Nwkey32.exe

Порядок защиты

Перед началом защиты подсоедините к компьютеру электронный ключ нужного типа.

Формат вызова утилиты автоматической защиты:

```
NwKey32.exe [] []_
```

или

```
NwKey32.exe [] @[]filename.fil
```

Укажите в командной строке необходимые для защиты параметры и нажмите на кнопку **[Enter]**. Утилита приступит к защите, выдавая по ходу работы необходимые сообщения:

- Значения полей памяти ключа, участвующих в защите. Это могут быть значения из реально подсоединенного ключа, либо значения, указанные в опциях.
- Список указанных опций защиты (режимы привязки к ключу, кодирования приложений).
- Список сообщений, которые может выдавать внешняя вакцина при работе защищенных приложений.
- Имя каталога, в который будут помещены защищенные приложения (выходной путь).
- Сообщения об ошибках, возникших в процессе защиты.

Утилита завершит защиту текущего файла и закончит работу.

Процесс защиты можно прервать в любой момент, нажав **Esc.**

Принцип защиты

Основа автоматической защиты исполняемых **Native-приложений** – вакцина, выполненная в виде универсального внешнего модуля. Все функции защиты поддерживаются этим модулем, что позволяет унифицировать процесс защиты.

Автозащита исполняемых **Native-приложений** работает следующим образом: в тело защищаемого приложения вписывается небольшой исполняемый модуль (внутренняя вакцина). В момент запуска приложения он загружает из отдельного файла внешнюю вакцину. И уже эта внешняя вакцина производит необходимые проверки и преобразования кода защищенного приложения и запускает его. Кроме того, использование внешнего модуля защиты усиливает стойкость к изучению логики ее работы при помощи отладчиков.

Файл вакцины для исполняемых **Native-приложений** называется **GrdVkc32.dll** и входит в комплект автоматической защиты.

> В момент запуска защищенного приложения вакцина GrdVkc32.dll должна находиться там, где ее может найти функция LoadLibrary (это может быть текущий каталог, системные каталоги Windows, каталог, в котором находится само защищенное приложение, один из каталогов списка PATH).

Ограничения

Автозащита исполняемых файлов Native-приложений имеет следующие ограничения:

- Не поддерживаются самораспаковывающиеся архивы **ZIP, RAR** и т. д.
- Не поддерживаются программы-мастера установки приложений, созданные в специализированных средах разработки: **Wise Installer, Install Shield** и других.
- Не гарантируется корректная защита или последующая работа приложения, которое перед защитой было упаковано специальным упаковщиком *EXE-файлов:***UPX, ASPACK** и др.
- Не гарантируется корректная защита **EXE-** файлов, кодкоторых был предварительно защищен от модификации или анализа.

Автозащита должна выполняться на ключе той же модели, что будет поставляться с защищенной программой. Для успешной установки и работы автозащиты в ключе, к которому привязывается приложение, должен содержаться алгоритм типа **GSII64** или **AES.** Определитель аппаратного алгоритма в ключе, используемом при защите, должен быть идентичен определителю этого же алгоритма в ключе из комплекта поставки защищенного приложения.