

# Не «очищать» приложение

## Не «очищать» приложение:

/NOS

## Тип электронного ключа:

Все

## Описание:

Обычно автозащита удаляет из **Native-приложений** данные, не входящие в состав сегментов. Это позволяет в большинстве случаев удалить забытую отладочную информацию и даже зачастую сэкономить на размере защищенного приложения: файл станет меньше, чем был до защиты.

Однако в некоторых случаях подобное «очищение» негативно сказывается на дальнейшей работе приложений, т. к. некоторые из них могут хранить свои важные данные нестандартным образом в произвольном месте **EXE-файла**. Например, в **FoxPro-приложениях**, интерпретируемый байт-код хранится нестандартно – не в соответствующем сегменте, а просто в конце **EXE-файла**.

Опция / **NOS** (*No Strip*, не очищать приложение) позволяет отменить операцию «очистки». Если защищенное Windows-приложение работает некорректно, защитите его с опцией /**NOS**.

## Пример:

**NwKey32.exe /GS3S /NOS MyProg.exe**

Пример защиты **Native-приложения** с ключом *Guardant Sign*. При защите из приложения не будут удалены данные, не входящие в состав его сегментов (т. е. приложение не будет «очищено»).