Профилирование Native-приложений

Одной из технологий автоматической защиты исполняемых **Native-файлов** является обработка инструкций, извлеченных из тела приложения **RIP CODE.** При помощи мини-виртуальной машины некоторые наборы инструкций в защищаемом приложении преобразуются определенным образом. Это позволяет защитить функции приложения от изучения и анализа, а также значительно затрудняет создание автоматических инструментов снятия автозащиты.

Однако при использовании **RIP CODE** следует учитывать, что работа защищенного приложения может замедляться, вследствие того, что инструкции виртуализируются. Чтобы подобрать оптимальные функции для защиты применяется технология профилирования. С помощью специальных инструментов приложение анализируется (как статически, при помощи дизассемблера, так и динамически, в процессе исполнения), после чего создается конфигурационный файл **PRC** (*.prc), содержащий информацию о функциях, подлежащих защите.

Новым шагом в развитии перспективной технологии виртуализации защищаемых участков кода стал выпуск утилиты **Guardant Armor**. Для защиты приложения при помощи данной утилиты необходимо создать конфигурационный файл **PRC.**

Рассмотрим процесс защиты и профилирования тестового приложения, созданного в Visual Studio 2010 по шаблону **MFC Application**.