

# Grdarmor.exe

Guardant Armor – это решение для защиты программного обеспечения от анализа и модификации путем обфускации и виртуализации кода.

Утилита **grdarmor.exe** бывает 2 видов в зависимости от функциональности:

- **защита кода и привязка ПО к ключу**  
входит в состав **Guardant SDK** (версии не ниже 7 Update 3), является консольной, предоставляется бесплатно поддерживает все указанные ниже опции
- **только защита кода**  
предоставляется по запросу (<https://www.guardant.ru/products/all/guardant-armor/request/>) поддерживает только опции защиты (в таблицах ниже выделены **жирным**)

## Запуск

Запустить **grdarmor.exe** можно через стандартную командную строку, Windows Power Shell или при помощи заранее подготовленных пакетных файлов (\*.BAT, \*.CMD). Расположение версий:

Версия	Расположение
x86	C:\Program Files (x86)\Guardant\SDK7\Bin
x64	C:\Program Files (x86)\Guardant\SDK7\Bin\x64

## Порядок защиты

Для защиты файлов утилитой Guardant Armor необходимо провести ряд действий:

№	Действие
1	Выполнить сборку защищаемого приложения в среде разработки с активированной опцией генерации MAP-файла сопоставления (например, для Visual Studio варианты включения данной опции описаны в MSDN <a href="#">по ссылке</a> ).
2	Подготовить ключ, к которому будет осуществляться привязка файлов:  После применения Guardant Armor приложение будет готово к продаже. Поэтому перед его использованием необходимо при помощи утилиты для <a href="#">программирования ключей</a> сформировать <b>образ</b> для нужной модели электронного ключа, который будет содержать набор <b>аппаратных алгоритмов</b> шифрования с <b>определителями</b> , и <b>записать (прошить)</b> этот образ в ключ. Понадобится, как минимум, один алгоритм для <b>симметричного шифрования</b> , т.к. он будет использоваться для защиты приложения. Также аппаратные алгоритмы используются для установки лицензионных ограничений для защищенного приложения.
3	Подготовить один из файлов, указанных ниже и содержащих перечень защищаемых функций: <ul style="list-style-type: none"><li>• PRC-файл Имеет расширение *.prc, создается в результате обработки защищаемого приложения <a href="#">утилитой профилирования</a>. В случае необходимости его можно редактировать. При защите измененного приложения (например, новой версии, в которую добавлены и/или переработаны функции) можно воспользоваться «старым» PRC-файлом, но в таком случае защитятся <b>только</b> те функции, hash которых <b>не изменился</b>. При формировании PRC-файла необходимо использовать MAP-файл (генерируется в среде разработки приложения, см. пункт №1). Это позволит утилите профилирования оперировать осмысленными именами функций, которые используются в приложении и известны разработчику.</li><li>• INI-файл Имеет расширение *.ini, создается разработчиком вручную <b>в кодировке ANSI</b>. На отдельных строках указывается опция включения (+r) и через пробел имя функции со всеми искажениями из MAP-файла (генерируется в среде разработки приложения): +r &lt;имя функции&gt;  Пример: <code>+p ?OnPaint@CWnd@Win32xx@@@MAEJIIJ@Z</code>  При повторном использовании INI-файла будет произведена попытка защиты всех указанных функций вне зависимости от того, менялся их hash или нет.</li></ul>
4	Использовать утилиту <b>grdarmor.exe</b> (см. ниже)

## Использование утилиты

### Внимание!

- Нельзя выполнять защиту файлов, которые ранее уже были защищены другими протекторами, в том числе утилитами автозащиты Guardant.
- Для защиты с использованием опции "-MAP" необходимо при сборке приложения включать опцию генерации MAP-файла.
- Опция режима работы конверта "-ENVELOPE\_MODE" должна быть задана всегда.
- Всегда должна быть указана опция "-PRC" или "-INI".
- В одном каталоге с утилитой grdarmor.exe должен находиться файл nvcodes.dat (по умолчанию лежит только в папке \Bin).
- Опции, особенным образом **выделенные** в таблицах, работают и в обычной версии Guardant Armor и в версии, которая защищает файлы без привязку к ключу

