

Programy antywirusowe

Najlepszą metodą ochrony przed niebezpiecznym oprogramowaniem jest korzystanie z antywirusów. Często jedynym rozwiązaniem jest ponowna instalacja całego systemu.

Programy antywirusowe możemy podzielić na następujące grupy funkcjonalne:

Blokery - są to jedyne programy, próbujące przeciwdziałać inwazji.

Zasadą ich działania jest monitorowanie poczynąń uruchamianych programów i w przypadku odkrycia "podejrzanych" operacji alarmowanie użytkownika i pozostawianie mu decyzji o dalszym działaniu. Jest to znakomita metoda, ale jak każda posiada oczywiście swoje wady. Jedną z nich jest przede wszystkim mała skuteczność, gdyż nowe wirusy bardzo często posiadają mechanizmy uniemożliwiające wyodrębnienie z nich operacji "podejrzanych". Kolejną wadą jest zajmowanie części zasobów komputera - pamięci operacyjnej oraz obciążanie w jakimś stopniu procesora. Ostatnią wadą jest to, iż programy owe mają tendencję do częstego "mylenia się" co związane jest z "fałszywym alarmem".

Programy diagnostyczno-leczące - ta grupa programów opiera się na poszukiwaniu na dysku i w pamięci znanych już wirusów i w przypadku wykrycia (na podstawie charakterystycznych algorytmów zawartych w plikach) - usuwaniu skutków infekcji.

Są to programy najczęściej stosowane i najbardziej przydatne w profilaktyce.

Niestety są nieskuteczne w przypadku zainfekowania nieznanym wirusem bądź wtedy, gdy wirus zadziała natychmiast po zainfekowaniu komputera i dokona nieodwracalnych zniszczeń.

Do programów tego typu zaliczamy, już chyba legendę programów antywirusowych - Mks_Vir-a, autorstwa Marka Sella.

Programy sprawdzające sumy kontrolne plików - istotą tej grupy programów jest zakładanie bazy danych, zawierających pewne cechy zbiorów dyskowych i newralgicznych obszarów dysków.

Te programy, przez systematycznym stosowaniu, umożliwiają wykrycie źródła infekcji, a czasem odzyskanie pozornie bezpowrotnie straconych informacji.

Skaner rezydentny - skaner, który pracuje w tle przez cały czas.