# Ограничение времени работы приложения

Электронные ключи **Guardant Time/ Net Time / Code Time** оснащены часами реального времени и позволяют ограничивать астрономическое время работы защищенного приложения.

Смысл технологии ограничения времени заключается в том, что работоспособность алгоритма зависит от таймера **(RTC),** встроенного в ключ.

С помощью ключей с часами реального времени можно реализовывать различные лицензионные политики, влияющие на время работы защищенного приложения:

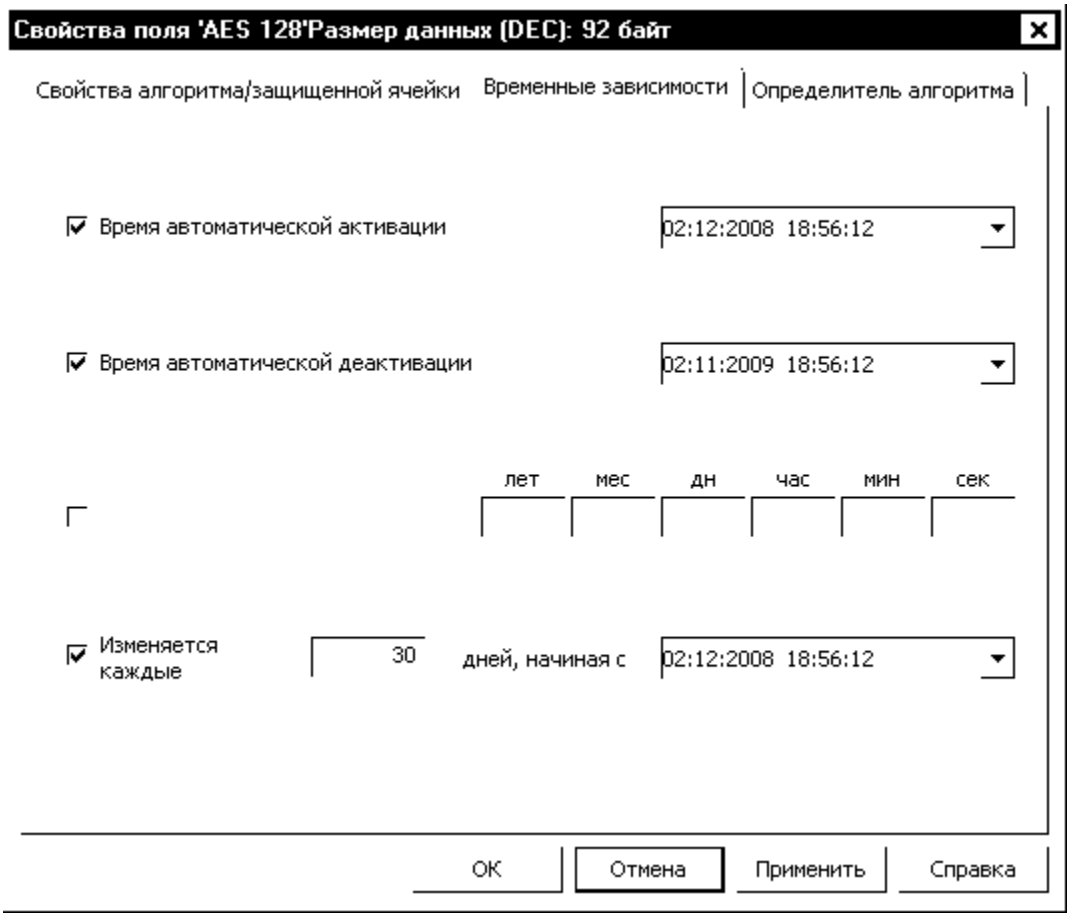
- Приложение сможет работать только после активации алгоритма, которая произойдет по наступлению указанной даты
- Приложение перестанет работать после деактивации алгоритма, которая произойдет по наступлению указанной даты
- Срок работы приложения ограничен заданным периодом работоспособности, т. н. «временем жизни», алгоритма. Алгоритм активируется при первом запуске приложения и деактивируется по истечению «времени жизни»

## Установка временной зависимости алгоритма

1

Выберите в маске для ключа с **RTC** аппаратный алгоритм, который будет использоваться для защиты, и выполните команду меню **«Образ ключа | (Поле) Свойства поля»**.

При автозащите установка временной зависимости имеет смысл только для алгоритма типа **GSII64** и **AES128,** и именно того, который будет использоваться для защиты




В появившемся диалоге **Свойства поля** перейдите на вкладку **Временные зависимости**

2
3

С помощью флагов установите нужные временные зависимости (подробное описание см. *в таблице ниже*).
Запишите образ в ключ.

