

Разработка программных модулей для стеганографии и анализа распределения данных в электронных документах

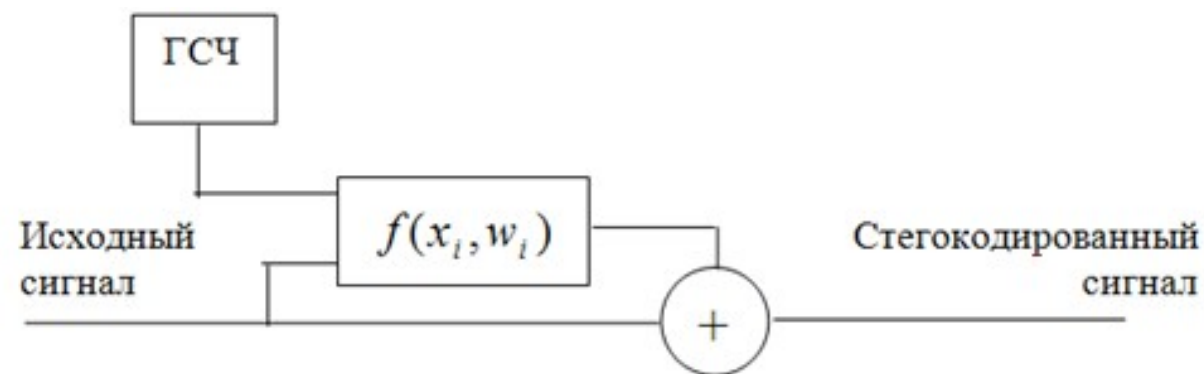
Студент: Тарасов Владислав Валентинович, ИСз-128

Научный руководитель: Коденцев Евгений Иванович

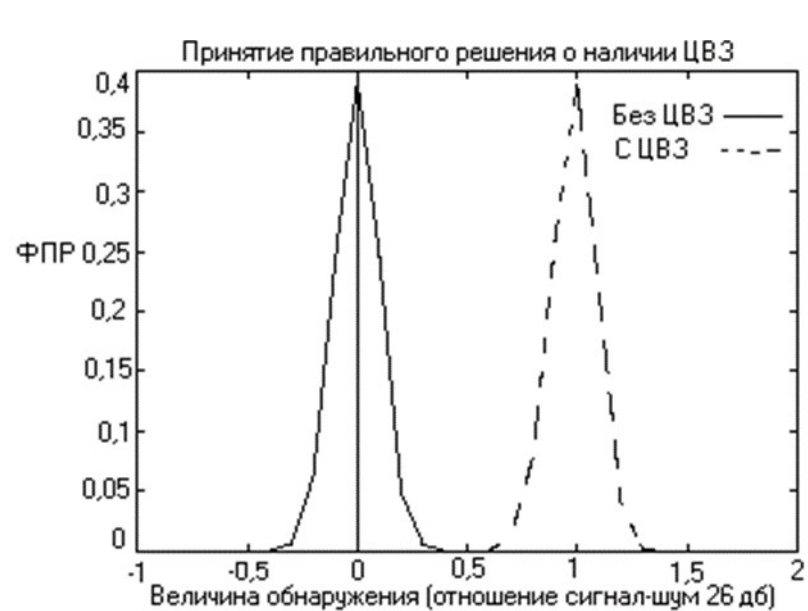
Цель дипломной работы заключается в разработке программного средства реализующий алгоритмы криптографии и стеганографии, и разработки подсистемы анализа распределения данных в электронных документах, при защите информации.

Для достижения поставленной цели необходимо решить следующие **задачи**:

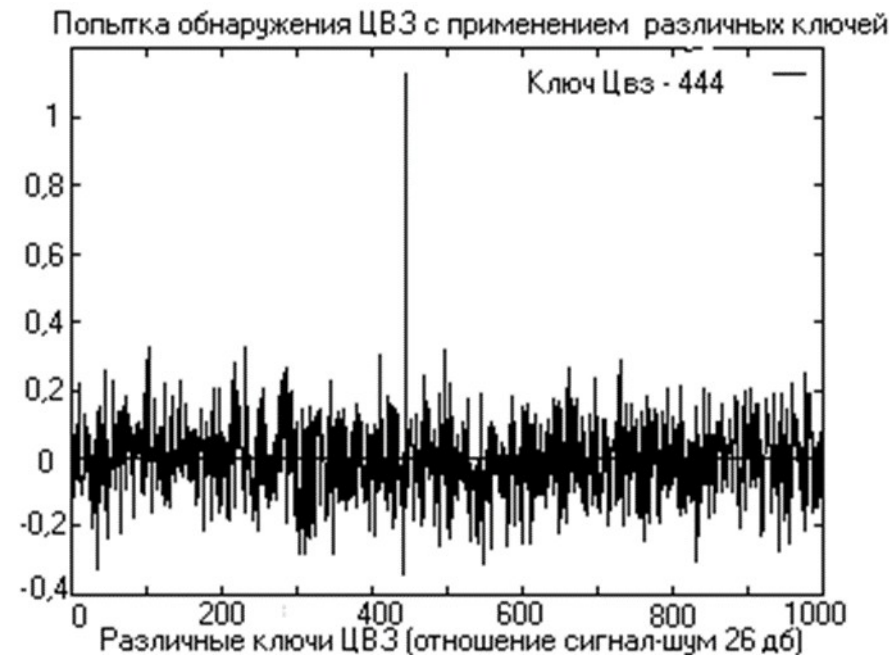
1. Выбор алгоритма стеганографии для скрытия информации в звуковых сигналах.
2. Построение обобщенного алгоритма анализа распределение данных в электронных документах.
3. Разработка программного средства реализующих выбранный алгоритм стеганографии и криптографии.
4. Определение границ применимости исследуемого алгоритма.



