

УДК 004.056  
А 47

Стеганографические и криптографические методы защиты информации;  
учебное пособие/ Алексеев А. П. Орлов В.В./ ИУНЛ ПГУТИ - 2010 - 330 с.

**ISBN 978-5-904029-12-8**

**Рецензенты:**

декан факультета телекоммуникаций и радиотехники ПГУТИ д.т.н.,  
профессор Карташевский В.Г.,  
заведующий кафедрой «Защита информации» СамГУ Осипов М.Н.

В учебном пособии в компактной форме описаны основные принципы защиты информации. В книге содержится большое число методических указаний на выполнение лабораторных и практических работ по криптографии и стеганографии. Оптический диск, прилагаемый к этой книге, содержит необходимые программы и начинённые контейнеры, из которых студенты в процессе выполнения лабораторных работ должны суметь извлечь скрытую там информацию.

Книга предназначена для студентов и преподавателей. Преподаватели с помощью этого учебного пособия смогут «беззаботно» провести два семестра занятий. Студенты смогут получить практические навыки в шифровании, дешифровании и создании скрытых каналов связи.

Учебное пособие ориентировано на студентов телекоммуникационных специальностей 210400...210406, 210302, изучающих информатику, на студентов специальностей 210403 и 090106, изучающих защищенные системы связи.

**ISBN 978-5-904029-12-8**

© Алексеев А. П.

© Орлов В.В

© ПГУТИ

## Оглавление

<b>Введение .....</b>	<b>4</b>
<b>1. Криптографические методы защиты информации</b>	<b>7</b>
1.1. Классические симметричные шифры.....	7
1.1.1. Шифр атбаш .....	7
1.1.2. Шифр Цезаря .....	8
1.1.3. Квадрат Полибия .....	9
1.1.4. Аффинные криптосистемы.....	10
1.1.5. Шифр Виженера .....	11
1.1.6. Система Плейфейра.....	13
1.1.7. Система Хилла .....	14
1.1.8. Метод гаммирования.....	15
1.1.9. Метод перестановок .....	17
1.1.10. Перестановки по сложным траекториям	19
1.2. Асимметричные системы .....	22
1.2.1. Алгоритм RSA .....	23
1.3. Шифрование с помощью графических матриц	27
1.4. Шифрование с помощью управляемых операций*	46
1.5. Многоалфавитный адаптивный шифр, основанный на интегральных преобразованиях* .....	54
<b>2. Стеганографические методы защиты информации</b>	<b>61</b>
2.1. Соккрытие информации в рисунках и фотографиях	61
2.2. Соккрытие информации в текстовых документах*	67
2.3. Соккрытие информации в субтитрах фильма*	74
2.4. Основные понятия.....	80
аналога-цифрового преобразования.....	80
2.5. Соккрытие информации в электронных контейнерах	83
2.6. Пространственно-временное распыление .....	91
информации .....	91
2.7. Скрытая передача информации в сегментах TCP	95
<b>3. Лабораторный практикум.....</b>	<b>100</b>
3.1. Симметричные шифры* .....	101
3.2. Моделирование криптосистемы с помощью программы EWB.....	110
3.3. Моделирование криптосистем с помощью программы Multisim .....	114
3.4. Обмен зашифрованными сообщениями .....	123
с помощью программы PGP .....	123
3.5. Стеганографические программы .....	135
Courier и S-Tools .....	135
3.6. Соккрытие информации в текстовых .....	150
и графических файлах.....	150

3.7. Соккрытие информации на HTML – страницах	173
3.8. Соккрытие информации в звуковых файлах формата WAV	208
3.9. Соккрытие информации в субтитрах .....	217
3.10. Внедрение информации в звуковой файл..	228
формата MP3 .....	228
3.11. Стеганографические методы передачи информации в сетях TCP/IP	231
3.12. Соккрытие информации методом временного	242
распыления .....	242
3.13. Соккрытие информации с помощью .....	250
программы Mathcad .....	250
3.14. Соккрытие информации в музыкальных .....	258
файлах формата MIDI .....	258
<b>4. Приложения</b> .....	264
Приложение 4.1 .....	265
Приложение 4.2 .....	266
Приложение 4.3 .....	273
Приложение 4.4. ....	274
Приложение 4.5 .....	275
Приложение 4.6 .....	278
Приложение 4.7 .....	282
<b>Заключение</b> .....	283
<b>Научно- техническая литература</b> .....	285