При работе с утилитой можно применять различные схемы защиты:

Файлы привязываются к <b>одному ключу</b> и имеют <b>одинаковые опции защиты</b>	Файлы привязываются к <b>разным ключам</b> и имеют <b>разные опции защиты</b>
grdarmor.exe <опции защиты>  <опции поиска ключа> <модель ключа>[=<параметры привязки>]  <опции защиты файлов> [<файл 1>] ... [<файл N>]	grdarmor.exe <опции защиты>  <опции поиска ключа> <модель ключа>[=<параметры привязки>]  <опции защиты файлов> [<файл 1>] [<файл 2>]  <опции поиска ключа> <модель ключа>[=<параметры привязки>]  <опции защиты файлов> [<файл 3>] [<файл 4>]

### <опции защиты>

-RC=N	Количество неудачных обращений к ключу (по умолчанию 50)
-FAST	Использовать все доступные ключи для ускорения защиты
-SILENT	Отключить вывод сообщение в защищенном приложении (отключает опцию -RC)
-MSG=<msg-файл>	Использовать сообщения об ошибках из msg-файла (по умолчанию сообщения об ошибках берутся из ресурсов)
<b>-PP</b>	Вероятность генерирования полиморфных инструкций (по умолчанию 100%)
<b>-PD</b>	Фактор глубины полиморфных инструкций. Допустимые значения от 2 до 100 (по умолчанию 10)
<b>-HP</b>	Фактор уменьшения вероятности вызова функций контроля целостности. Допустимые значения от 1 до 1000 (по умолчанию 10)
<b>-PRC=&lt;prc-файл&gt;</b>	Установить имя входного <b>*.prc файла</b>
- PROTECT_DLL_NAME=<файл>	Установить имя защищённого хранилища данных
<b>-OUT=&lt;путь&gt;</b>	Установить выходную директорию для защищаемых файлов. Если не указывать эту опцию, то, "по умолчанию", будет использоваться текущая директория.  <b>Важно:</b> если использовать директорию с незащищенным приложением как выходную, то оно будет заменено защищенным.
-Q	Запретить вывод сообщений утилитой защиты

-ENVELOPE_MODE=S H:[N]:[L]	режим работы конверта (способ шифрования секций защищаемого модуля) <ul style="list-style-type: none"> <li>• S – программный режим конверта без использования алгоритмов электронного ключа</li> <li>• H – режим работы конверта с использованием аппаратного алгоритма с номером N и длиной вопроса L</li> </ul> <p><b>Важно:</b> привязать одно приложение к разным моделям электронных ключей возможно только в программном режиме работы конверта “-ENVELOPE_MODE=S”.</p>
-SP_ACTIVATE=<grdvd-файл>	Путь к файлу лицензии Guardant SP
-SP_TRIAL_ACTIVATE=<grdvd-файл>:<файл>	Путь к файлам лицензии и серийного номера Guardant SP (рекомендуется для автоматической активации триальных версий программ)
-USE_NET_AS_LOCAL	Использовать сетевые ключи в качестве локальных (при привязке к локальным ключам игнорируется)

Опции для установки пути к конфигурационному файлу клиента для подключения к серверу Guardant Net:

-RCS_USER_DEFINED=<каталог>	Полный или относительный путь к файлу или каталогу
-RCS_PROGRAM_DATA=<каталог>	Путь относительно папки "ProgramData" к файлу или каталогу
-RCS_ENV_VAR=<имя>	Имя переменной окружения, в которой установлен полный или относительный путь к файлу или каталогу (используется только для подключения к серверу Guardant Net)

**<опции поиска ключа>**

-UI[=ID]	Привязка к уникальному ID
-UN[=NPROG]	Привязка к уникальному номеру программы
-US[=SN]	Привязка к уникальному серийному номеру
-UV[=VER]	Проверка версии
-UM=MASK	Проверка маски запусков

Примечание: при привязке к нескольким моделям ключей опция -UI недоступна, опции -UV, -UN, -US, -UV не имеют значений по умолчанию. Опция -USE\_NET\_AS\_LOCAL игнорируется для локальных ключей.