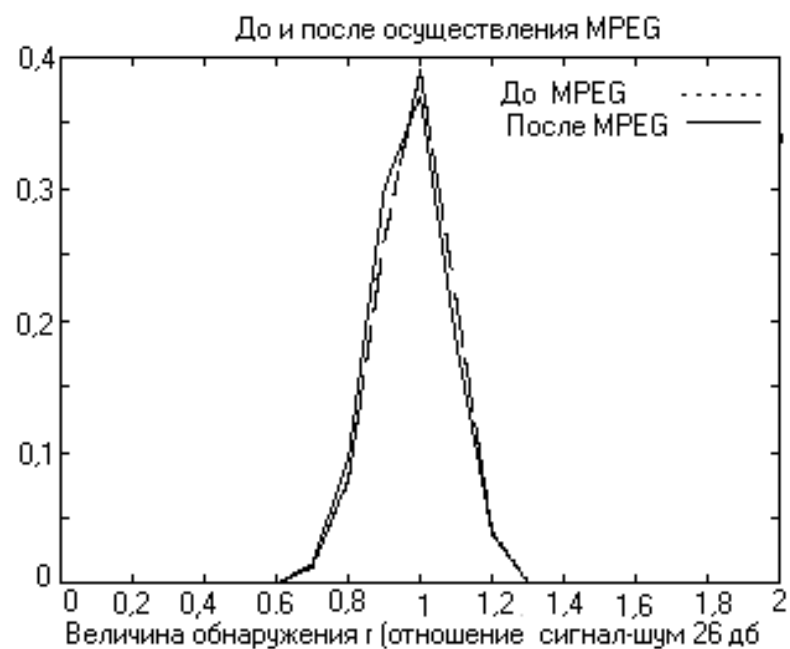
Блок-схема стегокодера и стегодекодера



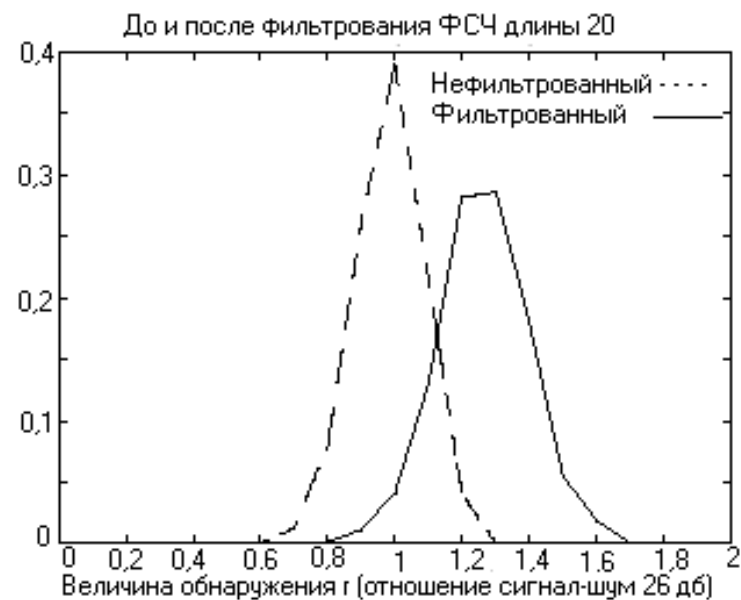
Функция плотности
распределения величины
обнаружения для
сигналов с ЦВЗ и без ЦВЗ



