

Автоматические инструменты

Для защиты разных типов приложений, работающих в ОС Windows, применяются различные автоматические средства:

	.NET-приложение		Native-приложение	
	x86	x64	x86	x64
Консольная утилита	Утилиты для защиты .Net-приложений		Guardant Armor nwkey32.exe (устаревшая)	Guardant Armor
GUI-утилита	Мастер автозащиты (LicenseWizard.exe)			-

Автоматическая защита может быть установлена на приложение только при наличии в порту ключа нужной модели. Несмотря на свои богатые возможности, рекомендуем усилить защиту при помощи [Guardant API](#).

Использование утилит автоматической защиты в консольном режиме (в режиме командной строки) подразумевает самостоятельное [программирование](#) электронных ключей при помощи специальной утилиты [GrdUtil.exe](#).

Возможности автозащиты

Автоматическая защита Guardant предоставляет широкие возможности для защиты приложений. Она имеет несколько режимов, позволяющих настроить процесс защиты, а также способ привязки защищаемого приложения к электронному ключу, частоту и характер производимых проверок и возвращаемых сообщений в случае неудачного завершения проверок. Конечной целью является ограничение числа запусков или времени работы защищенного приложения и защита приложения от анализа и отладки.

Возможности автоматической защиты, в общем случае, можно классифицировать следующим образом:

- Схема лицензирования приложения
- Возможность привязки к одному ключу любого количества защищенных приложений с независимыми друг от друга лицензиями
- Наличие различных режимов лицензирования по локальной сети

Ограничение работы защищенного приложения:

- По времени использования (для Guardant Time)
- По количеству запусков (для всех типов ключей)
- С использованием периодических проверок наличия ключа
- С использованием принудительного завершения работы приложения через заданный интервал времени после обнаружения нарушения

Способы привязки приложения к ключу:

- К статическим данным ключа
- С использованием алгоритмов ключа

Защита приложения использует:

- Шифрование кода и данных приложения
- Технологию псевдокода (противодействие статическому и динамическому анализу)
- Контроль целостности приложения

Режимы работы автоматической защиты приложений:

- с записью созданной лицензии в ключ
- на основе ранее записанных в ключ данных
- без привязки к электронному ключу (режим предполагает, что привязка к ключу полностью реализуется при помощи Guardant API и необходимость дублирования вызовов ключа отсутствует)

Содержание раздела

См. также

- [API](#)

