Расчет потерь энергии, идущей на нагрев АД, выполняют двумя способами: методом конечных сумм $\Delta P_i t_i$ на каждом i-ом интервале за цикл и непосредственным вычислением по программе интегралов $\int[\alpha(t)]^{1,5}dt$, $\int[\nu(t)]^2dt$, $\int[\mu(t)]^2dt$, которые умножаются на свои коэффициенты. В настоящее время второй способ имеет большее распространение.

УДК 004.89:728

Программное обеспечение для поиска и анализа аномалий в загрузочных областях диска

Велесик А.Т., Разорёнов Н.А.
Белорусский национальный технический университет

Под аномалией в загрузочной области диска подразумевается вредоносный код, внедрённый в загрузочный код Master Boot Record или Volume Boot Record. Вредоносные программы, заражающие загрузочный код MBR или VBR носят название «bootkit» (от англ. boot – загрузка и kit – набор инструментов).

В ходе исследования были изучены основные особенности вредоносных программ типа bootkit, проанализировано поведение основных их представителей, проведен анализ до и после заражения загрузочных областей диска вредоносной программой, определены механизмы, с помощью которых вредоносные программы типа bootkit внедряются в загрузочные области диска, а также изучены стандартные средства защиты от вредоносных программ типа bootkit.

По результатам исследования был сделан вывод, что стандартных средств защиты от вредоносных программ типа bootkit недостаточно и необходимо разработать программное обеспечение, которое позволяет определять заражён диск или нет.

Было разработано программное обеспечение для поиска и анализа аномалий в загрузочных областях диска, которое выполняет следующие функции: эмулирует загрузочный код выбранного физического диска и, на основании полученных данных при его эмуляции, делает заключение о наличии аномалий в загрузочных областях этого диска.