Только для сетевых ключей (при использовании для локальных игнорируются):

-MN=N	Номер модуля в таблице лицензий (по умолчанию -1)
-LOGIN_MODE[=H,S,P]	Выбрать режим лицензирования: <ul style="list-style-type: none"> <li>• H - по хендлам,</li> <li>• P - по процессам,</li> <li>• S - по рабочим станциям (установлено по умолчанию)</li> </ul>

**<модель ключа>**

-GC=N:L:[ID]:[ECC:<файл ключа>]]	Привязать к Guardant Code
-GCN=N:L:[ID]:[ECC:<файл ключа>]]	Привязать к Guardant Code Net
-GSP=[N]:[L]:[ID]:[ECC:<файл ключа>]]	Привязать к Guardant SP

-GSPN=[N]:[L]:[ID]:[ECC:<файл ключа>]]	Привязать к Guardant SP Net
-GS3S=[N]:[L]:[ID]:[ECC:<файл ключа>]]	Привязать к Guardant Sign/Time
-GN3S=[N]:[L]:[ID]:[ECC:<файл ключа>]]	Привязать к Guardant Sign/Time Net
-GS3=[N]:[L]:[ID]]	Привязать к Guardant Stealth III
-GN3=[N]:[L]:[ID]]	Привязать к Guardant Net III
-GS2=[N]:[L]:[ID]]	Привязать к Guardant Stealth II
-GN2=[N]:[L]:[ID]]	Привязать к Guardant Net II

Примечание: для ключей Guardant Stealth/Net II по умолчанию используется номер алгоритма GSII64 N=4 и длина вопроса L=8.  
Для ключей Guardant Stealth/Net III и Guardant Sign/Time/Net по умолчанию используется номер алгоритма GSII64 N=0 и длина вопроса L=8.

#### <параметры привязки>

N	Номер алгоритма ключа (GSII64 или AES)
L	Длина вопроса к алгоритму
ID	ID ключа, на котором будет происходить защита
ECC	Номер алгоритма ECC160
<файл ключа>	Путь к файлу с открытым ключом ECC160

#### <опции защиты файлов>

-ATR=N	Количество таблиц вопросов к алгоритму (по умолчанию 2)
-AES_COUNT=N	Количество ключей шифрования (по умолчанию 5)
<b>-INI=&lt;ini-файл&gt;</b>	Использовать ini-файл. Кодировка ANSI.
<b>-MAP=&lt;map-файл&gt;</b>	Использовать map-файл
-LICENSE_COUNTER=limit	Предупреждать при запуске, если счетчик запусков меньше, чем limit
-LICENSE_TIME [=days]	Предупреждать при запуске, если количество дней использования осталось меньше, чем days. Работает только для ключей семейства Guardant Time. Значение по умолчанию – 14 дней.
-LICENSE_URL=s tring	Отображать URL в сообщении
<b>-SPLASH=&lt;bmp- file&gt;</b>	Устанавливает изображение-заставку, выводимую перед запуском приложения

## Примеры использования

```
grdarmor.exe -ENVELOPE_MODE=H:5:16 -GS3S=0:16 -OUT=./result -PRC=clock.prc -MAP=Clock.map Clock.exe
```

Защищенное приложение Clock.exe будет запускаться в случае, если к компьютеру подсоединен ключ Guardant Sign\Time с симметричными алгоритмами #0 и #5, а длина вопроса 16. Код для защиты указан в файле clock.prc, а исполняемый файл будет помещен в подкаталог result.

```
grdarmor.exe -ENVELOPE_MODE=S -GC=0:16 -GS3S=0:16 -OUT=./result -INI=Clock.ini -MAP=Clock.map Clock.exe
```

Защищенное приложение Clock.exe будет запускаться в случае, если к компьютеру подсоединен ключ Guardant Sign\Time или Code\Code Time с симметричным алгоритмом #0 и длиной вопроса 16. Режим работы конверта программный. Для различных моделей аппаратных ключей можно использовать алгоритмы с разными номерами (числовыми именами).