

**Д. А. Э д е л ь, А. А. К о в а л ь** (Ростов-на-Дону, ФГНУ НИИ «Специализация в области информатики»). **Вероятностный анализ метода обнаружения вредоносного кода в файлах на основе сигнатур.**

В современной информационной безопасности угроза несанкционированного проникновения и последующей работы вирусного вредоносного программного обеспечения в компьютер пользователя или организации крайне актуальна. Единственным способом противостояния этой угрозе является антивирусная проверка всех исполняемых файлов на компьютере. Одним из методов обнаружения вредоносного кода в файле является поиск по сигнатуре [1]. Сигнатура — последовательность байт кода в определенном месте программы, уникально определяющая файл. В качестве сигнатуры может выступать хэш-функция от определенных байт кода, также уникально идентифицирующая файл. По базе данных сигнатур, путем поиска вирусной сигнатуры, определяется наличие вредоносного кода в программе [2]. Проанализируем вероятность обнаружения настоящей вирусной сигнатуры в файле.

Последовательность команд языка ассемблер может выглядеть как «пор пор jmp» — заголовочным фрагментом вирусного кода в файле. Эта последовательность в машинном виде выглядит как 0x90 0x90 0x90 0xEB. Или же в 4-х байтовом представлении 0x909090EB. Весь диапазон представляемых значений в 4-х байтах кода 0x00000000 ... 0xFFFFFFFF, что представляет собой значение от 0 до 4294967295. Таким образом, вероятность нахождения в 4-х байтовом фрагменте файла указанного значения составляет  $2,3283064 \cdot 10^{-10}$ . Поэтому, если вирусный сканер обнаружит такую сигнатуру в файле, то вероятность того что анализируемый файл содержит вирус равна 0,9999999999997671. Метод позволяет с высокой эффективностью (на всем множестве всех возможных файлов) определять является ли сканируемый файл вирусом или нет, а также позволяет определять наличие вирусных фрагментов кода в файле. Главный недостаток метода — это обнаружение исключительно уже существующих вирусных программ, сигнатуры которых занесены в базу сигнатур. Метод не позволяет определять новый вирусный вредоносный код, а также модификации уже известных вирусов. Ввиду постоянно увеличивающегося числа модификаций одной и той же программы, а также невозможностью предсказать дальнейшие изменения в ее коде выделим и второй, существенный недостаток метода — необходимость ручной разработки сигнатур, а также создания нескольких сигнатур для одного и того же вирусного вредоносного кода.

#### СПИСОК ЛИТЕРАТУРЫ

1. *Расторгуев С.* Программные методы защиты информации в компьютерах и сетях. М.: Издательство Агентства «Яхтсмен», 1993.
2. *Касперски К.* Записки исследователя комп вирусов. СПб.: Питер, 2006, 316 с.