Распознавание заданного
ключа встраивания ЦВЗ



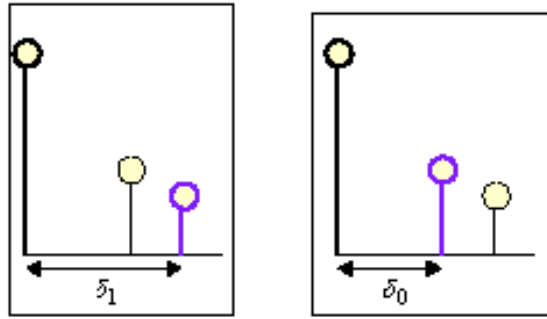
Влияние сжатия
данных на ЦВЗ



Влияние на ЦВЗ применения к
аудио-сигналу скользящего
фильтра средних частот



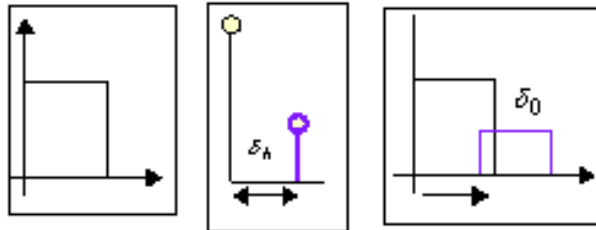
Влияние переквантования
сигнала на ЦВЗ



а) Единица

б) Ноль

Кодирование одного бита информации

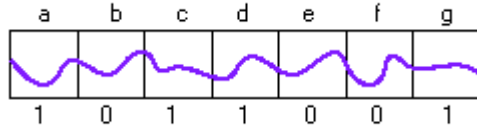


Исходный сигнал

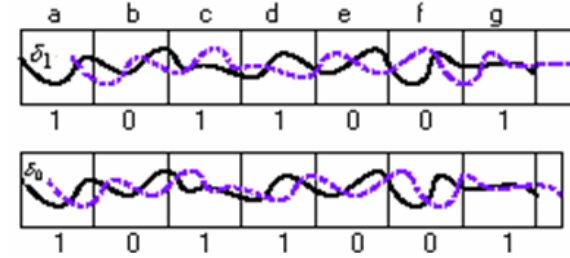
$h(t)$

Выход

Внедрение одного бита информации

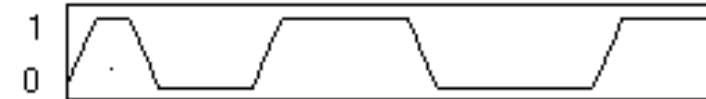
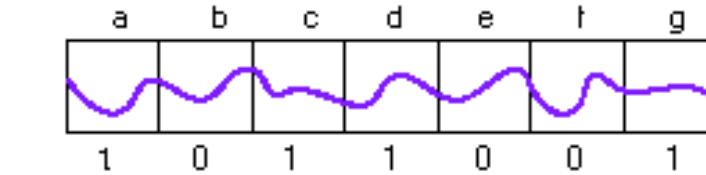