### Элементы управления диалога «Временные зависимости»:

| Элемент интерфейса | Назначение |
|---|---|
| Флаг **Время автоматической активации** | Если флаг установлен, то алгоритм (а, следовательно, и защищенное приложение) станет работоспособным только после наступления указанной даты активации |
| Комбинированное поле ввода/ календарь для установки даты активации | Установка календарной даты активации аппаратного алгоритма.<br><br>*Дату можно установить как непосредственно в поле ввода, так и используя календарь* |
| Флаг **Время автоматической деактивации** | Если флаг установлен, то аппаратный алгоритм (а, следовательно, и защищенное приложение) перестанет быть работоспособным сразу после наступления указанной даты деактивации |
| Комбинированное поле ввода/ календарь для установки даты деактивации | Установка календарной даты деактивации аппаратного алгоритма |
| Флаг **Время жизни алгоритма** | Если флаг установлен, то время работы аппаратного алгоритма (а, следовательно, и защищенного приложения) будет ограничено указанным календарным периодом времени.<br><br>Отсчет времени работы начинается после первого обращения к алгоритму (после первого старта приложения)<br><br>При автозащите этот флаг нужно включать только после ее выполнения. Т.е. перед автозащитой маска прошивается в ключ без использования данного флага, а после того как приложение было защищено нужно включить флаг и снова прошить ключ. |
| Поля ввода периода работоспособности алгоритма | Указание временного периода работоспособности алгоритма в формате **лет:мес:дн:час:мин:сек** |
| Флаг **Алгоритм изменяется каждые…** | Если флаг установлен, то определитель алгоритма будет постоянно изменяться через определенный временной промежуток, начиная с указанной даты (см. **FlipTime**) |
| Поле ввода, указывающее через сколько дней изменится алгоритм | Установка периодичности изменения определителя алгоритма для механизма **FlipTime** (в днях) |
| Комбинированное поле ввода/ календарь для установки даты первого изменения алгоритма | Установка календарной даты активации механизма **FlipTime** |

## FlipTime. Изменение ответов алгоритма через указанный период времени

В ключах с RTC реализована технология FlipTime, позволяющая автоматически изменять значения, возвращаемые алгоритмом ключа по наступлению заданного временного значения.

Технология FlipTime неприменима к ячейкам типа **«Загружаемый код»** в ключах Guardant Code Time!

**FlipTime** – это механизм, модифицирующий часть определителя алгоритма по достижению указанной при программировании ключа даты. Причем это изменение не однократное, определитель будет продолжать изменяться через заданный промежуток времени (в днях). Соответственно, всякий раз после изменения определителя, алгоритм будет возвращать другие значения в ответ на запросы.

Чтобы использовать механизм **FlipTime**, разработчик должен знать, какие ответы вернет алгоритм в каждом случае. Для решения этой задачи в комплект разработчика включена консольная утилита **FlipTime.exe**, генерирующая массивы вопросов-ответов алгоритму для каждого факта изменения определителя.

Чтобы активировать механизм **FlipTime**:

1. Выделите в маске ключа с RTC нужный алгоритм, выполните команду меню **Образ ключа | (Поле) Свойства поля** и перейдите на вкладку **Временные зависимости**.
2. Установите флаг **Алгоритм изменяется каждые…** и в появившемся поле задайте период (в днях) изменения алгоритма.
3. С помощью комбинированного поля/календаря определите дату, по достижении которой механизм **FlipTime** будет задействован.
4. Сохраните маску и запишите ее в ключ (команда меню **Ключ | (Операции с ключом) Записать образ в ключ**).
5. Запустите утилиту **FlipTime.exe** и, следуя ее указаниям, получите массивы вопросов-ответов алгоритма после каждого факта изменения определителя.
6. Используйте полученные массивы в приложении согласно заданным временным зависимостям.

1. Технология FlipTime предназначена для использования только при защите с помощью Guardant API. **Недопустимо ее использование при автозащите!**
2. Пользоваться FlipTime следует с известной осмотрительностью, т. к. если в расчетах при проектировании защиты, программировании ключа или защите приложения будет допущена ошибка, то ее достаточно сложно будет диагностировать и исправлять в «боевых» условиях, когда ключ находится у конечного пользователя.

Технология **FlipTime** дает разработчику возможность реализовать изощренную стратегию защиты, при которой защитные механизмы будут видоизменяться через заданное время без дополнительного перепрограммирования ключа.

## Установка запрета на изменение времени

В ключах **Guardant Time/ Time Net/ Code Time** можно задавать новое значение для встроенного таймера при помощи специальной функции Guardant API (см. описание **GrdSetTime**).

