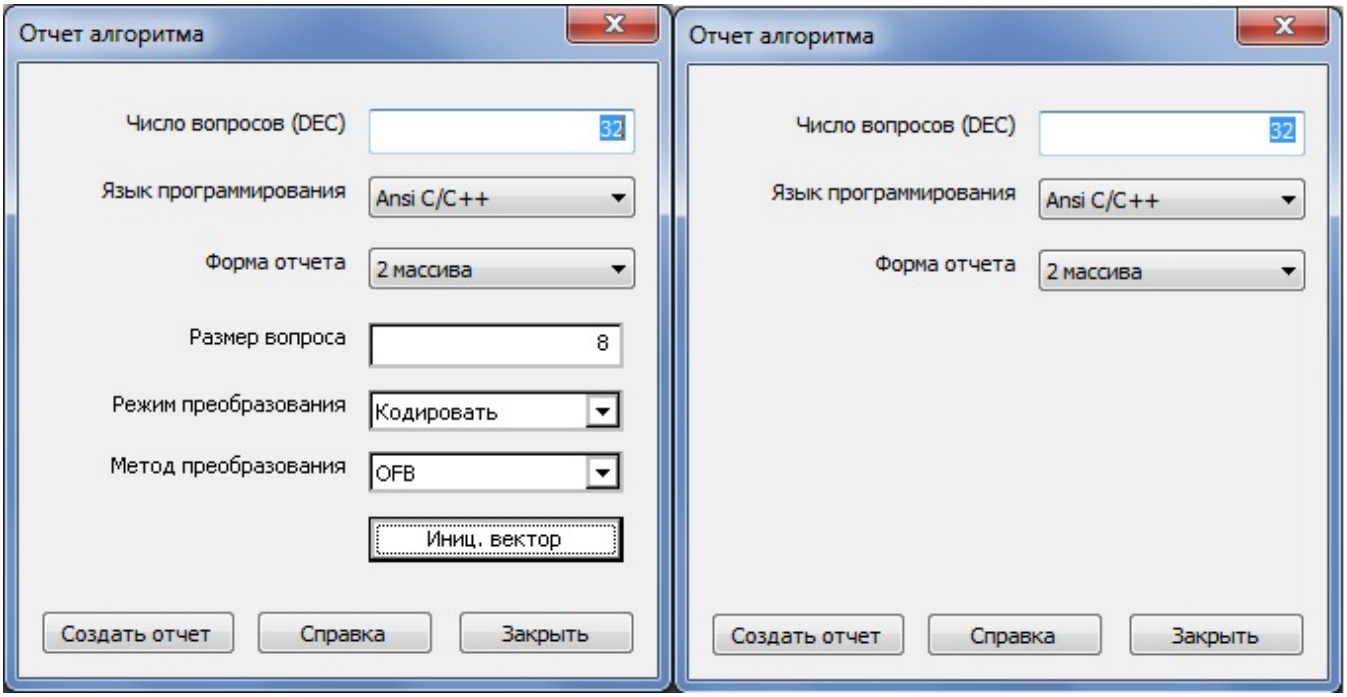
Получение ответов симметричных алгоритмов

Чтобы использовать симметричные алгоритмы шифрования, необходимо знать, какую последовательность вернет алгоритм в ответ на заданный вопрос. Затем эту последовательность (ответ алгоритма) можно использовать для усложнения логики работы защиты.

GrdUtil.exe предоставляет удобный сервис для получения ответов симметричных алгоритмов. Утилита обращается к выбранному алгоритму, получает его ответы и сохраняет результаты в специальном файле отчета.

Важно!
Если алгоритм, для которого выполняется отчет, еще не был записан в память ключа, или свойства и/или определитель алгоритма были изменены в ходе редактирования образа, то перед генерацией отчета выполните команду меню **Ключ | (Операции с ключом) Запись образ в ключ**

Чтобы получить массив ответов, выделите алгоритм в списке и выполните команду меню **Разное | (Алгоритмы) Создать отчет алгоритма**:



В появившемся диалоге укажите число вопросов к алгоритму, нужный язык программирования и форму отчетов. Дополнительно для алгоритмов типа **GSII64** укажите размер вопроса, а также метод и режим преобразования.
Вопросы к алгоритму представляют собой последовательности случайных чисел.

В поле **Число вопросов** укажите число обращений в выбранной системе счисления к алгоритму функции *GrdTransform*.

На каждое обращение (вопрос) алгоритм генерирует ответную последовательность, длина которой равна длине вопроса.
С помощью раскрывающегося списка **Язык программирования** выберите язык, по правилам синтаксиса которого будет создан файл отчета.

