

Зашифрование случайных таблиц

Оглавление

Зашифрование случайных таблиц	1
НАЗНАЧЕНИЕ	1
Пакеты случайных чисел	2
Файл-хранилище сертификатов получателей.....	3
Формирование зашифрованных таблиц.....	4
НТЦ "Система"	10

НАЗНАЧЕНИЕ

Пакет прикладных программ "Зашифрование случайных таблиц" предназначен для защиты таблиц случайных десятичных чисел, используемых при кодировании финансовых документов по алгоритму TELEX. Зашифрованные с помощью данного пакета таблицы могут быть расшифрованы только с помощью секретного ключа участника финансовых расчетов, которому они предназначены.

Для работы с пакетом на компьютере предварительно должен быть установлен пакет "Криптоядро для BANCS EXP".

Пакеты случайных чисел

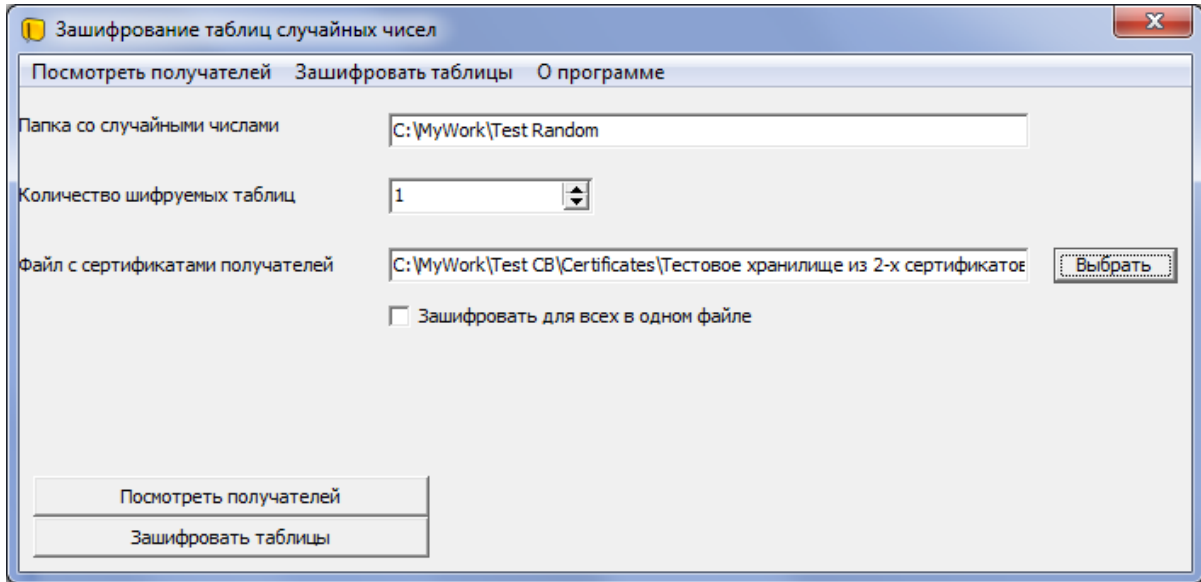
Для работы с программой шифрования таблиц предварительно должны быть выработаны пакеты для таблиц случайных чисел. Такая выработка осуществляется с помощью подсистемы "Генератор случайных десятичных чисел" автоматизированной системы BANCS EXP. Пакеты располагаются в виде файлов в специальной папке. Более подробная информация о пакетах случайных десятичных чисел содержится в документации к пакету "Генератор случайных десятичных чисел".

