

GrdProtect

Функция(метод) **GrdProtect** устанавливает аппаратные запреты на чтение и запись, а также количество аппаратных алгоритмов и адрес таблицы лицензий LMS.

C

```
int GRD_API GrdProtect(
    HANDLE hGrd,
    DWORD dwWrProt,
    DWORD dwRdProt,
    DWORD dwNumFunc,
    DWORD dwTableLMS,
    DWORD dwGlobalFlags,
    void *pReserved
);
```

Для ключей Guardant Sign/Time														
hGrd	хэндл, для которого будет выполнена операция													
dwWrProt	SAM-адрес первого байта, доступного для записи (в байтах)													
dwRdProt	SAM-адрес первого байта, доступного для чтения (в байтах)													
dwNumFunc	количество аппаратных алгоритмов и защищенных ячеек (Protected Item), дескрипторы которых записаны в память ключа													
dwTableLMS	Номер защищенной ячейки, в которой хранится таблица лицензий LMS. Для локальных ключей не используется (значение должно быть равно 0)													
dwGlobalFlags	Описание флагов dwGlobalFlags: <table><tr><td>GrdGF_Protect Time</td><td>1</td><td>Блокировка вызова функции GrdSetTime. Автоматически выставляется при программировании ключа из GrdUtil. Если данный флаг был выставлен, то изменить время микросхемы таймера невозможно без перезаписи маски</td></tr><tr><td>GrdGF_HID</td><td>2</td><td>Ключ работает в HID-режиме</td></tr><tr><td>GrdGF_OnlyOn eSessKey</td><td>4</td><td>Единственный сессионный ключ для Guardant API. При установленном флаге будет работоспособна только одна копия приложения, защищенного Guardant API</td></tr><tr><td>GrdGF_2ndSes sKey</td><td>8</td><td>Единственный сессионный ключ для автозащиты. При установленном флаге будет работоспособна только одна копия приложения, накрытого автозащитой</td></tr></table>		GrdGF_Protect Time	1	Блокировка вызова функции GrdSetTime . Автоматически выставляется при программировании ключа из GrdUtil . Если данный флаг был выставлен, то изменить время микросхемы таймера невозможно без перезаписи маски	GrdGF_HID	2	Ключ работает в HID-режиме	GrdGF_OnlyOn eSessKey	4	Единственный сессионный ключ для Guardant API. При установленном флаге будет работоспособна только одна копия приложения, защищенного Guardant API	GrdGF_2ndSes sKey	8	Единственный сессионный ключ для автозащиты. При установленном флаге будет работоспособна только одна копия приложения, накрытого автозащитой
GrdGF_Protect Time	1	Блокировка вызова функции GrdSetTime . Автоматически выставляется при программировании ключа из GrdUtil . Если данный флаг был выставлен, то изменить время микросхемы таймера невозможно без перезаписи маски												
GrdGF_HID	2	Ключ работает в HID-режиме												
GrdGF_OnlyOn eSessKey	4	Единственный сессионный ключ для Guardant API. При установленном флаге будет работоспособна только одна копия приложения, защищенного Guardant API												
GrdGF_2ndSes sKey	8	Единственный сессионный ключ для автозащиты. При установленном флаге будет работоспособна только одна копия приложения, накрытого автозащитой												
pReserved	зарезервировано. Значение должно быть равно NULL													

Для ключей Guardant Stealth III/Net III		
hGrd	хэндл, для которого будет выполнена операция	
dwWrProt	SAM-адрес первого байта, доступного для записи (в байтах)	
dwRdProt	SAM-адрес первого байта, доступного для чтения (в байтах)	
dwNumFunc	количество аппаратных алгоритмов и защищенных ячеек (Protected Item), дескрипторы которых записаны в память ключа	
dwTableLMS	Номер защищенной ячейки, в которой хранится таблица лицензий LMS. Для локальных ключей не используется (значение должно быть равно 0)	
dwGlobalFlags	зарезервировано. Значение должно быть равно 0	
pReserved	зарезервировано. Значение должно быть равно NULL	

Для ключей Guardant Stealth II/Net II и Guardant Stealth /Net		
hGrd	хэндл, через который будет выполнена данная операция	

<i>dwWrProt</i>	SAM-адрес первого байта, доступного для записи (в байтах). Адрес должен быть четным, в противном случае возвращается ошибка GrdE_InvalidArg
<i>dwRdProt</i>	SAM-адрес первого байта, доступного для чтения (в байтах). Адрес должен быть четным, в противном случае возвращается ошибка GrdE_InvalidArg
<i>dwNumFunc</i>	количество аппаратных алгоритмов, дескрипторы которых записаны в память ключа
<i>dwTableLMS</i>	Для Guardant Net II: SAM-адрес в двухбайтовых словах первого байта таблицы лицензий LMS. Если LMS не используется или ключ Guardant Stealth II, значение должно быть равно 0
<i>dwGlobalFlags</i>	зарезервировано. Значение должно быть равно 0
<i>pReserved</i>	зарезервировано. Значение должно быть равно NULL