Разделение сигнала на участки

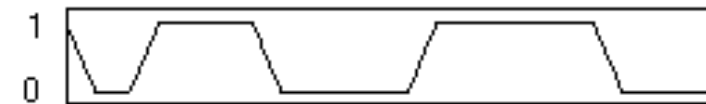


Пунктирной линией показаны эхо-сигналы

Сигналы, содержащие только одно бинарное значение

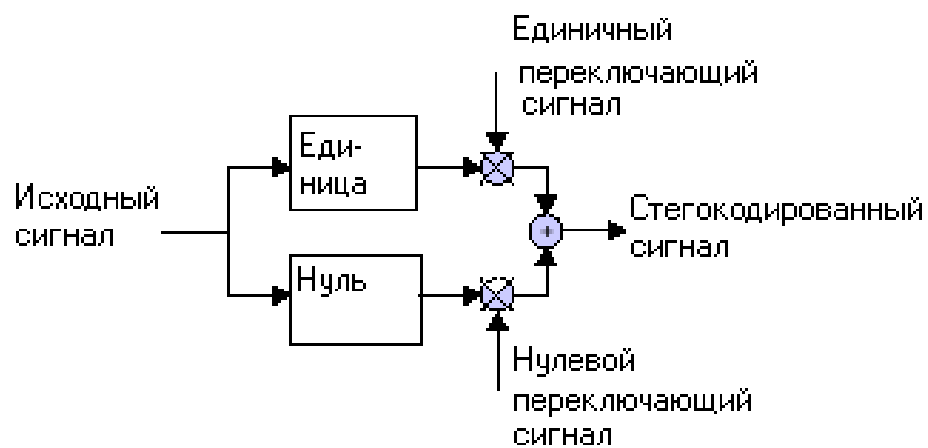


Единичный переключающий сигнал

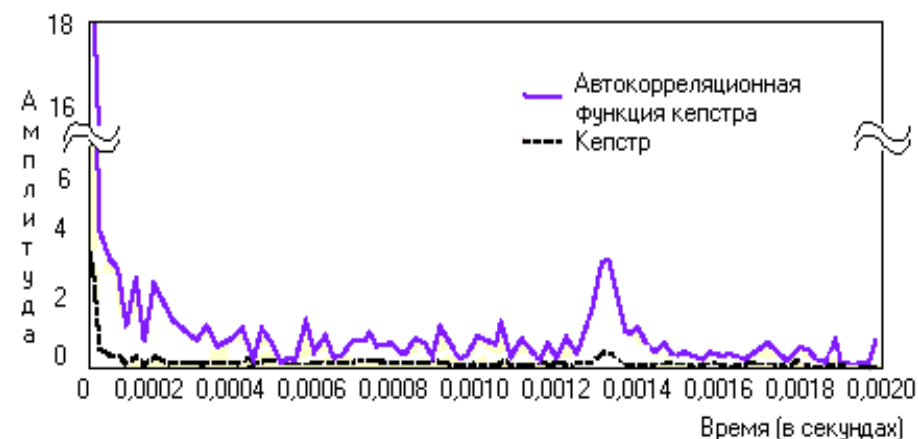


