МЕТОДИКА ВЫЯВЛЕНИЯ ПРИЗНАКОВ ВРЕДОНОСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ПОМОЩЬЮ ВИРТУАЛЬНОЙ МАШИНЫ

А.Э. Ивашков

Технология виртуальных машин позволяет запускать на одном компьютере несколько различных операционных систем одновременно. При работе с дополнительной, "гостевей" операционной системой исследователь не испытывает никаких затруднений в использовании ее возможностей, то есть происходит полная иллюзия функционирования реальной системы.

Предложенная методика исследования включает: установку и конфигурирование необходимой для исследования операционной системы с помощью виртуальной машины; запуск исследуемой программы на виртуальной машине; поиск внесенных изменений в элементы автозагрузки; поиск внесенных изменений в "Диспетчере задач"; поиск внесенных изменений в файлы на носителях информации (появление новых файлов, удаление старых файлов, изменение атрибутов файлов, таких как размер, дата создания, имя владельца, права доступа к файлу, метод доступа к файлу); поиск внесенных изменений в реестр; исследование сетевой активности (если необходимо); в зависимости от результатов поиска, запуск стандартных программ операционной системы; перезагрузку операционной системы; повторение пунктов 3–8; оформление отчета с выводами о проделанной работе.

Представлен пример использования данной методики. Для исследования используется вирус Virus.Win32.Neshta.b (согласно номенклатуре "Антивируса Касперского).

Описаны преимущества и недостатки использования виртуальной машины по сравнению с другими исследованиями программно-компьютерной системы.