Файл-хранилище сертификатов получателей

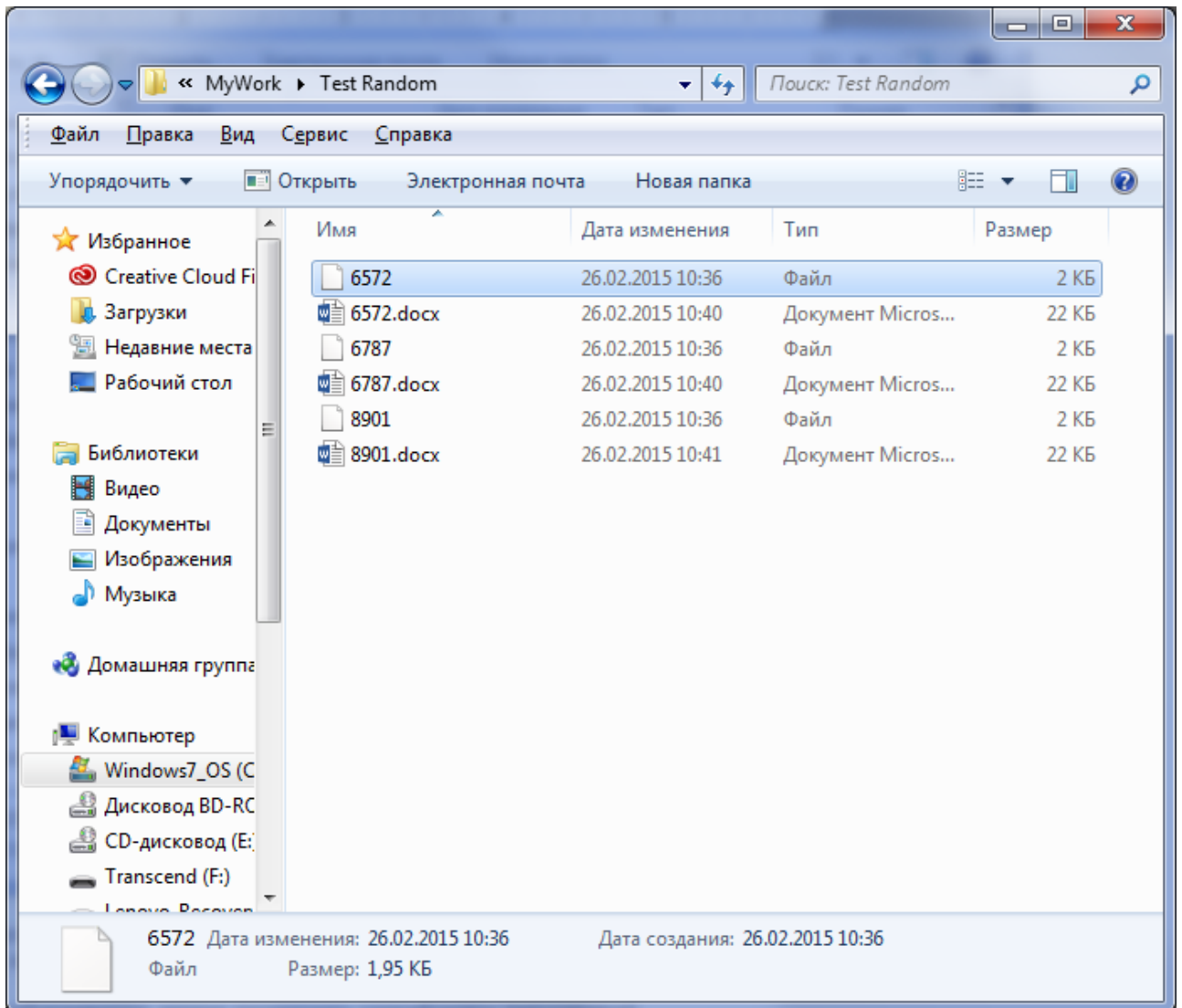
Для создания зашифрованных пакетов необходим файл-хранилище сертификатов получателей. Это стандартный файл с расширением *.p7b, содержащий один или несколько сертификатов участников финансовых расчетов. Более подробная информация о способах создания такого файла содержится в документации к подсистеме "Участник BANCS EXP".

