

Вечная лицензия

Модель лицензирования может быть реализована при помощи нескольких утилит автоматической защиты. Выбор конкретной утилиты или набора утилит зависит от типа приложения (native или .Net) и его разрядности (x86 или x64). На вкладках с названиями утилит описаны действия, которые нужно выполнить чтобы реализовать защиту своего приложения и установить нужные условия лицензирования:

- [LicenseWizard.exe](#) — графическое приложение (оболочка), для удобной защиты и лицензирования как native, так и .Net приложений. Режимы работы перечислены на странице [как сделать](#).
- [grdarmor.exe](#) — современная консольная утилита автоматической защиты x86 и x64 native приложений
- [CodeObfuscator.exe](#) — консольная утилита обфускации кода .Net приложений
- [CodeProtect.exe](#) — консольная утилита защиты и шифрования кода .Net приложений
- [nwkey32.exe](#) — консольная утилита "прошлого поколения" для защиты только x86 native приложений

LicenseWizard.exe

Полностью автоматический режим

Внимание!

В этом режиме настройка лицензионных ограничений, программирование памяти ключа и защита выполняются только при помощи GUI-утилиты **LicenseWizard.exe** («Мастер лицензирования и автоматической защиты»)

1

Запустить «Guardant Интегратор»

2

Нажать [Мастер лицензирования и автоматической защиты]

3

Нажать [Пустой проект]

4

- «Способ программирования ключей» оставить «Алгоритмы и данные в ключе генерируются автоматически мастером»
- «Средство лицензирования (как защищаться от копирования)» в выпадающем списке «Использовать аппаратный ключ модели:» указать модель ключа
- Нажать [Продолжить]

5

- Указать имя проекта и каталог, в котором сохраняются файлы проекта
- Нажать [Продолжить]

6

- Выбрать нужный ключ из списка подсоединенных и, если нужно, включить опцию «Использовать ключ в HID режиме»
- Нажать [Продолжить]

7

Введите свои значения или оставьте стандартные настройки для

8

- Нажать [Добавить] и в проводнике Windows выбрать защищаемые файлы
- На вкладке «Лицензирование» не применять дополнительные настройки лицензирования (для усиления защиты лучше включить опцию «Использовать алгоритм ЭЦП»)
- Включить нужные опции защиты на вкладке «Защита»
- Настроить сервисные опции на вкладке «Сервис»

- Нажать [Продолжить]

9

После завершения работы мастера защищенное приложение и дополнительные файлы будут в каталоге указанном на шаге №5, в подкаталоге **«Result»**

Ключ программируется самостоятельно

Внимание!

В этом режиме настройка лицензионных ограничений производится при программировании памяти ключа через утилиту **«Редактор памяти ключей Guardant» (grdutil.exe)**, а защита выполняется GUI-утилитой **LicenseWizard.exe** (**«Мастер лицензирования и автоматической защиты»**)

1

Запустить **«Guardant Интегратор»**

2

Нажать [Программирование электронных ключей]

3

При помощи утилиты программирования электронных ключей **«Редактор памяти ключей Guardant» (grdutil.exe)** создать новый образ нажав [Ctrl+N], или:

- Меню [Файл]
- [Создать образ...]

Внимание!

В диалоговом окне создания нового образа нужно выбрать тип ключа из нижней области **«Создание пустого образа»**

4

Создать поле с аппаратным алгоритмом симметричного шифрования **AES128**:

- Для усиления защиты лучше еще создать поле с аппаратным алгоритмом выработки ЭЦП **ECC160**
- Двойным кликом на поле открыть его свойства
- Вкладка **«Ключ ECC160»**
- Нажать [Экспорт в bin-файл автозащиты] и выполнить сохранение *.bin-файла открытого ключа

5

Записать образ в ключ нажав [Ctrl+W], или:

- Меню **«Ключ»**
- Если нужно, включить опцию **«Записывать ключи как HID»**
- Нажать [Записать образ в ключ]

6

В **«Guardant Интегратор»** нажать [Мастер лицензирования и автоматической защиты]

7

Нажать [Пустой проект]

8

Настройка параметров нового проекта:

- «Способ программирования ключей» выбрать «Ключ программируется разработчиком самостоятельно»
- «Средство лицензирования (как защищаться от копирования)» в выпадающем списке «Использовать аппаратный ключ модели:» указать модель ключа
- Нажать [Продолжить]

9

Создание нового проекта:

- Указать имя проекта и каталог, в котором сохраняются файлы проекта
- Нажать [Продолжить]

10

Выбор ключа:

- Выбрать нужный ключ из списка подсоединенных
- Нажать [Продолжить]

11

Выбор защищаемых приложений:

- Нажать [Добавить] и в проводнике Windows выбрать защищаемые файлы
- На вкладке «Лицензирование» указать размер вопроса алгоритма (16, 32 или 64 для **AES128**) и номер (числовое имя) (узнать номер алгоритма можно в **grdutil.exe**, посмотрев столбец [Тип] — например, если для нужного алгоритма в столбце [Тип] указано **Алгоритм 00 (AES128)**, то номер будет 0)
- Для усиления защиты лучше включить опцию «Использовать алгоритм ЭЦП», нажать [...] и в проводнике Windows выбрать ранее сохраненный (п. 4) *.bin-файла открытого ключа
- Включить нужные опции защиты на вкладке «Защита»
- Включить нужные сервисные опции на вкладке «Сервис»
- Нажать [Продолжить]

12

После завершения работы мастера защищенное приложение и дополнительные файлы будут в каталоге указанном на шаге №9, в подкаталоге «**Result**»

grdarmor.exe

Внимание!