Однако если такая необходимость и возникает, то, как правило, на этапе программирования ключа (например, при реализации утилиты прошивки ключа, альтернативной **GrdUtil.exe**).

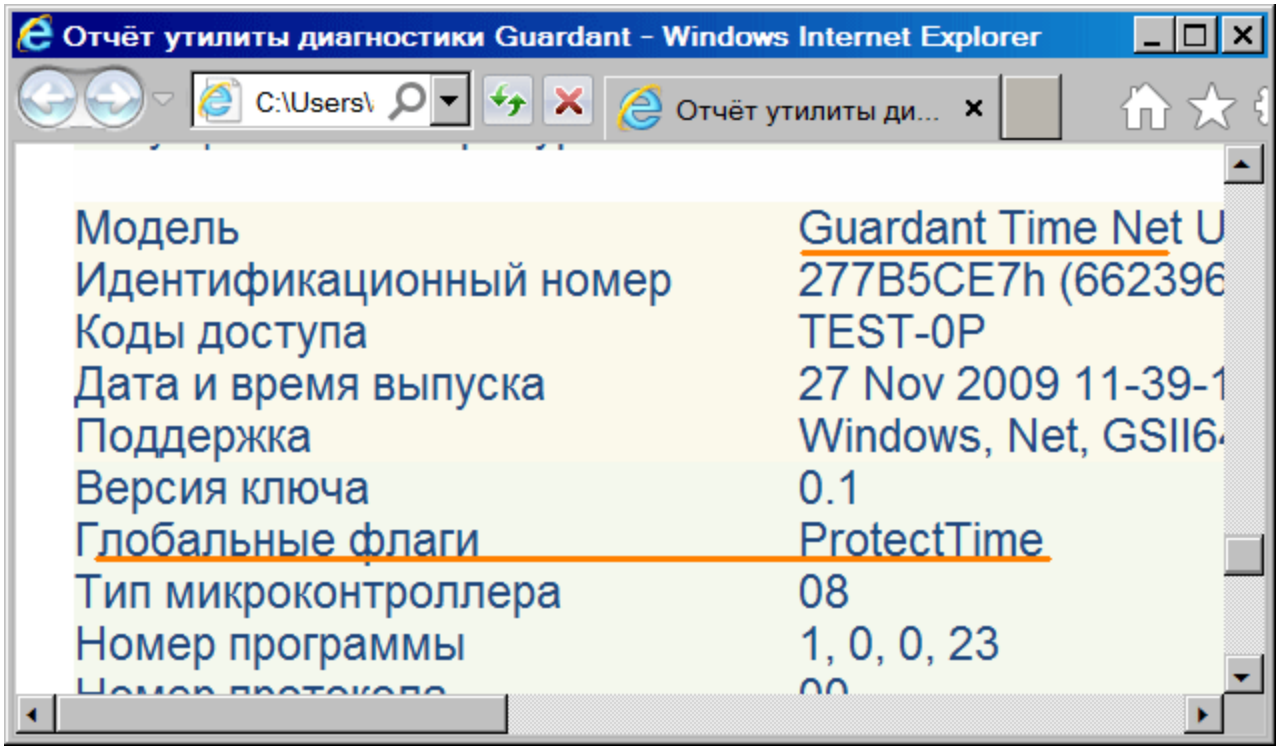
И, наоборот, для защиты приложения это несет угрозу, потому что при некоторых обстоятельствах (к примеру, компрометации кодов доступа), станет возможным перепрограммирование таймера ключа и незаконное продление лицензии.

Поэтому в ключах с таймером предусмотрена возможность блокировать на низком уровне вызов функции **GrdSetTime**.

**Важно!**
В RTC-ключах, поступающих с производства компании «Актив», а также в образах, создаваемых для RTC-моделей, блокировка времени уже выставлена по умолчанию (см. состояние флага **Запретить изменение времени в ключе** в **Панели инструментов/ленточном интерфейсе GrdUtil.exe**).

**Категорически не рекомендуется менять умолчательное значение без особой необходимости.**

Чтобы проверить, блокирована ли возможность изменения времени в ключе, выполните его диагностику (см. предыдущий пункт или описание утилиты диагностики). Глобальный флаг **ProtectTime** должен быть установлен:




В случае отсутствия блокировки изменения времени в ключе загрузите в ***Редактор*** нужный образ RTC-ключа, проверьте состояние флага **Запретить изменение времени**, и если он не установлен, выполните команду меню **Ключ | (Режимы) Запретить изменение времени в ключе**. После этого запишите образ в ключ.

В результате в ключе будет выставлен глобальный флаг **GrdGF_Pro-tectTime** (см. описание GrdProtect), и изменение состояния таймера станет невозможным без инициализации памяти ключа.