Формирование зашифрованных таблиц

В основном окне программы

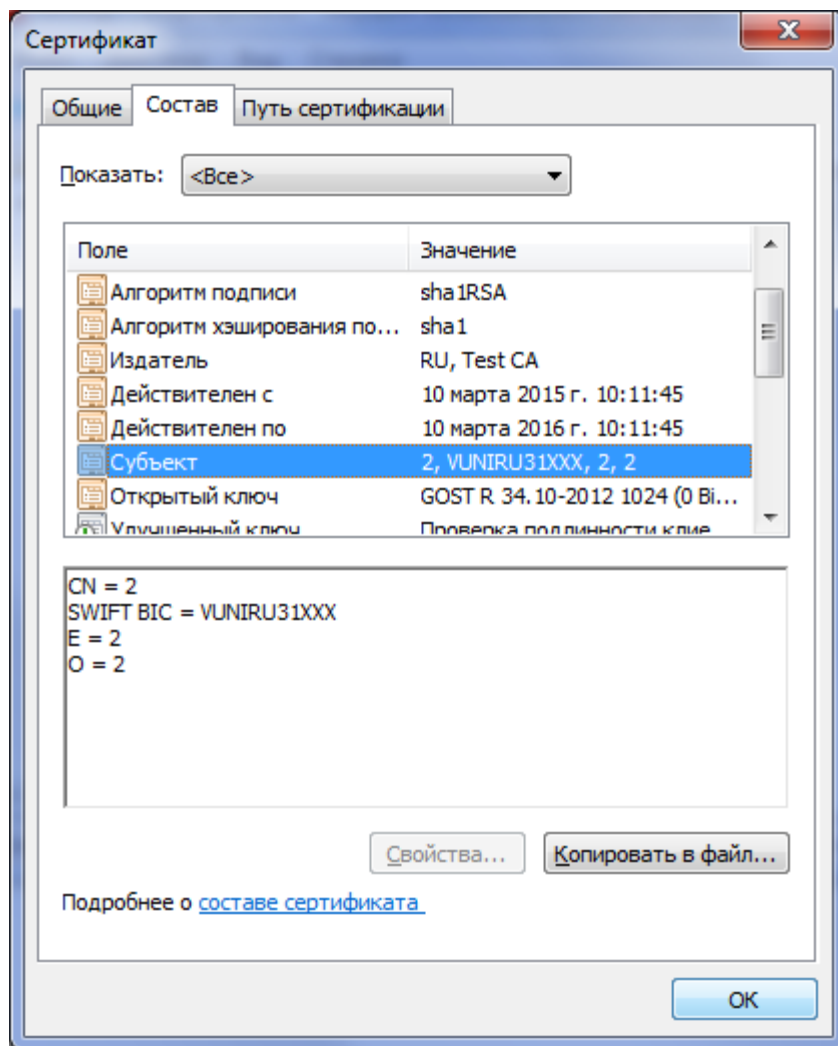
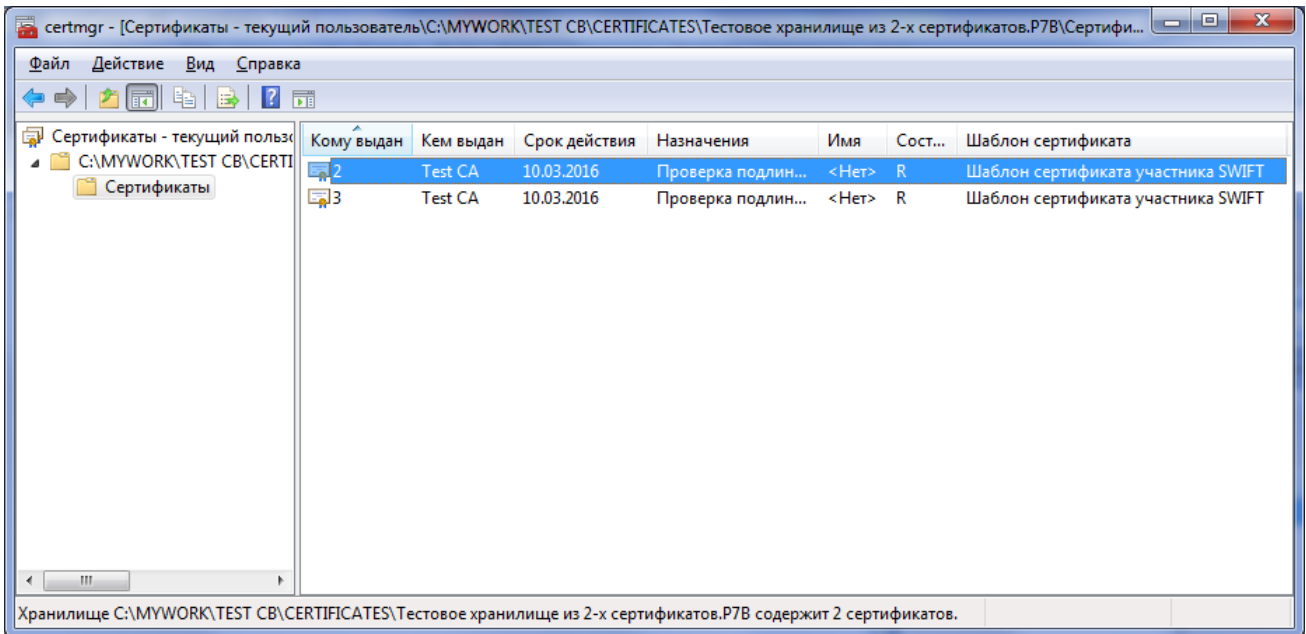