Нулевой переключающий сигнал

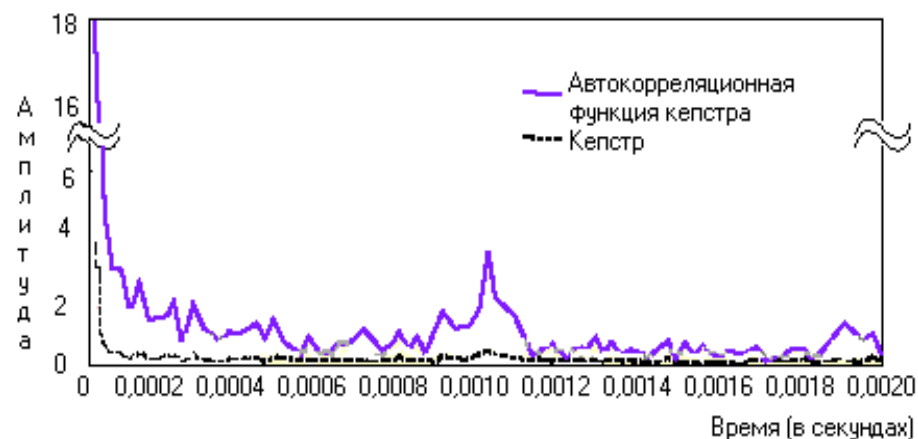
Переключающие сигналы



Блок-схема стегокодера



а) Нуль

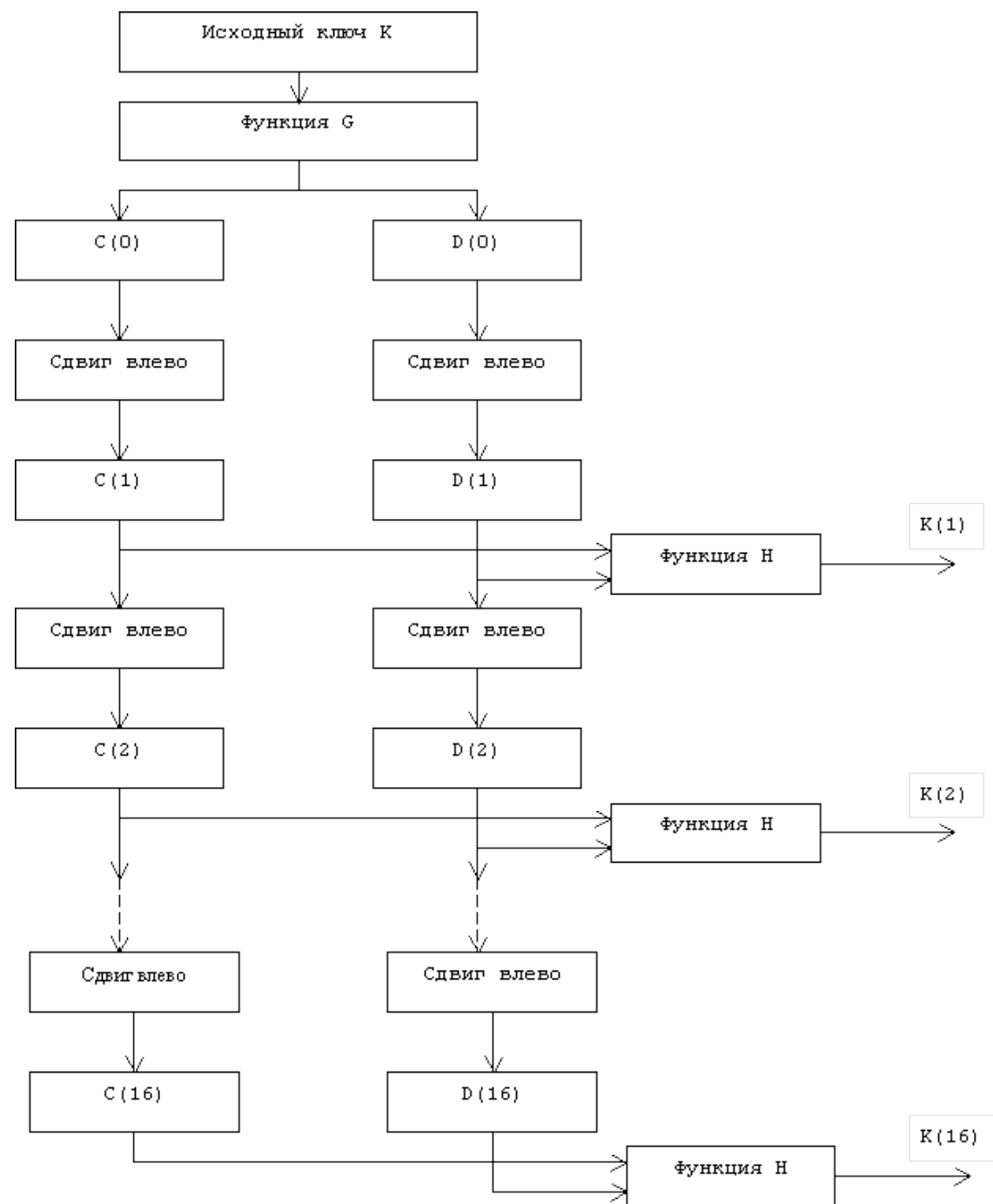


б) Единица

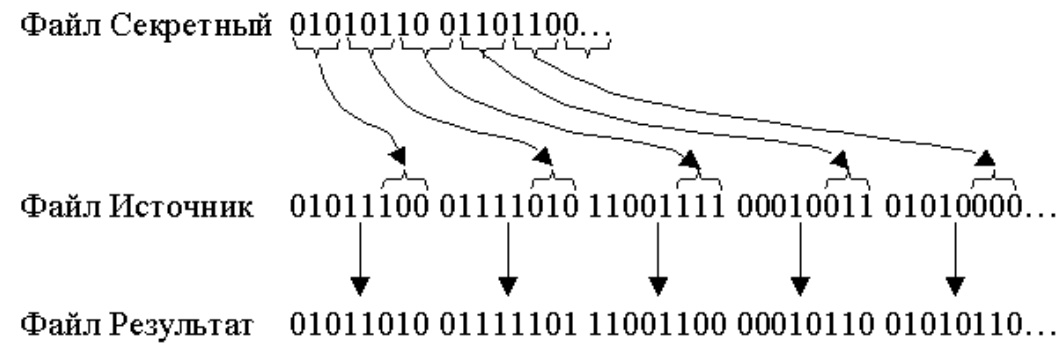
Поведение автокорреляционной функции при различной внедренной информации



