

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,  
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»  
(СПбГУТ)

---

Факультет инфокоммуникационных сетей и систем  
Кафедра защищенных систем связи  
Дисциплина стеганография

ПРАКТИЧЕСКАЯ РАБОТА №5

Идеальные и почти идеальные стegosистемы  
(тема практической работы)

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи  
(код и наименование направления/специальности)

Студенты:

Громов А. А., ИКТЗ-83

(Ф.И.О., № группы)

\_\_\_\_\_  
(подпись)

Жиляков Г. В., ИКТЗ-83

(Ф.И.О., № группы)

\_\_\_\_\_  
(подпись)

Мазеин Д. С., ИКТЗ-83

(Ф.И.О., № группы)

\_\_\_\_\_  
(подпись)

Миколаени М. С., ИКТЗ-83

(Ф.И.О., № группы)

\_\_\_\_\_  
(подпись)

Научный руководитель:

К.т.н., доцент каф. ЗСС, Герлинг Е. Ю.

(ученая степень, ученое звание, ФИО)

\_\_\_\_\_  
(подпись)

## ОГЛАВЛЕНИЕ

ЦЕЛЬ РАБОТЫ .....	3
ЗАДАЧА.....	3
ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ .....	4
ВЫВОДЫ.....	6

## ЦЕЛЬ РАБОТЫ

Целью данного практического занятия является закрепление на практике, материала, пройденного на лекции. В данном практическом занятии будут даны примеры, для практического решения задачи по теме – лингвистические стегосистемы.

## ЗАДАЧА

### Задачи

Для модели SG-R рассчитать двоичную последовательность после погружения информационной цепочки «1001» в двоичную последовательность (ПО) abaabaabbbabbbaaaabbbb.

Найти другую двоичную последовательность ПО, которая при вложении той же информационной цепочки «1001» приведет к прежней двоичной стегоцепочке.

Ответ:

Погружаем 1001

ab aa ba ab bb ab ba aa ab bb  
v0 u v1 v0 u v0 v1 u v0 u  
v1 u v0 v0 u v1 v1 u v0 u  
ba aa ab ab bb ba ba aa ab bb

ba bb ab ab aa b aba bb ab aa  
v1 u v0 v0 u v1 v1 u v0 u  
v1 u v0 v0 u v1 v1 u v0 u  
ba bb ab ab aa b aba bb ab aa

## ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ

1. Что такое идеальные и почти идеальные СГ? - СГС называется идеальной, если ее обнаружение, при использовании наилучших статистических методов, равносильно случайному угадыванию ее наличия или отсутствия. СГС называется почти идеальной, если при использовании наилучших статистических методов  $\min\{P_m, P_{fa}\} \geq \sigma$ , где  $P_m$  – вероятность пропуска СГС,  $P_{fa}$  – вероятность ложного обнаружения СГС.
2. Какой метод погружения обеспечивает получение идеальной СГ, если отсчеты ПО являются одинаково распределенным и взаимонезависимым гауссовскими величинами. - Модельно-обусловленная СГС.
3. В чем состоит принцип погружения информации для модельно обусловленных СГ, использующих идеальное сжатие ПО? – Предполагается, что статистические свойства ПО известны в точности. Тогда ПО, который является окрашенным гауссовским шумом, преобразуется в белый гауссовский шум. После чего туда вкладывается сообщение и происходит обратное преобразование.
4. В чем состоит принцип погружения информации для СГ с адаптивным квантованием (СГ-АК)? – Необходимо использовать при вложении в квантователе тот факт, что атакующему никогда не известны отсчеты ПО до квантования. Вложение производится только в те отсчеты, которые попадают в интервал шириной  $\epsilon$ , вокруг середин (промежутков) между уровнями. В этом случае отсчет квантуется в ближайший четный уровень, если  $b = 0$  и в нечетный, если  $b = 1$ .
5. В чем состоит принцип погружения информации для СГ с сохранением статистики (СГ-Р) и почему он не является практически реализуемым в полном объеме? - Принцип погружения заключается в разделении ПО на пары, после чего замены этих пар по правилу, представленному выше, в ответе к заданию. Данный принцип не является практически

реализуемым так как количество бит, вложенных в ПО длины « $n$ » всегда будет меньше, чем  $n/2$  и данная величина будет зависеть от статистики ПО ( $P(a), P(b)$ ). Данный принцип можно применять для НЗБ.

## ВЫВОДЫ

В данной практической работе, результаты которой представлены выше, мы закрепили материал, пройденный по теме идеальные и почти идеальные стегосистемы.