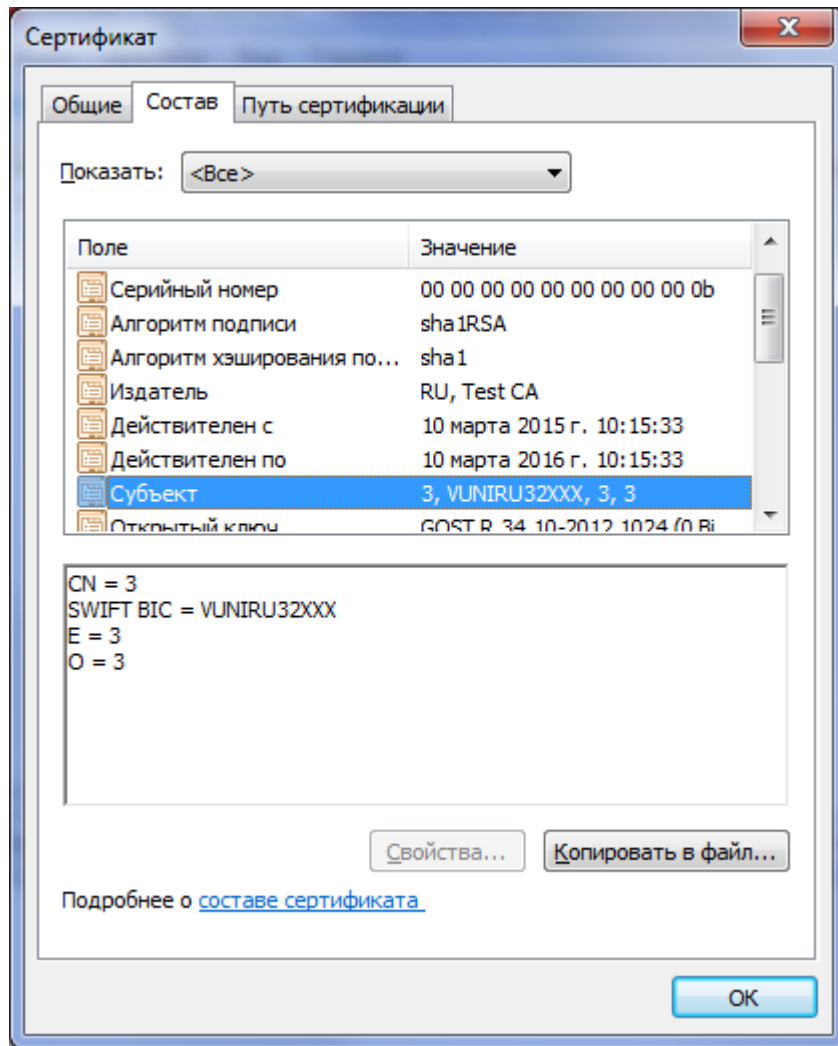
необходимо выбрать папку с пакетами случайных чисел, число шифруемых таблиц и файл-хранилище сертификатов получателей.