Для ключей Guardant Fidus		
<i>hGrd</i>	хэндл, для которого будет выполнена операция	
<i>dwWrProt</i>	SAM-адрес первого байта, доступного для записи (в байтах). Адрес должен быть четным, в противном случае возвращается ошибка GrdE_InvalidArg	
<i>dwRdProt</i>	SAM-адрес первого байта, доступного для чтения (в байтах). Адрес должен быть четным, в противном случае возвращается ошибка GrdE_InvalidArg	
<i>dwNumFunc</i>	параметр игнорируется, должен быть равен 0	
<i>dwTableLMS</i>	параметр игнорируется, должен быть равен 0	
<i>dwGlobalFlags</i>	зарезервировано. Значение должно быть равно 0	
<i>pReserved</i>	зарезервировано. Значение должно быть равно NULL	
GrdE_VerifyError	Ошибка верификации после нескольких повторов; запись прекращена	
GrdE_CRCErrorWrite	Ошибка CRC; запись прекращена	

Функция **GrdProtect** позволяет установить аппаратные запреты на чтение/запись заданной области памяти ключа, а также назначить в ключе количество аппаратных алгоритмов и защищенных ячеек (Protected Item). Для сетевых ключей Guardant Net, в случаях когда используется система управления лицензиями, функция также задает адрес (для Net II) или номер защищенной ячейки (для Sign Net / Time Net), где хранится таблица лицензий LMS.

Аппаратные запреты можно устанавливать на непрерывную область памяти ключа, начиная с адреса 44 SAM. Параметр *dwWrProt* задает адрес первого байта, не защищенного от записи. Если значение параметра равно 0, это означает отсутствие запретов на запись. Параметр *dwRdProt* задает адрес первого байта, не защищенного от чтения. Если значение параметра равно 0, это означает отсутствие запретов на чтение.

Параметр *dwNumFunc* задает количество аппаратных алгоритмов в ключе, а также (для Sign / Time) защищенных ячеек, включая таблицу лицензий LMS. Все эти алгоритмы и защищенные ячейки должны быть предварительно созданы, т.е. в память ключа должны быть записаны их дескрипторы.

Параметр *dwTableLMS* задает SAM-адрес первого байта таблицы лицензий LMS (для Guardant Net I/II) или номер защищенной ячейки, в которой хранится таблица лицензий LMS (для Sign Net / Time Net).

Функция **GrdProtect** используется на завершающем этапе реорганизации памяти сетевого ключа «вручную» (без помощи программы GRDUTIL). Сначала функцией [GrdInit](#) память ключа инициализируется, затем в нее заносится таблица размещения алгоритмов, дескрипторы алгоритмов и защищенных ячеек. И, наконец, функцией **GrdProtect** устанавливаются запреты на память, занятую дескрипторами, и назначается количество созданных в ключе алгоритмов и защищенных ячеек.

Программа GRDUTIL позволяет проделать ту же работу быстрее и проще, поэтому не рекомендуется пользоваться функциями [GrdInit](#) и **GrdProtect** без особой необходимости.

C#

```
public static GrdE GrdProtect(Handle grdHandle, uint wrProt, uint rdProt, uint numFunc, uint tableLMS)
public static GrdE GrdProtect(Handle grdHandle, uint wrProt, uint rdProt, uint numFunc, uint tableLMS, uint
globalFlags)
```

grdHandle [in]

Тип: [Handle](#)

Хэндл, через который будет выполнена данная операция

wrProt [in]

Тип: uint

SAM-адрес первого байта, который доступен для записи (в байтах).

rdProt [in]

Тип: uint

SAM-адрес первого байта, который доступен для чтения (в байтах).

numFunc [in]

Тип: uint

Количество аппаратных алгоритмов и защищенных ячеек, дескрипторы которых записаны в память ключа.

tableLMS [in]

Тип: uint

Номер защищенной ячейки, в которой хранится таблица лицензий LMS.

globalFlags [in]

Тип: uint

Флаги.

GrdE.VerifyError	Ошибка верификации после нескольких повторов; запись прекращена
GrdE.CRCErrWrite	Ошибка CRC; запись прекращена

Метод **GrdProtect** позволяет установить аппаратные запреты на чтение/запись заданной области памяти ключа, а также назначить в ключе количество аппаратных алгоритмов и защищенных ячеек (Protected Item). Для сетевых ключей Guardant Net, в случаях когда используется система управления лицензиями, метод также задает адрес (для Net II) или номер защищенной ячейки (для Sign Net / Time Net), где хранится таблица лицензий LMS.

