

ISBN 978-5-904029-72-2

УДК 004.056

А 47

Рецензенты:

заведующий кафедрой «Вычислительная техника» Самарского государственного технического университета д.т.н., профессор

Орлов С.П.,

заведующий кафедрой «Безопасность информационных систем» Самарского университета к.ф.м.н., доцент

Осипов М.Н.

Алексеев А.П. Многоуровневая защита информации. Самара: ПГУ-ТИ-ИУНЛ, 2017. – 128 с. ISBN 978-5-904029-72-2

Книга посвящена вопросам повышения криптостойкости передаваемой информации. Предлагается использовать несколько уровней защиты: криптографический, стеганографический, а также пространственно-временное распыление информации.

Дано описание классических симметричных шифров, асимметричного шифра RSA. Приведён криптоанализ шифра RSA, указаны уязвимости шифра RSA.

Описаны оригинальные симметричные шифры: с помощью графических матриц, управляемых операций и многоалфавитный адаптивный шифр.

Описаны новые способы скрытой передачи информации в TCP-пакетах, в старших разрядах WAV-файла.

Книга предназначена для студентов (специальности 10.03.01, 10.05.02), дипломников, магистров, аспирантов, преподавателей и специалистов, занимающихся вопросами защиты информации.

УДК 004.056

ISBN 978-5-904029-72-2

© Алексеев А.П., 2017

© ФГБОУВО ПГУТИ, 2017

Оглавление

	Введение	3
1	Принципы многоуровневой защиты информации.....	4
2.	Криптографические методы защиты информации	8
	2.1. Симметричные шифры.....	10
	2.1.1. Классические симметричные шифры.....	10
	2.1.2. Шифрование с помощью графических матриц.....	26
	2.1.3. Шифрование с помощью управляемых операций	50
	2.1.4. Многоалфавитный адаптивный шифр.....	59
	2.2. Асимметричные шифры.....	67
	2.2.1. Асимметричный шифр RSA	67
	2.2.2. Криптоанализ шифра RSA.....	76
3.	Стеганографические методы защиты информации	80
	3.1. Основные понятия стеганографии.....	80
	3.2. Метод LSB.....	91
	3.3. Форматная стеганография.....	96
	3.4. Внедрение информации в старшие разряды WAV-файла...	102
	3.5. Скрытая передача информации в сегментах TCP/IP.....	109
4.	Пространственное распыление информации.....	114
5.	Временное распыление информации.....	119
	Заключение.....	122
	Список литературы.....	124
	Оглавление.....	127