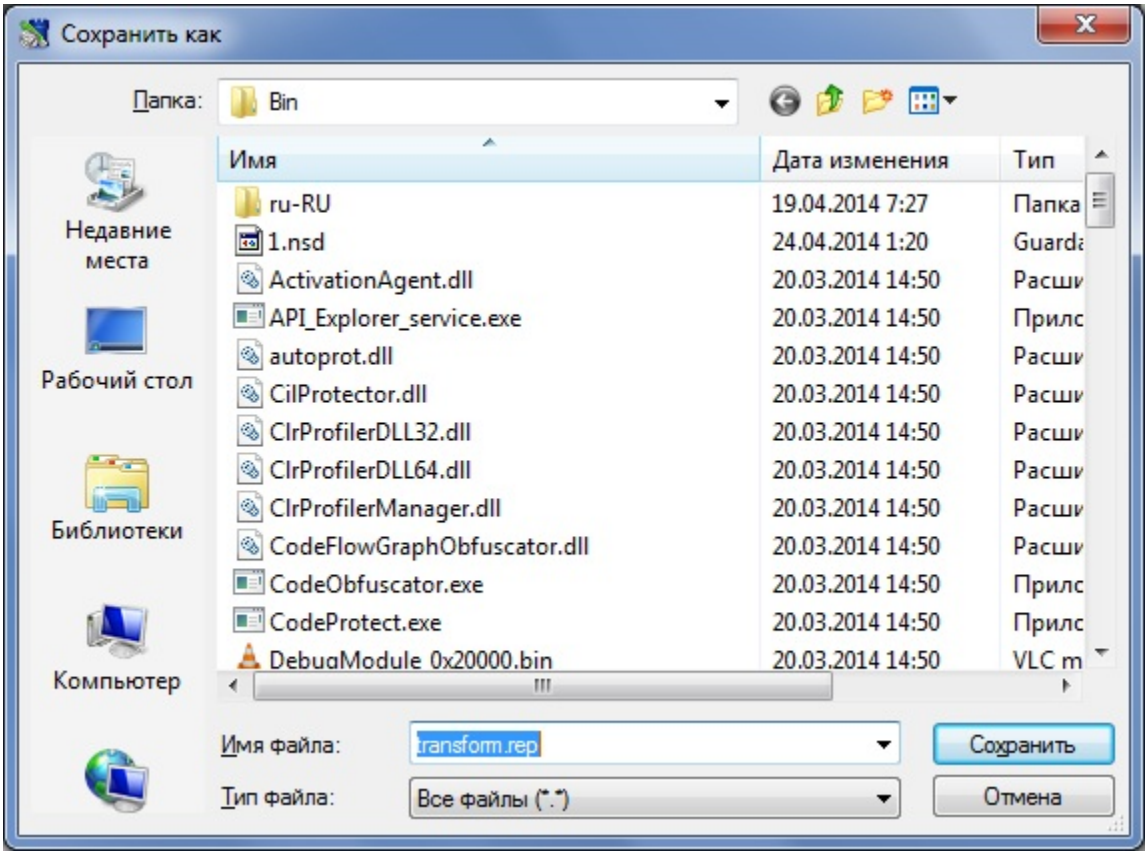
Возможные варианты выбора: C/C++, Pascal/Delphi, Ассемблер.
Вопросы и полученные ответы алгоритма сохраняются в файле отчета в виде одного или двух массивов. Выберите форму отчета с помощью одноименного раскрывающегося списка.

Форма отчета	**Описание**
1 массив	Вопрос и ответ алгоритма представляют чередующиеся элементы массива. Количество элементов массива равно удвоенному числу вопросов

2 массива	Вопросы алгоритма составляют первый массив элементов, соответствующие им ответы – второй. Количество элементов каждого массива равно числу вопросов

Дополнительные параметры для алгоритмов GSII64

После нажатия кнопки **[Создать отчет]** появляется стандартный системный диалог сохранения файла (имя файла по умолчанию ***Transform.rep***):



После этого начинается создание отчета. Используя операцию GrdTransform, **GrdUtil.exe** обращается к выбранному алгоритмув ключе, получает ответы этого алгоритма и сохраняет их в файле отчета.

Процесс генерации отчета иллюстрирует индикатор выполнения.
Массивы, записанные в файле отчета, используются в защищаемом приложении.

Массив вопросов хранится в теле приложения и применяется для последующих обращений к ключу (настоятельно рекомендуется хранить его в закодированном виде).

Массив ответов не следует хранить в приложении, в противном случае уровень защищенности не может быть приемлемым. При помощи этого массива лучше закодировать какие-либо важные данные, используемые приложением (можно, к примеру, использовать быстрое взаимообратное преобразование, паролем которого будет массив ответов).