Продажа обновлений

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

Важно!

Схема защиты базируется на проверке номера версии хранящегося в памяти электронного ключа. Механизм проверки позволяет работать с новой версией приложения только если в ключе будет записано соответствующее значение. При этом младшие версии будут работать с этим же ключом (т.е. **приложение v.1** будет работать с ключом для **приложения v.1.1**).

LicenseWizard.exe

Полностью автоматический режим

Внимание!

При реализации этой схемы лицензирования не рекомендуется использовать полностью автоматический режим.

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

Указать нужное значение версии:

- Двойным кликом на поле **«Версия»** открыть его свойства
- В открывшемся диалоговом окне ввести нужное значение в специальное текстовое поле
- Нажать **[OK]**

Внимание!

При создании образа значение версии автоматически устанавливается как **1**

5

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

6

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

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

7

Запустить **LicenseWizard.exe**

8

Нажать **[Пустой проект]**

9

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]**

10

Создание нового проекта:

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

11

Выбор ключа:

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

12

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]** указанно **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. 5) *.bin-файл открытого ключа
- Нажать **[Дополнительные настройки]**
- Активировать опцию **«Проверять поле версия»** и задать нужный номер версии в соответствующем текстовом поле
- Нажать **[<< Вернуться]**
- Включить нужные опции защиты на вкладке **«Защита»**
- Включить нужные сервисные опции на вкладке **«Сервис»**
- Нажать **[Продолжить]**

13

После завершения работы мастера защищенное приложение и дополнительные файлы будут в каталоге указанном на шаге №10, в подкаталоге **«Result»**

Выпуск новой версии приложения

Внимание!

Для защиты новой версии приложения необходимо использовать тот же образ (маску) ключа, который применялся при защите предыдущей версии. Нужно только записать большее значение в поле «Версия» и выполнить защиту как описано выше, с указанием нового значения версии в дополнительных настройках лицензирования. Записать новую версию в ключ клиента нужно при помощи удаленн ого обновления.

1

Запустить **«Guardant Интегратор»**

2

Нажать **[Программирование электронных ключей]**

3

При помощи утилиты программирования электронных ключей **«Редактор памяти ключей Guardant» (grdutil.exe)** найти и открыть со зданный на этапе защиты или выпуска предыдущей версии образ нажав **[Ctrl+F]**, или:

- Меню **«База данных»**
- Нажать **[Поиск записанных образов]**

4

Указать новое значение версии:

- Двойным кликом на поле **«Версия»** открыть его свойства
- В открывшемся диалоговом окне ввести нужное значение в специальное текстовое поле
- Нажать **[OK]**

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 **LicenseWizard.exe**

7

В области **«Последние проекты»** выбрать имя нужного проекта защиты (имя проекта задается на этапе защиты) и нажать на него

8

Несколько раз подряд нажать продолжить и дойти до диалогового окна выбора приложений:

- В области **«Приложения:»** нажать **[удалить]** в строке с указанием старой версии приложения
- Нажать **[Добавить]** и в проводнике Windows выбрать защищаемые файлы новой версии приложения
- Нажать **[Дополнительные настройки]**
- Задать нужный номер версии в соответствующем текстовом поле
- Нажать **[<< Вернуться]**
- Если нужно то перенастроить опции защиты на вкладке **«Защита»**
- Если нужно то перенастроить сервисные опции на вкладке **«Сервис»**
- Нажать **[Продолжить]**

9

После завершения работы мастера защищенное приложение и дополнительные файлы будут в каталоге с проектом защиты, в подкаталоге **«Result»**

Важно!

Защищенное приложение и дополнительные файлы в **«Result»**, сформированные на этапе защиты или выпуска предыдущей версии, будут удалены и заменены новыми. При необходимости нужно выполнить сохранение этих файлов до начала защиты новой версии.

