Tato práce rekapituluje vybrané metody pro sledování chování procesů na operačních systémech Windows. Zvláštní pozornost je věnována použití virtualizace jako pomocného prostředku k řešení problému. Cílem práce bylo zhodnotit možnosti jednotlivých metod a navrhnout systém pro sledování chování procesů za pomoci virtualizace. Navržený systém je postaven na virtualizačním software VirtualBox od Sun Microsystems a operačním systému Windows XP Service Pack 3. Běh virtualizovaného systému Windows je upraven tak, že v přesně definovaných stavech jsou na základě aktuálního stavu paměti vytvářeny elementární události sledovacího systému. Tyto události lze dále analyzovat a pomocí nich modelovat objekty existující v systému a jejich interakce. Zjištěné interakce mezi sledovanými procesy a objekty v systému determinují chování těchto procesů.