Использование таймера для управления статусом аппаратных алгоритмов

Наличие в моделях Guardant Time/Net Time/ Code Time таймера реального времени (Real Time Clock, RTC) дает возможность управлять активацией и деактивацией аппаратных алгоритмов в этих ключах, а также периодическим изменением определителя алгоритма в зависимости от времени.

Эти возможности используются для управления сроками лицензий на защищаемые приложения, а также для автоматической перестройки защитных механизмов с течением времени.

Деактивация по таймеру

При решении задач по ограничению срока действия лицензии могут возникнуть следующие потребности:

- завершить действие лицензии в заданное время (дата окончания действия лицензии)
- завершить действие лицензии через определенное время, начиная с первого использования (срок действия лицензии)

Эффективным методом ограничения срока лицензии является ограничение времени работы одного или нескольких аппаратных алгоритмов, используемых в системе защиты. В период действия лицензии аппаратный алгоритм должен корректно преобразовывать данные, а по окончании этого срока алгоритм блокируется (переводится в неактивное состояние) и перестает обрабатывать данные. Т. о., выполнение защищенного приложения также блокируется.

Для ограничения срока лицензии конкретным временем в дескрипторе аппаратного алгоритма должно быть установлено значение поля **rs_DeadTime** и флаг **nsafh_DeadTime** в поле флагов **rs_HiFlags**. При наступлении времени **rs_DeadTime** алгоритм будет переведен в деактивированное состояние. Изначально алгоритм должен находиться в активном состоянии.

Для ограничения срока лицензии заданным периодом в дескрипторе аппаратного алгоритма должно быть установлено значение поля **rs_LifeTime** и флаг **nsafh_LifeTime** в поле флагов **rs_HiFlags**. По истечении времени **rs_LifeTime** алгоритм будет переведен в деактивированное состояние. Условием использования данного ограничения является отсутствие установленных флагов **nsafh_DeadTime** и **nsafh_BirthTime** в поле флагов **rs_HiFlags**, то есть должна быть запрещена активация и деактивация алгоритма иными методами.

Активация в заданное время

Для активации алгоритма в заданное время в его дескрипторе должно быть установлено значение поля **rs_BirthTime** и флаг **nsafh_BirthTime** в поле флагов **rs_HiFlags**. При наступлении времени **rs_BirthTime** алгоритм будет автоматически переведен в активное состояние. При этом сам алгоритм изначально должен находиться в неактивном состоянии.

С этого момента аппаратный алгоритм сможет преобразовывать данные, и, соответственно, может быть задействован в защитном механизме. Сама схема такого механизма может выглядеть как «передача эстафеты» от автоматически деактивированного алгоритма к активированному. Эти алгоритмы могут обрабатывать данные по-разному, а потому изменится и сам алгоритм защиты, что увеличивает стойкость.

Кроме того, автоматическая активация позволяет при необходимости задавать момент начала действия лицензии.

Автоматическое изменение определителя алгоритма

Другим способом динамически изменять защитные механизмы является возможность модифицировать определитель алгоритма по таймеру. При этом алгоритм постоянно остается активным, и «передачи эстафеты», как и в случае, рассмотренном выше, не происходит.

Для использования данного свойства алгоритма необходимо задать периодичность смены определителя **rs_DaysGap** и время **rs_ChangeFlipTime Start**, начиная с которого будет производиться периодическая смена.

Можно комбинировать автоматическое изменение определителя с режимами ограничения времени жизни при помощи флагов **nsafh_DeadTime**, **nsafh_BirthTime** и **nsafh_LifeTime**.

Этот сервис доступен только для симметричных алгоритмов шифрования (AES128 и GSI164).