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

Добавить нужное значение в поле **«Версия»**:

- Выделить поле в редакторе
- Меню **«Образ ключа»**
- Нажать **[Свойства поля]**
- В текстовом поле задать нужное значение и нажать **[OK]**

Свойства поля можно также открыть двойным щелчком мыши

6

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

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

7

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

8

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

9

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)

10

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

grdarmor.exe ***-ENVELOPE_MODE=H:5:8 -GS3S -uv=1*** *-OUT=./PrcProtect* ***-PRC=app.prc*** *-MAP=app.map app.exe*	*grdarmor.exe* ***-ENVELOPE_MODE=S -GS3S -uv=1*** *-OUT=./IniProtect* ***-INI=app.ini*** *-MAP=app.map app.exe*
Используется *.prc-файл, аппаратный режим работы конверта и USB-ключ Guardant Sign. Защищенное приложение запустится если в ключе записано значение версии **>=1**	Используется *.ini-файл, программный режим работы конверта и USB-ключ Guardant Sign. Защищенное приложение запустится если в ключе записано значение версии **>=1**

Выпуск новой версии приложения

Для защиты новой версии приложения необходимо использовать тот же образ (маску) ключа, который применялся при защите предыдущей версии. Нужно только записать **большее** значение в поле **«Версия»** и выполнить защиту как описано выше, с указанием нового значения версии (например, **-uv=2**). Записать новую версию в ключ клиента нужно при помощи удаленного обновления.

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 производится 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

Добавить нужное значение в поле **«Версия»**:

- Выделить поле в редакторе
- Меню **«Образ ключа»**
- Нажать **[Свойства поля]**
- В текстовом поле задать нужное значение и нажать **[OK]**

Свойства поля можно также открыть двойным щелчком мыши

6

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

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

7

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

8

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

*CodeObfuscator.exe **/GS3S=0:16::1:app.exe.bin** /INIT /SO **/SE** /ATR=1 **/UV=1** /OUT=./Result /MAP=app.map app.exe*
.Net-приложение обфусцируется с применением шифрования строковых констант при помощи аппаратного электронного USB-ключа Guardant Sign. Защищенное приложение запустится если в ключе записано значение версии **>=1**

Выпуск новой версии приложения

Для защиты новой версии приложения необходимо использовать тот же образ (маску) ключа, который применялся при защите предыдущей версии. Нужно только записать **большее** значение в поле **«Версия»** и выполнить защиту как описано выше, с указанием нового значения версии (например, ***/UV=2***). Записать новую версию в ключ клиента нужно при помощи удаленного обновления.

CodeProtect.exe

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 производится 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

Добавить нужное значение в поле **«Версия»**:

- Выделить поле в редакторе
- Меню **«Образ ключа»**
- Нажать **[Свойства поля]**
- В текстовом поле задать нужное значение и нажать **[OK]**

Свойства поля можно также открыть двойным щелчком мыши

6

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

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

7

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

8

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

*CodeProtect.exe **/GS3S=0:16::1:app.exe.bin /PER=10** /ATR=1 **/UV=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. Защищенное приложение запустится если в ключе записано значение версии **>=1**

Выпуск новой версии приложения

Для защиты новой версии приложения необходимо использовать тот же образ (маску) ключа, который применялся при защите предыдущей версии. Нужно только записать **большее** значение в поле **«Версия»** и выполнить защиту как описано выше, с указанием нового значения версии (например, ***/UV=2***). Записать новую версию в ключ клиента нужно при помощи удаленного обновления.

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

Добавить нужное значение в поле **«Версия»**:

- Выделить поле в редакторе
- Меню **«Образ ключа»**
- Нажать **[Свойства поля]**
- В текстовом поле задать нужное значение и нажать **[OK]**

Свойства поля можно также открыть двойным щелчком мыши

6

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

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

7

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

8

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* ***/UV=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. Защищенное приложение запустится если в ключе записано значение версии **>=1**

Выпуск новой версии приложения

Для защиты новой версии приложения необходимо использовать тот же образ (маску) ключа, который применялся при защите предыдущей версии. Нужно только записать **большее** значение в поле **«Версия»** и выполнить защиту как описано выше, с указанием нового значения версии (например, ***/UV=2***). Записать новую версию в ключ клиента нужно при помощи удаленного обновления.