В этом режиме настройка лицензионных ограничений производится при программировании памяти ключа через утилиту «Редактор памяти ключей Guardant» (**grdutil.exe**), а защита выполняется консольной утилитой **grdarmor.exe** («Guardant Armor»)

1

Запустить «Guardant Интегратор»

2

Нажать [Программирование электронных ключей]

3

При помощи утилиты программирования электронных ключей «Редактор памяти ключей Guardant» (**grdutil.exe**) создать новый образ нажав [Ctrl+N], или:

- Меню [Файл]

- [\[Создать образ...\]](#)

Внимание!

В диалоговом окне создания нового образа нужно выбрать тип ключа из нижней области **«Создание пустого образа»**

4

[Создать](#) поле с аппаратным алгоритмом симметричного шифрования **AES128**:

- Для усиления защиты лучше еще создать поле с аппаратным алгоритмом выработки ЭЦП **ECC160**
- Двойным кликом на поле открыть его свойства
- Вкладка **«Ключ ECC160»**
- Нажать **[Экспорт в bin-файл автозащиты]** и выполнить сохранение *.bin-файла открытого ключа

5

Записать образ в ключ нажав **[Ctrl+W]**, или:

- Меню **«Ключ»**
- Если нужно, включить опцию **«Записывать ключи как HID»**
- Нажать **[Записать образ в ключ]**

6

Подготовить защищаемое приложение — выполнить его сборку с генерацией MAP-файла сопоставления

7

Подготовить файл (***.prc** или ***.ini**) с перечислением защищаемых функций

8

Запустить стандартное Windows-приложение **«Командная строка»** и перейти в папку **«Bin»**, установленного Guardant SDK («по умолчанию» C:\Program Files (x86)\Guardant\SDK7\Bin)

Внимание!

Для выполнения защиты 64-битных приложений необходимо перейти в папку **«x64»**, установленного Guardant SDK («по умолчанию» C:\Program Files (x86)\Guardant\SDK7\Bin\x64)

9

Запустить **grdarmor.exe** с параметрами привязки, защиты и нужным файлом защищаемых функций (***.prc** или ***.ini**)

```
grdarmor.exe -ENVELOPE_MODE=H:5:8 -GS3S -OUT=.\PrcProtect -PRC=a
pp.prc -MAP=app.map app.exe
```

Используется *.prc-файл, аппаратный режим работы конверта и USB-ключ Guardant Sign

```
grdarmor.exe -ENVELOPE_MODE=S -GS3S -OUT=.\IniProtect -
INI=app.ini -MAP=app.map app.exe
```

Используется *.ini-файл, программный режим работы конверта и USB-ключ Guardant Sign

CodeObfuscator.exe

Внимание!

В этом режиме настройка лицензионных ограничений производится при программировании памяти ключа через утилиту **«Редактор памяти ключей Guardant» (grdutil.exe)**, а обфускация кода .Net-приложения выполняется консольной утилитой **CodeObfuscator.exe**

Важно!

Если совместно с [обфускацией](#) кода .Net-приложения будет производиться и его [защита](#) с переносом кода в защищенное хранилище, то должна соблюдаться следующая последовательность использования утилит:

1. Утилита обфускации **CodeObfuscator.exe**
2. Утилита защиты кода **CodeProtect.exe**

1

Запустить «Guardant Интегратор»

2

Нажать [Программирование электронных ключей]

3

При помощи утилиты программирования электронных ключей «Редактор памяти ключей Guardant» (**grdutil.exe**) создать новый образ нажав **[Ctrl+N]**, или:

- Меню [Файл]
- [\[Создать образ...\]](#)

Внимание!