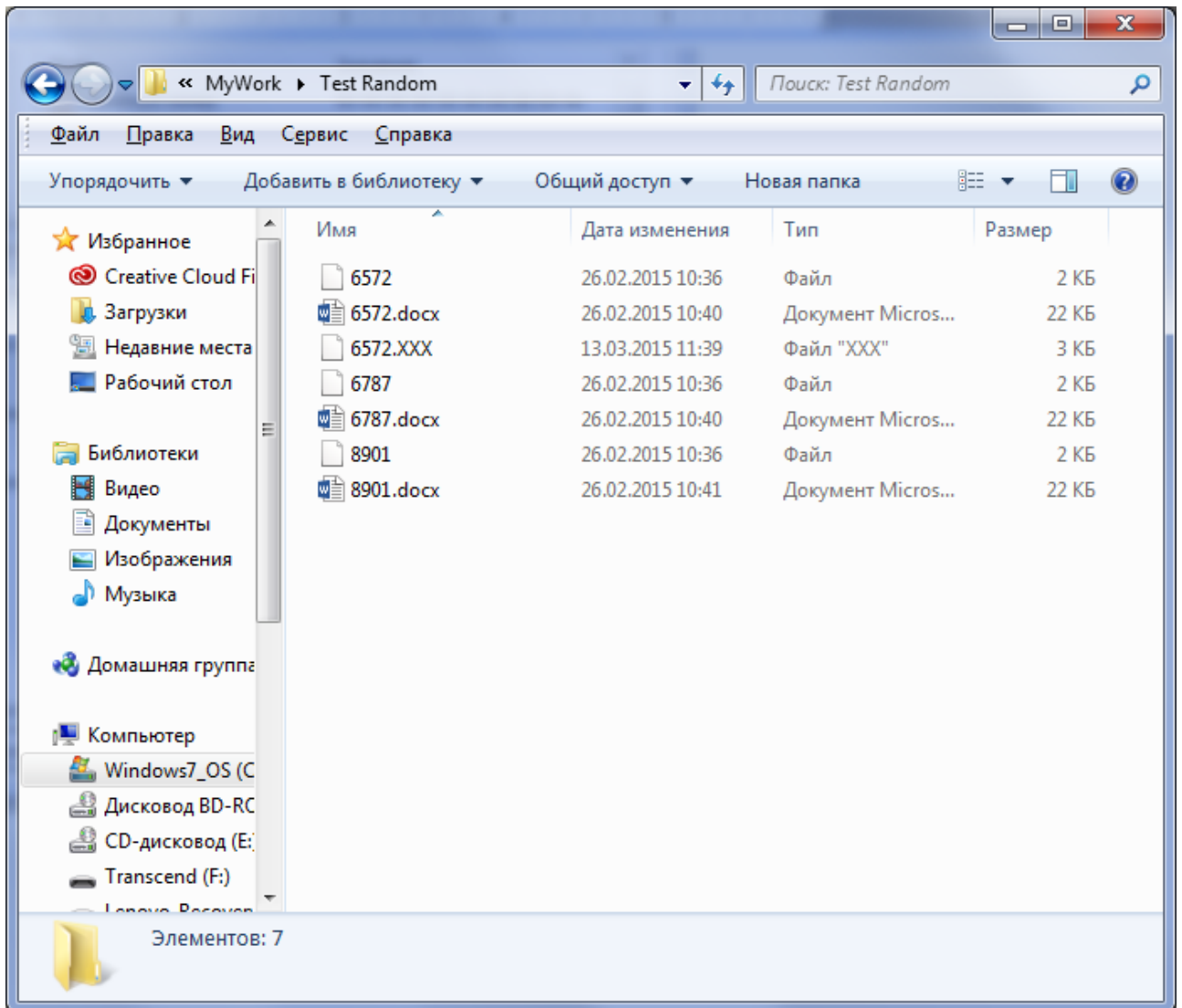
В папке с пакетами случайных таблиц должны быть пакеты, незашифрованные для данного получателя, т.е. те, у которых отсутствует расширение, совпадающее с ВИС получателя.

При необходимости, можно посмотреть сертификаты получателей.

