Установка аппаратных запретов

Аппаратные запреты – это программируемая блокировка чтения и записи выбранного участка памяти. Использование аппаратных запретов – эффективная мера защиты содержимого ключа.

Установка аппаратных запретов производится на нижнем уровне, что гарантирует невозможность их обхода обычными программными средствами. Ключ просто не отвечает на попытки чтения или записи защищенной области.

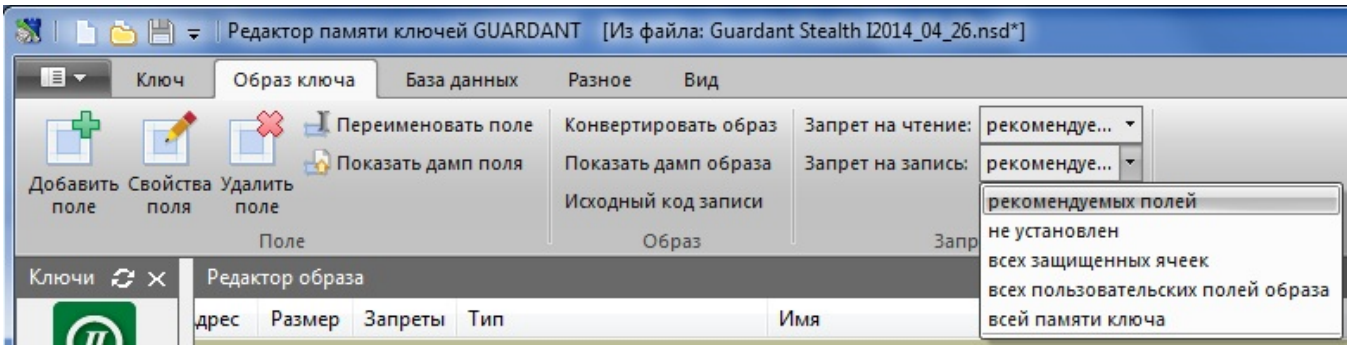
Важно!
С помощью специальных операций Guardant API можно получить доступ к части содержимого защищенных ячеек – особой разновидности полей памяти, защищенных запретами.

Запреты можно устанавливать на непрерывную область памяти свободного назначения, начиная с младших адресов (т. е. с адреса 14 UAM до области полей специальных операций).

GrdUtil.exe автоматически устанавливает аппаратные запреты на чтение и запись на следующие типы полей: аппаратные алгоритмы, защищенные ячейки памяти, таблица лицензий.

Важно!
Категорически не рекомендуется оставлять незащищенной аппаратными запретами на чтение и запись область памяти, занятую аппаратными алгоритмами, таблицей лицензий и защищенными ячейками памяти!

Чтобы установить аппаратные запреты, выполните команду меню **Образ ключа | (Запреты) Запрет на чтение** либо **Образ ключа | (Запреты) Запрет на запись** . Выберите из разворачивающегося списка запретов нужное значение:



Диалог позволяет выбрать следующие варианты установки запретов:

Запрет на чтение / запись	**Пояснение**
Не установлен	Запреты снимаются со всей памяти
Всех защищенных ячеек	Защищаются только ячейки и алгоритмы
Всех пользовательских полей образа	Защищаются все поля, созданные пользователем
Всей памяти ключа	Вся доступная память защищается запретами

Запреты можно выставлять как отдельно (только на чтение, только на запись), так и комбинировать их (и на чтение, и на запись).

Виды и обозначения аппаратных запретов в ***Редакторе образа***:

Аппаратный запрет	**Описание**
r	Поле целиком защищено от чтения
r-	Часть поля защищена от чтения
w	Поле целиком защищено от записи

w-	Часть поля защищена от записи
rw	Поле целиком защищено от чтения и записи
r-w-	Часть поля защищена от чтения и записи

Согласно идеологии ключей Guardant установка новых аппаратных запретов ведет к инициализации памяти ключа, т. е. все пользовательские данные удаляются из памяти.

Т. о., после установки новых значений запретов в ***Редакторе образа*** и записи образа в ключ, память ключа полностью обновляется. При этом выполняется целая цепочка операций Guardant API:

- Память ключа очищается (операция GrdInit)
- Информация из образа пишется в ключ (операция GrdWrite)
- На указанную область памяти устанавливаются аппаратные запреты (операция GrdProtect)