УДК 004.056.57

Э.Э. Шевцов, Н.И. Белодед

Академия управления при Президенте Республики Беларусь

ЗАЩИТА FLASH-НАКОПИТЕЛЕЙ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В настоящее время вирусы и другие виды вредоносного программного обеспечения представляют серьезную угрозу информационной безопасности. Как правило, используя в своей системе только один антивирус невозможно добиться высокой степени защищенности. В связи с этим ведутся разработки различного программного обеспечения для реализации комплексной безопасности.

При рассмотрении способов распространения вредоносного программного обеспечения доказано, что вирусы могут проникнуть из одной закрытой системы в другую только в случае переноса на каком-либо носителе. Ярким примером являются flash-накопители. В связи с этим возникает необходимость при помощи специального программного обеспечения исключить возможность распространения вредоносных программ таким способом.

Решением данной проблемы может послужить блокировщик записи. Основной целью данной программы является блокировка записи какой-либо информации сторонними процессами операционной системы на flash-накопитель.

Реализация основной функции программы заключается в заполнении всего свободного объема

памяти файлом, напоминающим по своей структуре образ. Таким образом, на flash-накопителе в корневом каталоге будут находиться только сам файл-образ и программа, осуществляющая запись.

Главной особенностью всего содержимого является невозможность их модификации либо удаления с этого носителя стандартными способами операционной системы.

Для осуществления записи необходимо запустить основную программу и воспользоваться ее интерфейсом. В ходе работы программы осуществляется строгая определенность действий:

- Проверка целостности содержимого накопителя.
- Считывание контрольной суммы файлов для копирования на жестком диске.
- Запись в файл.
- Проверка контрольной суммы.

В результате всех манипуляций на накопитель попадает только то, что пользователь собирался туда поместить. Интерфейс программы планируется максимально интегрировать с операционной системой, что на данный момент является основным приоритетом при разработке. Таким образом, мы имеем потенциально непреодолимую преграду против распространения вредоносного программного обеспечения.

Список литературы

1. *[Электронный ресурс]. – Режим доступа к ресурсу: http://protecttcp.org.ru*
2. *[Электронный ресурс]. – Режим доступа к ресурсу: www.viruslist.com*
3. *Козлов Д.А. Энциклопедия компьютерных вирусов / Д.А. Козлов, А.А. Парандовский, А.К. Парандовский – М.: СОЛОН – Р, 2005. – 464 с.*
4. *Касперски К. Компьютерные вирусы изнутри и снаружи / Крис Касперски. – СПб.: Питер, 2006. – 522 с.*
5. *[Электронный ресурс]. – Режим доступа к ресурсу: www.ru.wikipedia.org.*