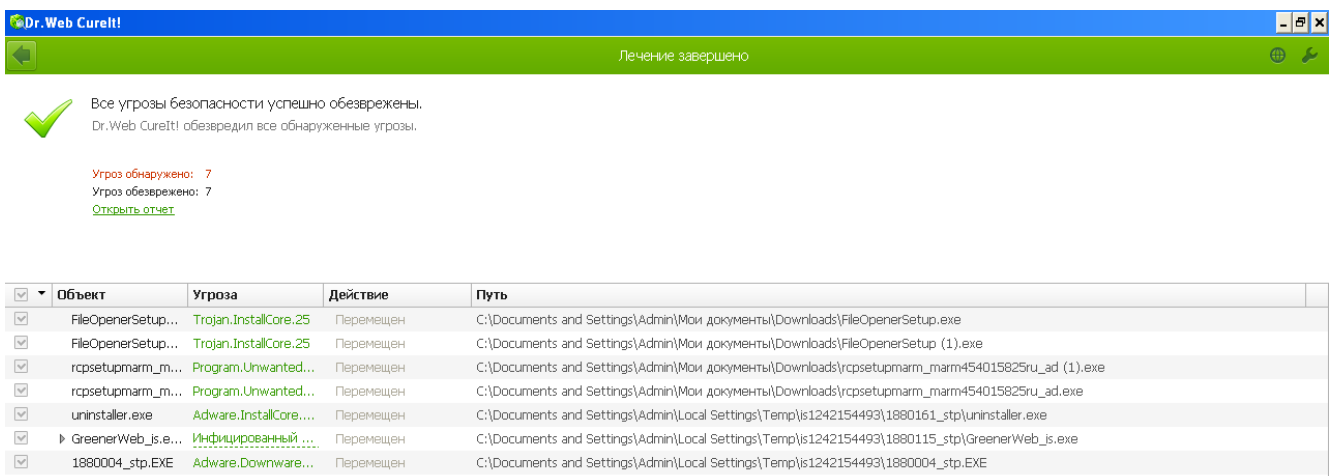


Рис.2_6

В итоге утилита формирует отчет о своей работе, ознакомьтесь с ним и сохраните в каталоге D:\студент\номер Вашей учебной группы. Назовите файл отчёта именем *_Vir , где * - Ваша фамилия. Например, если Ваша фамилия «Орлова», то имя Вашего файла Орлова_Vir.

Восстановите теперь подключение патч-корда к сетевой розетке и скопируйте Ваш файл отчёта в указанный преподавателем сетевой каталог.