

# Использование аппаратных алгоритмов

Guardant API – основной инструмент для работы с аппаратными алгоритмами из приложения. В зависимости от задачи, стоящей перед разработчиком, выбирается тот или иной тип алгоритма и соответствующая функция GrdAPI.

## Симметричное преобразование: функция GrdCryptEx

С помощью функции **GrdCryptEx** происходит вызов симметричных алгоритмов типа GSII64 или AES.

Преобразование при помощи этой функции имеет следующие свойства:

- Взаимообратность
- Стойкость к криптоанализу
- Выполнение преобразования электронным ключом

Такое преобразование используется для кодирования и декодирования данных, используемых приложением, внутри ключа. Объем преобразуемых данных должен быть относительно невелик.

## Однонаправленное преобразование: операция GrdHashEx

Преобразование при помощи операции **GrdHashEx** обычно производится при анализе легальности копии приложения. Главное предназначение этого метода – усложнить логику работы ключа и тем самым предотвратить его эмуляцию. Это преобразование можно использовать для контроля целостности и подлинности данных.

Преобразование имеет два важных свойства:

- Однонаправленность, т. е. для функции  $F(X)$  не существует функция  $F^{-1}()$  такая, что  $X = F^{-1}(F(X))$ .
- Стойкость к криптоанализу
- Выполнение преобразования электронным ключом

Исходя из этих свойств, можно очертить круг задач, которые можно решать при помощи такого преобразования. Его можно использовать в случае:

- Если объем преобразуемой информации невелик (десятки и сотни байт)
- Для кодирования данных, которые не потребуются затем декодировать в исходный вид. Например, в простейшем случае приложение может преобразовать некую произвольную последовательность данных, подсчитать хэш ответной последовательности и сравнить его с эталонным хэшем, полученным на этапе установки защиты. Если значения совпали, то копия защищенного приложения считается легальной.
- В комплексе с программно реализованными симметричными алгоритмами. Например, для получения ключа алгоритма AES.

Кодировать же данные, используемые приложением, этим методом не следует, т. к. преобразование однонаправленное.

## Выполнение загружаемого кода: функция GrdCodeRun(только для Guardant Code/Code Time)

Вызовы загружаемого кода осуществляются при помощи функции GrdCodeRun(). Если загружаемый код разработан в соответствии с рекомендациями и удовлетворяет требованиям, перечисленным в начале следующей главы, он реализует алгоритм, результаты работы которого можно использовать в приложении напрямую.

Таким образом, отсутствие электронного ключа лишает приложение части важной функциональности, без которой его работа перестает быть возможной.