Обобщенная схема шифрования в алгоритме DES

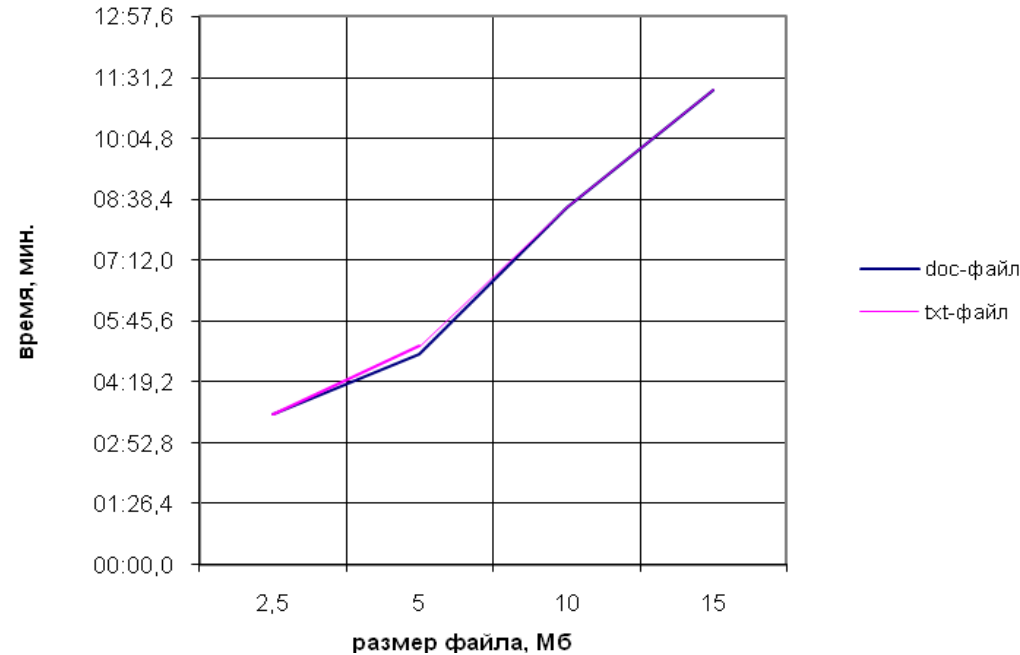


Блок-схема алгоритма
вычисления ключа $K(i)$

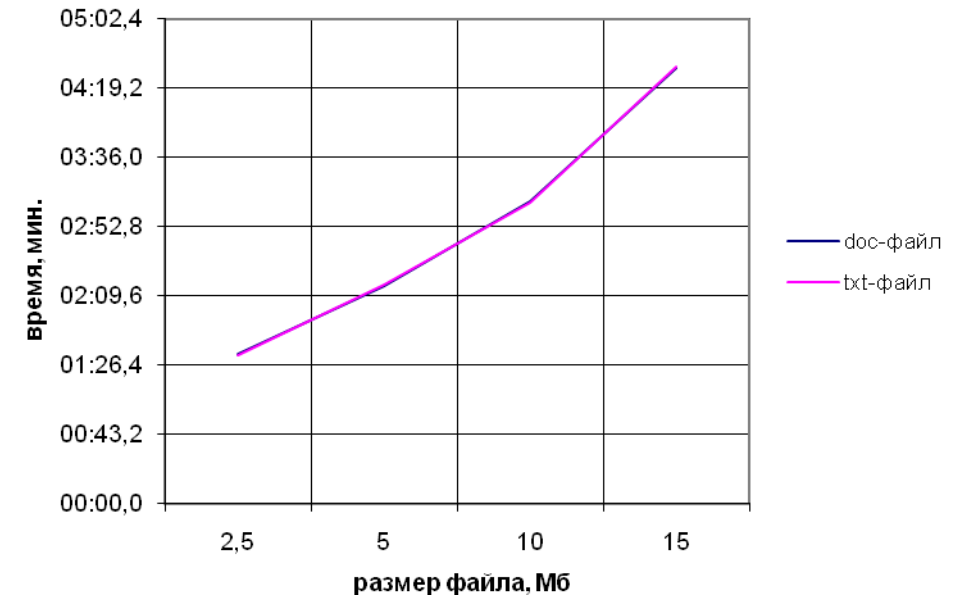


Процесс скрытия изображения

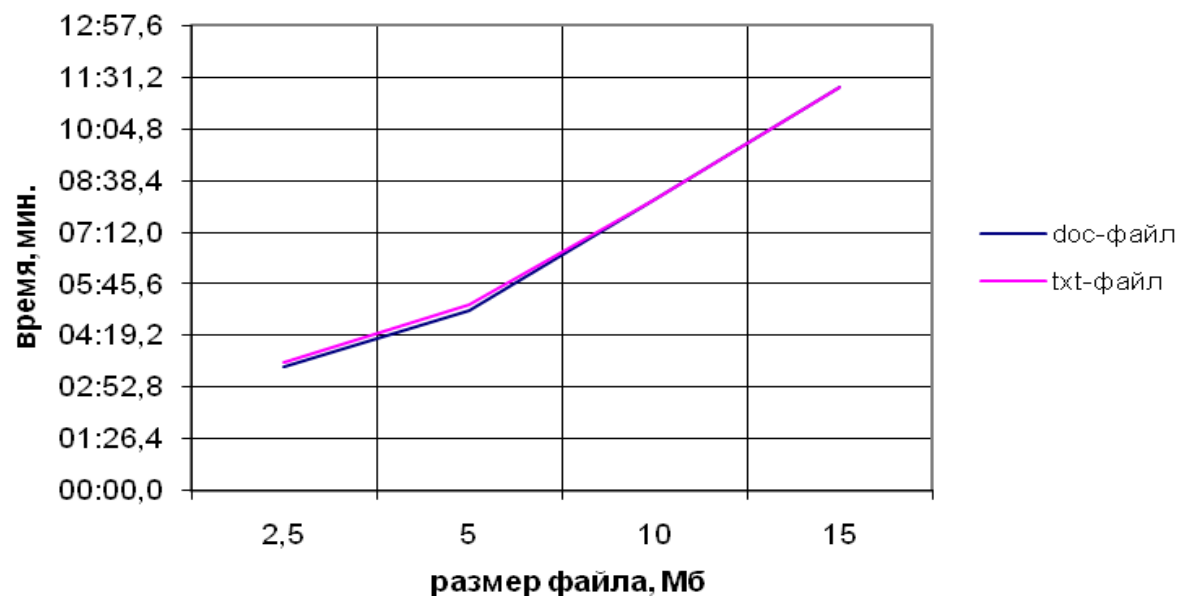
Шифрование (stereo)