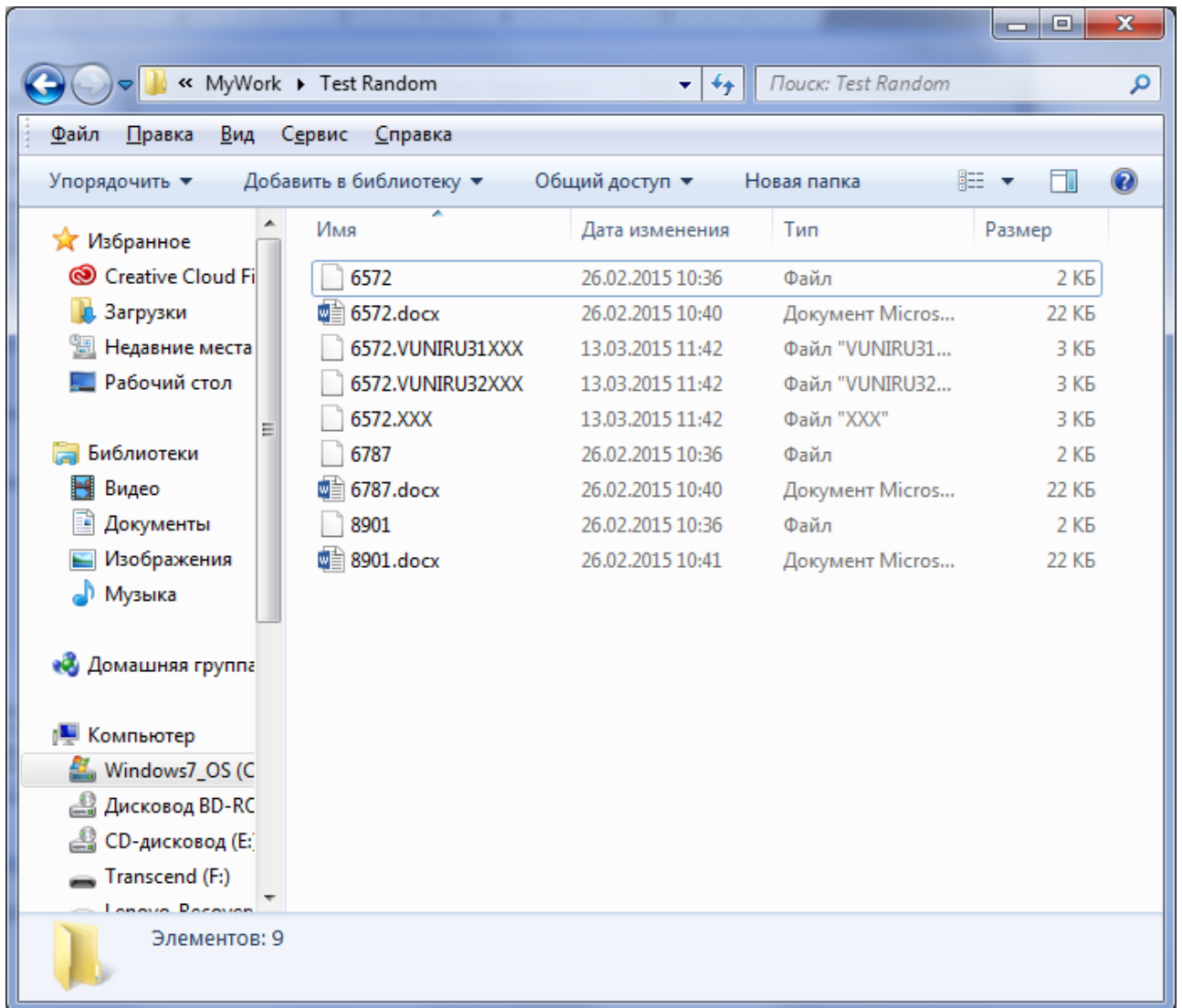




Зашифровать таблицы можно как для всех получателей одновременно, при этом зашифрованный файл будет с расширением *.XXX,



так и для каждого получателя в отдельности, при этом появятся два зашифрованных файла с расширениями, соответствующими VIC.



НТЦ "Система"

Разработчик пакета программ для шифрования таблиц со случайными числами -
Научно-технический центр "Система".

Центральный офис:

НТЦ «Система», ул. Мясницкая, дом 48, строение 1

Москва, 107078

Российская Федерация

Тел.: +7 (495) 628-6084

Факс: +7 (495) 628-5828

Адрес электронной почты: crypto@systema.ru

Веб-сайт: <http://crypto.systema.ru>

© НТЦ «Система», 2015