Шифрование данных симметричным алгоритмом

В электронных ключах Guardant реализованы симметричные аппаратные алгоритмы **GSII64** и **AES128.** Они выполняют аппаратное преобразование данных. Подробную информацию о симметричных алгоритмах см. *во 2-й части Руководства пользователя.*

Предварительно закодированные данные могут храниться в защищенном приложении или отдельных файлах и декодироваться непосредственно перед использованием.

Для вызова алгоритма из приложения используется операция *GrdTransform*. Подробную информацию об операциях Guardant API см. в разделе Guardant API.

GrdUtil.exe предоставляет удобный сервис для предварительной подготовки данных преобразования. С помощью утилиты можно закодировать и декодировать информацию. Подготовленные данные в дальнейшем используются при защите приложения.

Подготовка данных для преобразования

Выполнение преобразования

Процесс декодирования выполняется аналогично процессу кодирования (см. выше). В качестве данных на входе используется файл с кодированными данными. Направление преобразования меняется на декодирование (список **Команда**).

Важно!

Для корректного декодирования данных необходимо пользоваться тем же алгоритмом, вектором инициализации и методом преобразования, которые использовались для кодирования.