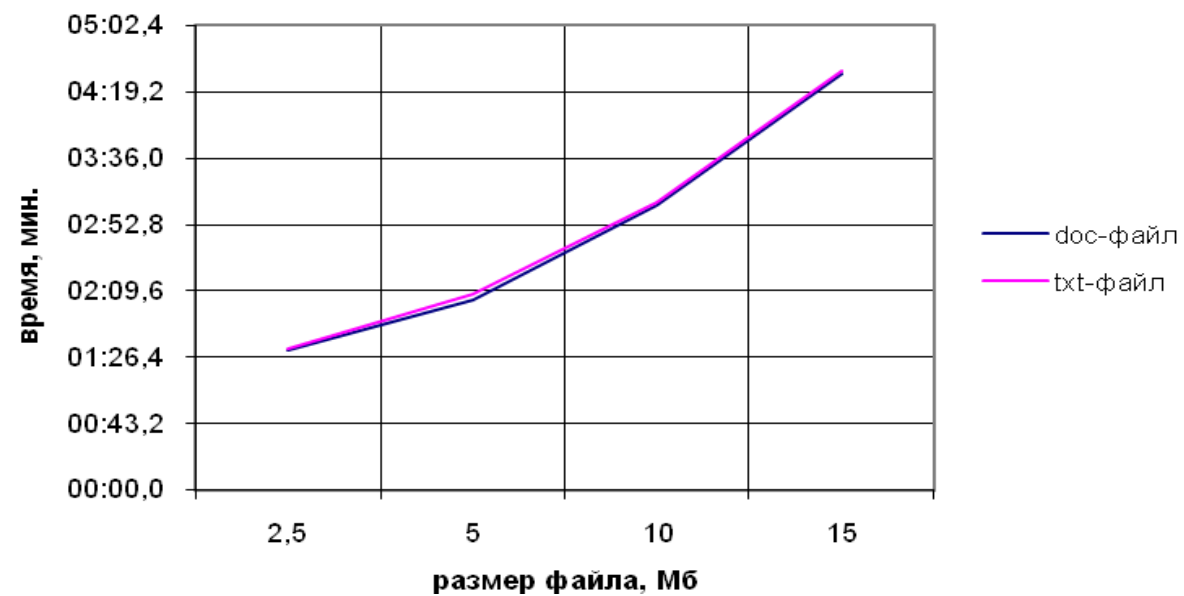
Дешифрование (stereo)

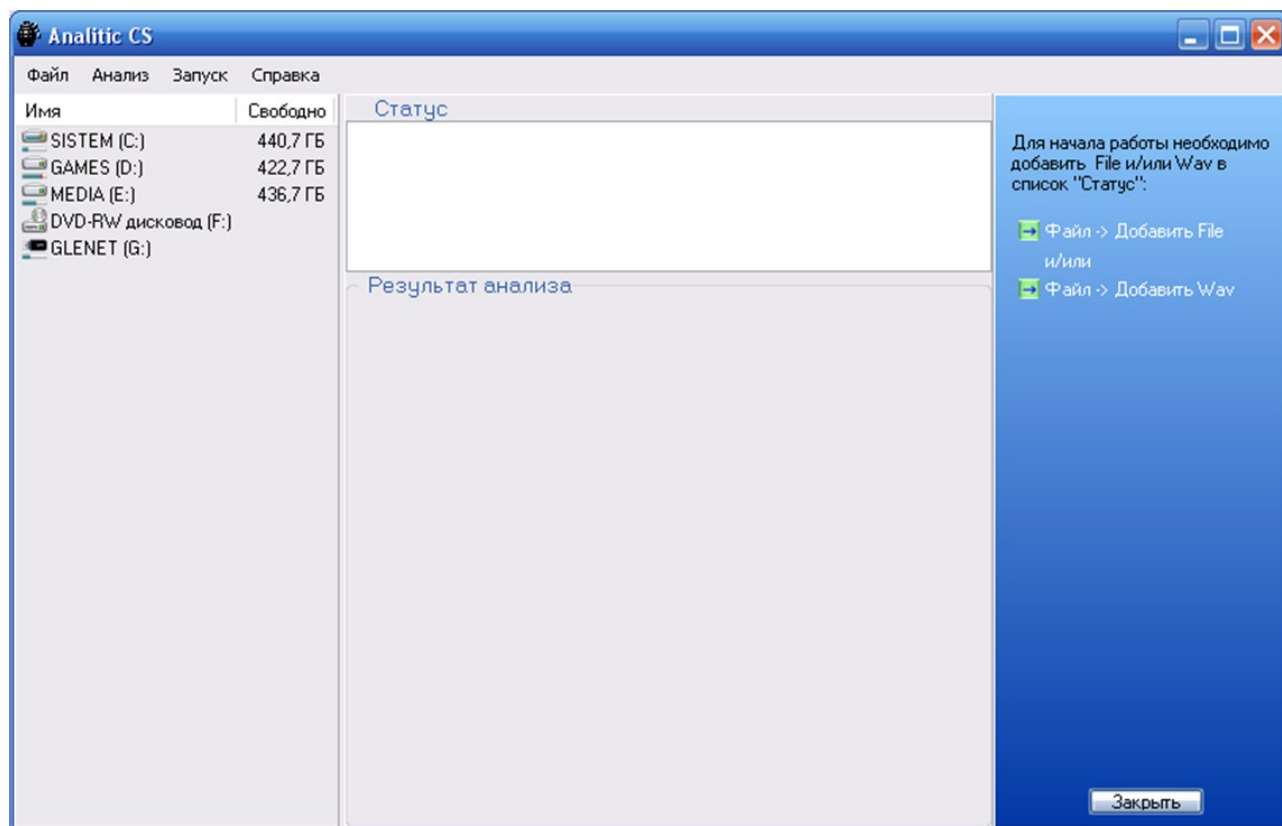


Шифрование (mono)



