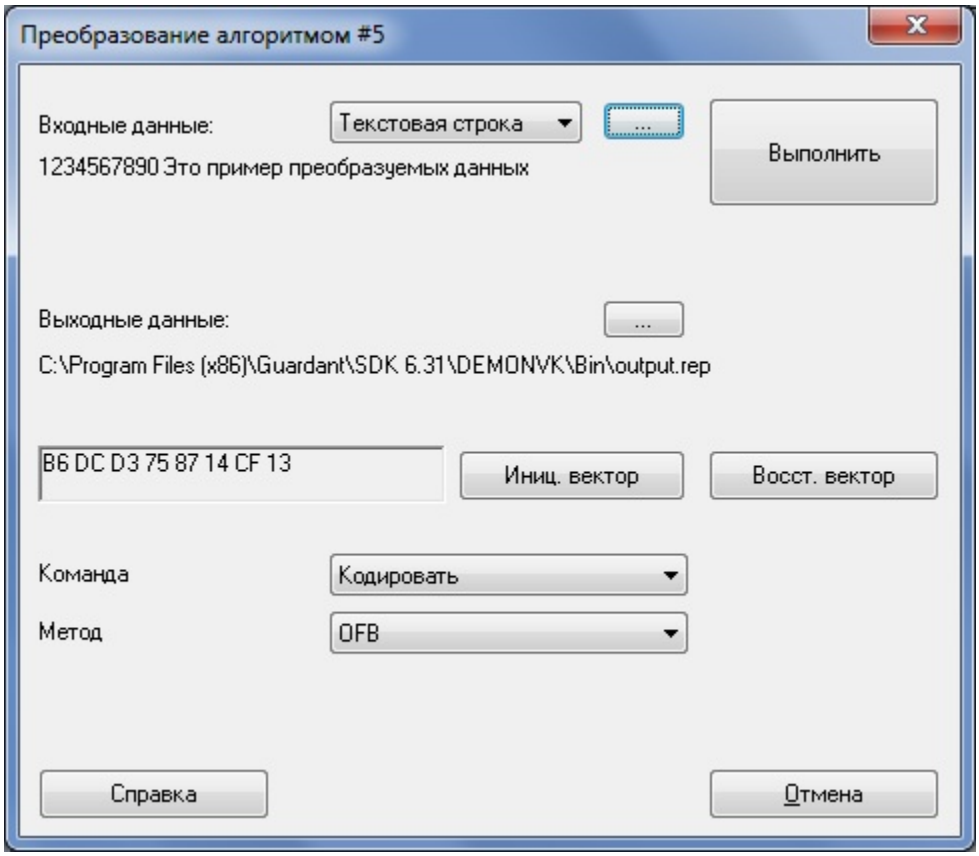
Подготовка данных для преобразования

Выделите в списке полей ***Редактора образа*** алгоритм типа **AES** или **GSII64** и выполните команду **Разное | (Алгоритмы) Шифрование данных алгоритмом**. На экране появится диалоговое окно **Преобразование алгоритмом №N**, где N – числовое имя (порядковый номер алгоритма).



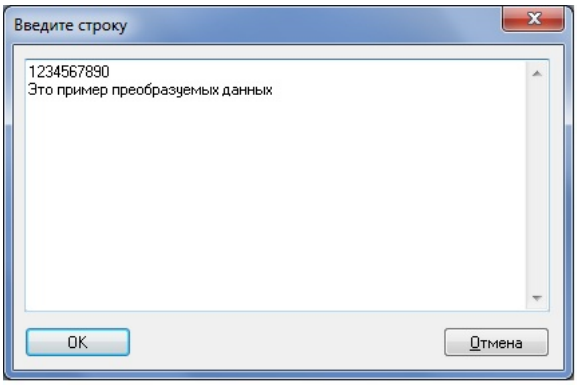
В диалоге определите следующие параметры:

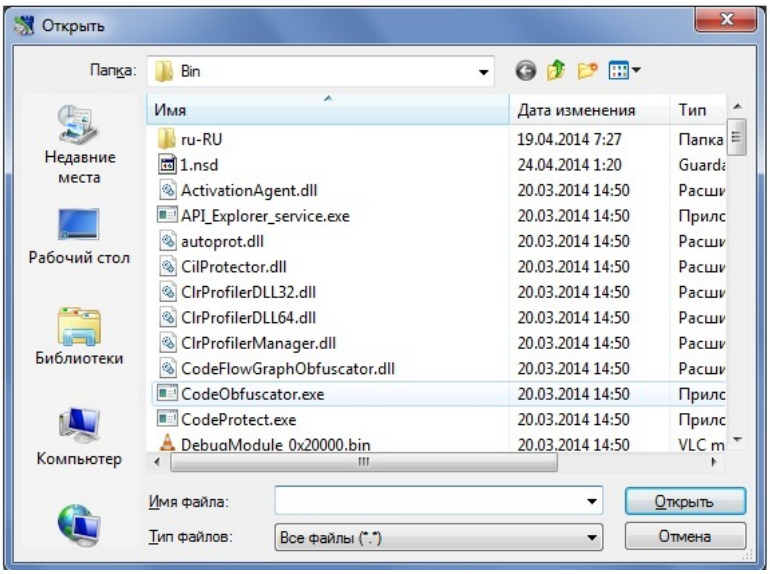
- Входные данные и их вид
- Выходные данные и их вид
- Вектор инициализации и восстановление вектора
- Направление и метод кодирования
- Язык программирования (если выходные данные представлены в виде исходного текста)

