UNIVERSITATEA TEHNICĂ A MOLDOVEI

METODE CRIPTOGRAFICE DE PROTECȚIE A INFORMAȚIEI

Partea I

CIFRURI SIMETRICE CLASICE

Indicații didactico-metodice

k	m	k	m
1	26047	6	71592
2	15936	7	60481
3	04825	8	59370
4	93714	9	48269
5	82603	0	37158

Chişinău
2013

UNIVERSITATEA TEHNICĂ A MOLDOVEI
FACULTATEA INGINERIE ŞI MANAGEMENT
ÎN ELECTRONICĂ ŞI TELECOMUNICAȚII
CATEDRA TELECOMUNICAȚII

METODE CRIPTOGRAFICE DE PROTECȚIE A INFORMAȚIEI

Partea I

CIFRURI SIMETRICE CLASICE

Indicații didactico-metodice

Chişinău
UTM
2013

Indicațiile didactico-metodice la disciplina *Teoria transmisiunii informație*i sunt dedicate analizei metodelor contemporane de protecție a informației în sistemele de comunicații digitale.

Indicațiile didactico-metodice sunt propuse studenților UTM la profilul 525 – *Electronică şi comunicații*, specialitatea *Teleradiocomunicații,* pentru ambele forme de învățământ.

Autori: conf., dr. **I. CHIȚUL**
conf., dr. **S. ANDRONIC**
conf., dr. **N. BEJAN**
conf., dr**. L. NEMERENCO**
conf., dr. **P.NISTIRIUC**

Recenzent: conf., dr. **V. MOROZOV**

Redactor coordonator: conf., dr. **I. CHIȚUL**

Redactor: **Eugenia BALAN**

Bun de tipar 19.02.13	Formatul hârtiei 60x84 1/16
Hârtie ofset. Tipar RISO	Tirajul 50 ex.
Coli de tipar 5,75	Comanda nr.16

UTM, 2004, Chişinău, bd. Ştefan cel Mare şi Sfânt, 168
Secția Redactare şi Editare a UTM
2068, Chişinău, str. Studenților 9/9

CUPRINS

BIBLIOGRAFIE

1. Алферов А.П. и др. Основы криптографии. – М.: Гелиос АПВ, 2005. – 478 с.
2. Бабаш А.В., Шанкин Г.П. Криптография. – М.: Солон-Пресс, 2007. – 512 с.
3. Брассар Ж. Современная криптология. М.: Полимед., 1999. – 175 с.
4. Введение в криптографию / Под ред. Ященко В.В. – М.: МНЦМО, 2000. - 288 с.
5. Грибунин В.Г. и др. Цифровая стенография. – М.: Солон-Пресс, 2002. – 272 с.
6. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1996. – 334 с.
7. Кан Д. Взломщики кодов / Пер. с англ. – М.: Центрполиграф, 2000. – 473 с.
8. Конахович Г.Ф. и др. Защита информации в телекоммуникационных системах. – К.: МК-Пресс, 2005. - 279 с.
9. Сидельников В.М. Теория кодирования. – М.: Изд. МГУ, 2006. – 285 с.
10. Смарт Н. Криптография / Пер. с англ. – М.: Техносфера, 2005. – 525 с.
11. Ван Тилберг Х.К.А. Основы криптологии / Пер. с англ. – М.: Мир,2006. – 476 с.
12. Фергюсон Н., Шнайер Б. Практическая криптография. / Пер. с англ. – Вильямс, 2005. – 424 с.
13. Шнайер Б. Прикладная криптография, 2-е изд. / Пер. с англ. – М.: Триумф, 2002. – 816 с.

14. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Пер. с англ. – СПб.: Питер, 2003. – 368 с.
15. Bodean Gh.C. Coduri nonbinare corectoare de erori. –Chişinău: UTM, 2010. –544 p.
16. Kahn D. The Codebreakers, Macmillan, N.Y., 1967, p.473.
17. Meneres A.J., van Oorschet P.C., Vanstone S.A. Handbook of applied cryptography, 1996, p.794.
18. Mollin R.A. Codes. The guide to secrecy from Ancient to modern times. Chapman & Hall / CRC, 2005, p.635.
19. Mollin R.A. An introduction to cryptography. 2-nd ed./ Chapman & Hall / CRC, 2007, p.413.
20. Shannon C.E. Communication Theory of Secrecy Systems, Bell Syst. Techn. J., vol. 28, October, 1949, pp. 656-715.
21. Stallings W/ Cryptography and network security. Principles and practices. 4-th ed., Prentice Hall, 2005, p.592.
22. Stamp M., Low R.M. Applied cryptoanalyses. John Wiley & Sons, 2007, p.425.