В диалоговом окне создания нового образа нужно выбрать тип ключа из нижней области «Создание пустого образа»

4

[Создать](#) поле с аппаратным алгоритмом симметричного шифрования **AES128**:

- Для усиления защиты лучше еще создать поле с аппаратным алгоритмом выработки ЭЦП **ECC160**
- Двойным кликом на поле открыть его свойства
- Вкладка «Ключ ECC160»
- Нажать [\[Экспорт в bin-файл автозащиты\]](#) и выполнить сохранение *.bin-файла открытого ключа

5

Записать образ в ключ нажав **[Ctrl+W]**, или:

- Меню «Ключ»
- Если нужно, включить опцию «Записывать ключи как HID»
- Нажать [\[Записать образ в ключ\]](#)

6

Запустить стандартное Windows-приложение «Командная строка» и перейти в папку «Bin», установленного Guardant SDK («по умолчанию» C:\Program Files (x86)\Guardant\SDK7\Bin)

7

Запустить **CodeObfuscator.exe** с параметрами привязки и защиты

```
CodeObfuscator.exe /GS3S=0:16::1:app.exe.bin /INIT /SO /SE /ATR=1 /OUT=../Result /MAP=app.map app.exe
```

.Net-приложение обфусцируется с применением шифрования строковых констант при помощи аппаратного электронного USB-ключа Guardant Sign

Внимание!

В этом режиме настройка лицензионных ограничений производится при программировании памяти ключа через утилиту «Редактор памяти ключей Guardant» (grdutil.exe), а защита кода .Net-приложения выполняется консольной утилитой **CodeProtect.exe**

Важно!

Если совместно с защитой кода .Net-приложения будет производиться и его обфускация, то должна соблюдаться следующая последовательность использования утилит:

1. Утилита обфускации **CodeObfuscator.exe**
2. Утилита защиты кода **CodeProtect.exe**

1

Запустить «Guardant Интегратор»

2

Нажать [Программирование электронных ключей]

3

При помощи утилиты программирования электронных ключей «Редактор памяти ключей Guardant» (grdutil.exe) создать новый образ нажав [Ctrl+N], или:

- Меню [Файл]
- [Создать образ...]

Внимание!

В диалоговом окне создания нового образа нужно выбрать тип ключа из нижней области «Создание пустого образа»

4

Создать поле с аппаратным алгоритмом симметричного шифрования **AES128**:

- Для усиления защиты лучше еще создать поле с аппаратным алгоритмом выработки ЭЦП **ECC160**
- Двойным кликом на поле открыть его свойства
- Вкладка «Ключ ECC160»
- Нажать [Экспорт в bin-файл автозащиты] и выполнить сохранение *.bin-файла открытого ключа

5

Записать образ в ключ нажав [Ctrl+W], или:

- Меню «Ключ»
- Если нужно, включить опцию «Записывать ключи как HID»
- Нажать [Записать образ в ключ]

6

Запустить стандартное Windows-приложение «Командная строка» и перейти в папку «Bin», установленного Guardant SDK («по умолчанию» C:\Program Files (x86)\Guardant\SDK7\Bin)

7

Запустить **CodeProtect.exe** с параметрами привязки и защиты

```
CodeProtect.exe /GS3S=0:16::1:app.exe.bin /PER=10 /ATR=1 /OUT=../Result /MAP=app.map app.exe
```

10 процентов методов .Net-приложения будут зашифрованы при помощи аппаратного электронного USB-ключа Guardant Sign и размещены в защищенном контейнере

nwkey32.exe

Внимание!

В этом режиме настройка лицензионных ограничений производится при программировании памяти ключа через утилиту «Редактор памяти ключей Guardant» (grdutil.exe), а защита выполняется консольной утилитой [nwkey32.exe](#)

1

Запустить «Guardant Интегратор»

2

Нажать [Программирование электронных ключей]

3

При помощи утилиты программирования электронных ключей «Редактор памяти ключей Guardant» (grdutil.exe) создать новый образ нажав [Ctrl+N], или:

- Меню [Файл]
- [\[Создать образ...\]](#)

Внимание!

В диалоговом окне создания нового образа нужно выбрать тип ключа из нижней области «Создание пустого образа»

4

[Создать](#) поле с аппаратным алгоритмом симметричного шифрования **AES128**:

- Для усиления защиты лучше еще создать поле с аппаратным алгоритмом выработки ЭЦП **ECC160**
- Двойным кликом на поле открыть его свойства
- Вкладка «Ключ ECC160»
- Нажать [\[Экспорт в bin-файл автозащиты\]](#) и выполнить сохранение *.bin-файла открытого ключа

5

Записать образ в ключ нажав [Ctrl+W], или:

- Меню «Ключ»
- Если нужно, включить опцию «Записывать ключи как HID»
- Нажать [\[Записать образ в ключ\]](#)

6

Запустить стандартное Windows-приложение «Командная строка» и перейти в папку «Bin», установленного Guardant SDK («по умолчанию» C:\Program Files (x86)\Guardant\SDK7\Bin)

7

Запустить [nwkey32.exe](#) с параметрами привязки и защиты

```
nwkey32.exe /GS3S=0:16::1:app.exe.bin /IMPORT_HOOK=30:5 /RIP_CODE=10 /T=5 /ATR=1 /OUT=../Result /MAP=app.map app.exe
```

Приложение будет защищено с использованием аппаратного электронного USB-ключа Guardant Sign. При этом будет защищено 30 процентов импортируемых функций по 5 инструкций из каждой функции, а также для инструкций в теле приложения существует 10-процентная вероятность переноса в виртуальную машину
