Д. А. Э д е л ь, **А. Г. С а м о й л о в**, **А. А. К о в а л ь** (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»). **Анализ метода отправки данных вредоносным программным обеспечением через OLE интерфейс и защита от нее.**

В современной вирусологии основное внимание уделено только обнаружению вирусов и защите от их вторжения [1]. Но открытым остается вопрос можно ли противостоять им, если все же вредоносная программа проникла в компьютер. Проанализируем механизмы работы вредоносных вирусных программ собирающих данные с компьютера и пытающиеся отправить собранную информацию на IP-адрес удаленного компьютера в сети Интернет.

После выполнения своей основной задачи вирусные программы используют различные методы отправки данных на удаленный компьютер. Одной из них является способ отправки данных, используя вызов обозревателя Интернета Microsoft Internet Explorer в качестве универсального передатчика данных [2]. Программно вызов реализован созданием OLE — объекта Internet Explorer и управлением им. Так как на каждой операционной системе семейства Windows компания Microsoft поставляется обозреватель Internet Explorer, то проблема при работе с OLE — необходимость наличия установленного используемого программного обеспечения — исчезает. Отправление информации вредоносным программным обеспечением осуществляется по протоколу HTTP методом POST. В качестве конечного адреса отправки модуля зачастую выступает специализированный PHP скрипт, предназначенный для «захвата» пересылаемой ему информации. Использование для отправления данных обозревателя Интернета Internet Explorer обеспечивает обход межсетевого экрана Windows. Нестандартный вызов приложения Internet Explorer через OLE-интерфейс не создает дополнительного процесса, а потому не обнаруживается стандартными способами ни пользователями компьютера, ни защитными антивирусными средствами.

В связи с этим предлагается следующий способ перехвата отправки данных вредоносным программным обеспечением. На компьютере пользователя, подвергшегося заражению, заменяется стандартный обозреватель Интернета на «свой» — файл iexplore.exe, задача которого анализировать вызовы программы Microsoft Internet Explorer, и в случае вызова через OLE-интерфейс (в командной строке будет передано значение «-Embedding») выдавать сообщение пользователю, в котором спрашивается, осуществить вызов или нет.

Таким образом, несанкционированная утечка данных с компьютера пользователя будет предотвращена.

СПИСОК ЛИТЕРАТУРЫ

1. *Мюллер Дж.* Технология COM+. СПб.: Питер, 2002, 464 с.
2. *Касперски К.* Компьютерные вирусы изнутри и снаружи. Спб.: BHV–Питер, 2006, 526 с.