Дешифрование (mono)

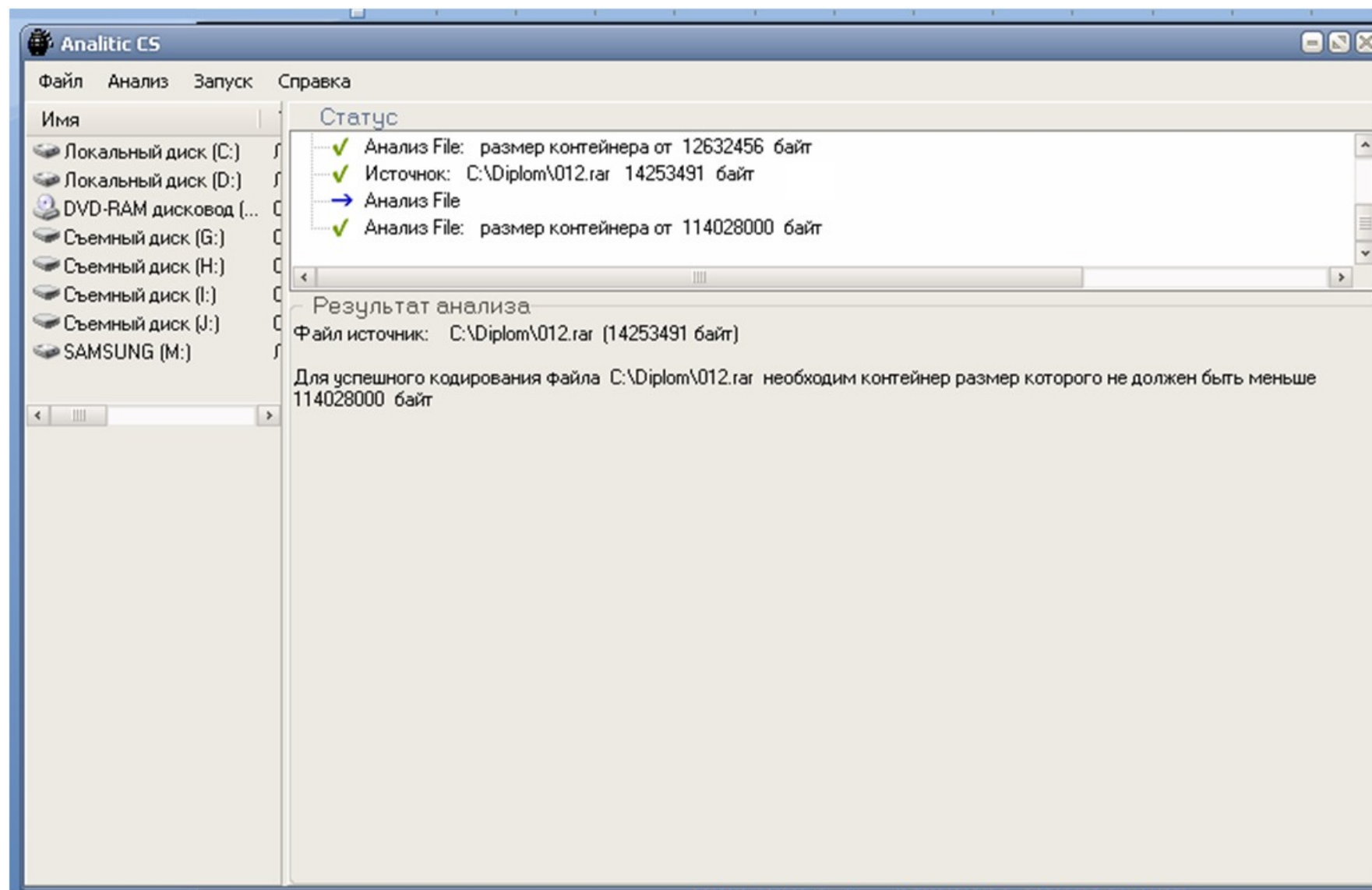




Главное окно Analitic CriptoSystem

Имя	Свободно
SISTEM (C:)	440,7 ГБ
GAMES (D:)	422,7 ГБ
MEDIA (E:)	436,7 ГБ
DVD-RW дискковод (F:)	
GLENET (G:)	

Информация о жестких дисках и носителях



 CryptoSystem

Скрытая информация

☐ Файл
☐ Сообщение

Выберите секретный файл

Путь

Browse

Введите секретное сообщение



Выберите файл, для кодирования

Путь

Browse

Введите пароль

Повторите пароль

Файл, хранящий исходный файл с секретной информацией

Путь

Browse

Выберите файл, в который запишется закодированная инф.

Путь

Browse

Выберите действие

Шифрование

Дешифрование

Статус

О программе

Перезагрузка

Выход