Данные, которые необходимо преобразовать, могут быть представлены в виде: строки символов или файла любого формата.

Для выбора вида данных на входе служит раскрывающийся список в верхней части диалога.

По нажатию кнопки **[…]**, расположенной напротив списка, открывается, либо диалог **Введите строку** для ввода строки символов, либо стандартный системный диалог для указания имени файла данных и пути к нему:



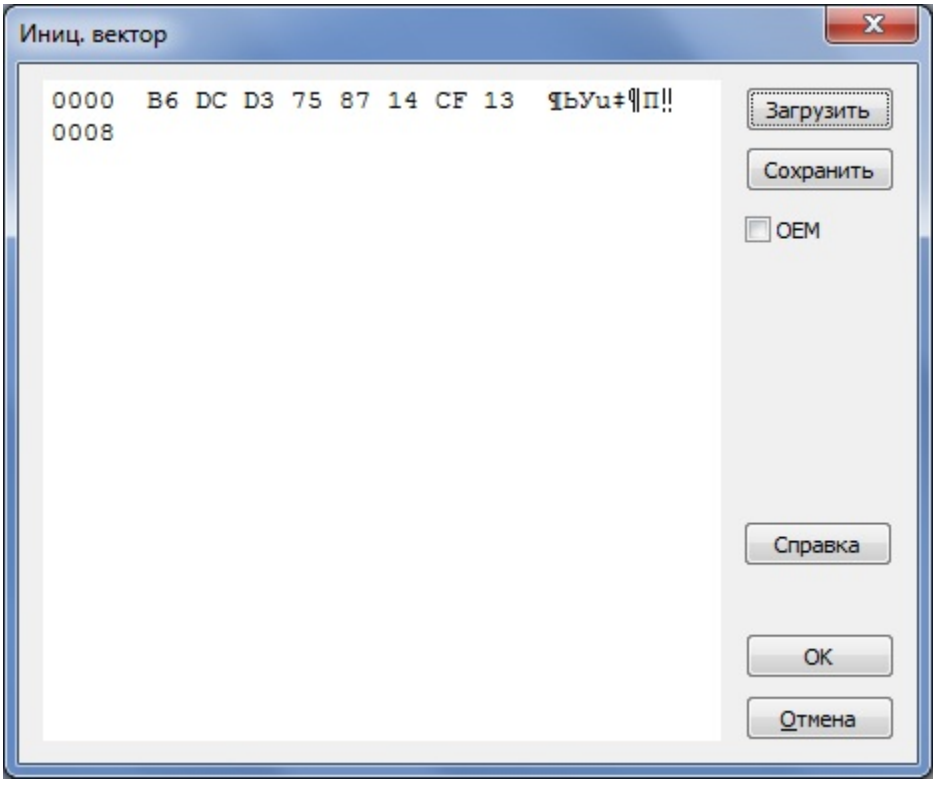


Заданная строка или имя файла с данными и путь к нему отображаются в поле ввода **Входные данные**.
Вектор инициализации – случайное число, которое используется для работы симметричного алгоритма в режимах работы **CFB, CBC** и **OFB.** Вектор инициализации для **GSII64** равен 8 байтов, для **AES128** – 16 байтов.

Вектор инициализации генерируется автоматически при открытии диалога **Преобразование алгоритмом №N** и отображается в соответствующем поле ввода.

При необходимости вектор инициализации по умолчанию можно изменить. По нажатию на кнопку **[Иниц. вектор]** на экране появляется шестнадцатеричный редактор, в окне которого можно скорректировать значение или ввести новый вектор.