Аппаратные запреты можно устанавливать на непрерывную область памяти ключа, начиная с адреса 44 SAM. Параметр *wrProt* задает адрес первого байта, не защищенного от записи. Если значение параметра равно 0, это означает отсутствие запретов на запись. Параметр *rdProt* задает адрес первого байта, не защищенного от чтения. Если значение параметра равно 0, это означает отсутствие запретов на чтение.

Параметр *numFunc* задает количество аппаратных алгоритмов в ключе, а также (для Sign / Time) защищенных ячеек, включая таблицу лицензий LMS. Все эти алгоритмы и защищенные ячейки должны быть предварительно созданы, т.е. в память ключа должны быть записаны их дескрипторы.

Параметр *tableLMS* задает SAM-адрес первого байта таблицы лицензий LMS (для Guardant Net I/II) или номер защищенной ячейки, в которой хранится таблица лицензий LMS (для Sign Net / Time Net).

Метод **GrdProtect** используется на завершающем этапе реорганизации памяти сетевого ключа «вручную» (без помощи программы GRDUTIL). Сначала методом [GrdInit](#) память ключа инициализируется, затем в нее заносится таблица размещения алгоритмов, дескрипторы алгоритмов и защищенных ячеек. И, наконец, методом **GrdProtect** устанавливаются запреты на память, занятую дескрипторами, и назначается количество созданных в ключе алгоритмов и защищенных ячеек.

Программа GRDUTIL позволяет проделать ту же работу быстрее и проще, поэтому не рекомендуется пользоваться методами [GrdInit](#) и **GrdProtect** без особой необходимости.

Java

```
public static GrdE GrdProtect(Handle grdHandle, int writeProt, int readProt, int numFunc, int tableLMS)
public static GrdE GrdProtect(Handle grdHandle, int writeProt, int readProt, int numFunc, int tableLMS, GrdGF
globalFlags)
```

grdHandle [in]

Тип: [Handle](#)

Хэндл, через который будет выполнена данная операция

writeProt [in]

Тип: int

SAM-адрес первого байта, который доступен для записи (в байтах).

readProt [in]

Тип: int

SAM-адрес первого байта, который доступен для чтения (в байтах).

numFunc [in]

Тип: int

Количество аппаратных алгоритмов и защищенных ячеек, дескрипторы которых записаны в память ключа.

tableLMS [in]

Тип: int

Номер защищенной ячейки, в которой хранится таблица лицензий LMS.

globalFlags [in]

Тип: [GrdGF](#)

Флаги.

GrdE.VerifyError	Ошибка верификации после нескольких повторов; запись прекращена
GrdE.CRCErrorWrite	Ошибка CRC; запись прекращена

Метод **GrdProtect** позволяет установить аппаратные запреты на чтение/запись заданной области памяти ключа, а также назначить в ключе количество аппаратных алгоритмов и защищенных ячеек (Protected Item). Для сетевых ключей Guardant Net, в случаях когда используется система управления лицензиями, метод также задает адрес (для Net II) или номер защищенной ячейки (для Sign Net / Time Net), где хранится таблица лицензий LMS.

Аппаратные запреты можно устанавливать на непрерывную область памяти ключа, начиная с адреса 44 SAM. Параметр *writeProt* задает адрес первого байта, не защищенного от записи. Если значение параметра равно 0, это означает отсутствие запретов на запись. Параметр *readProt* задает адрес первого байта, не защищенного от чтения. Если значение параметра равно 0, это означает отсутствие запретов на чтение.

Параметр *numFunc* задает количество аппаратных алгоритмов в ключе, а также (для Sign / Time) защищенных ячеек, включая таблицу лицензий LMS. Все эти алгоритмы и защищенные ячейки должны быть предварительно созданы, т.е. в память ключа должны быть записаны их дескрипторы.

Параметр *tableLMS* задает SAM-адрес первого байта таблицы лицензий LMS (для Guardant Net I/II) или номер защищенной ячейки, в которой хранится таблица лицензий LMS (для Sign Net / Time Net).

Метод **GrdProtect** используется на завершающем этапе реорганизации памяти сетевого ключа «вручную» (без помощи программы GRDUTIL). Сначала методом [GrdInit](#) память ключа инициализируется, затем в нее заносится таблица размещения алгоритмов, дескрипторы алгоритмов и защищенных ячеек. И, наконец, методом **GrdProtect** устанавливаются запреты на память, занятую дескрипторами, и назначается количество созданных в ключе алгоритмов и защищенных ячеек.

Программа GRDUTIL позволяет проделать ту же работу быстрее и проще, поэтому не рекомендуется пользоваться методами [GrdInit](#) и **GrdProtect** без особой необходимости.