Диалог **Вектор инициализации**:



Элементы управления диалога **Вектор инициализации**:

Элемент интерфейса	Назначение

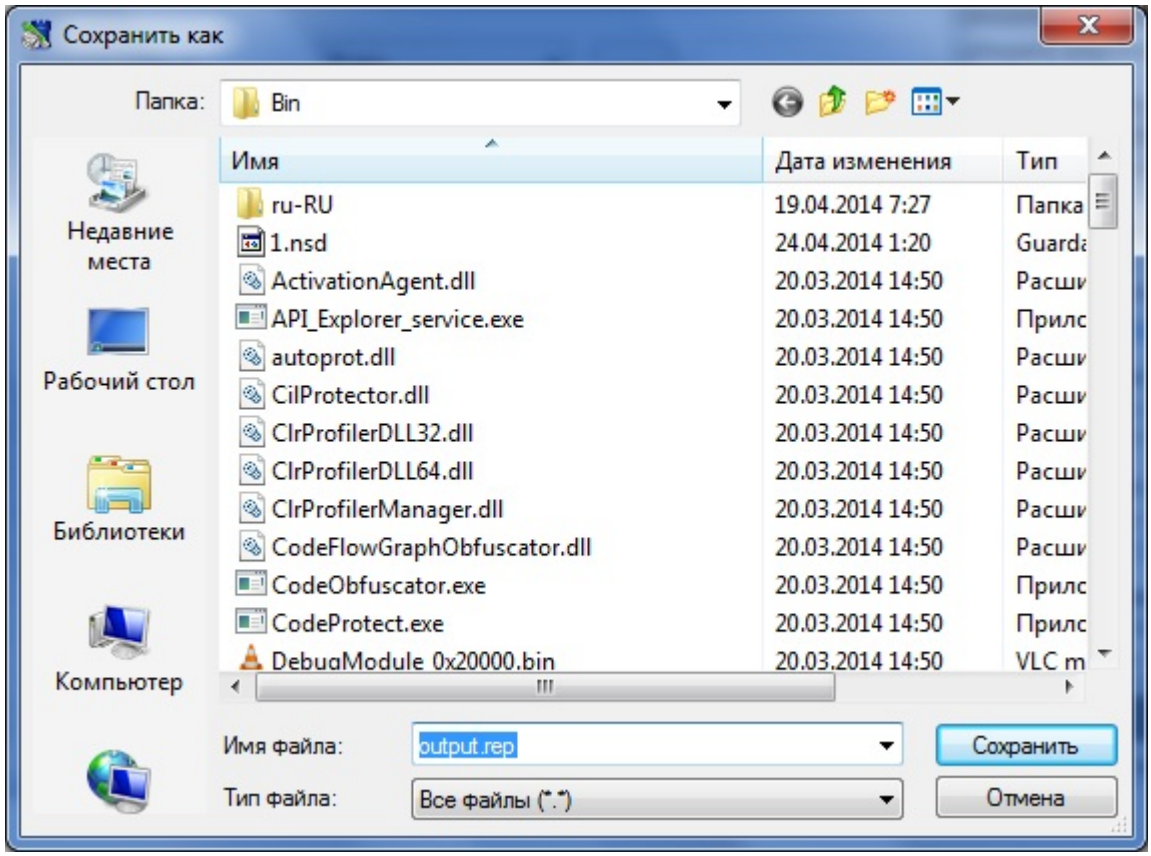
Окно шестнадцатеричного редактора	Ввести значение вектора инициализации
Кнопка **[Загрузить]**	Загрузить дамп из файла с расширением *.dmp
Кнопка **[Сохранить]**	Сохранить дамп в файле с расширением *.dmp
Флаг **OEM**	Выбрать Windows- / DOS-кодировку. По умолчанию используется Windows-кодировка (ANSI) – опция OEM отключена

При выполнении преобразования значение вектора изменяется. Кнопка **[Восст.вектор]** служит для восстановления исходного вектора инициализации.
Преобразованные данные могут иметь следующий вид:

Данные на выходе	**Описание**
Исходный текст	Текстовый файл, содержащий закодированные данные в виде массива чисел и созданный по правилам синтаксиса одного из основных языков программирования: Assembler, C/C++, Pascal/Delphi
Двоичный файл	Закодированная последовательность байтов

Для выбора представления данных на выходе служит раскрывающийся список в средней части диалога.

По нажатию кнопки **[...]**, расположенной напротив списка, открывается стандартный системный диалог для указания имени файлас преобразованными данными (по умолчанию - *Output.rep*) и пути к нему:



Имя файла с данными и путь к нему отображаются в поле ввода **Выходные данные**.
По нажатию на кнопку **[Выполнить]** начинается процесс кодирования (декодирования) данных. Кнопка становится доступной после заполнения секций **Входные данные** и **Выходные данные**.
Развертывающийся список **Язык программирования** расположен в нижней части диалога и становится доступным в том случае, если выбрано представление закодированных данных в виде исходного текста.

В списке представлены следующие языки программирования: Assembler, C/C++, Pascal/Delphi.
Разворачивающийся список **Команда** служит для выбора операции, которая будет совершена над входными данными: кодирование или декодирование.
Алгоритмы типа **GSII64** и **AES128** имеют 4 режима работы, которые отличаются по своим характеристикам и назначению. Подробнее см. *в разделе Симметричное шифрование*.

Для выбора метода преобразования предназначен одноименный разворачивающийся список.