

С.Е. Остапов, С.П. Євсєєв,
О.Г. Король

004.056.5
0-76

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник



Видавництво "Новий Світ – 2000"





Остапов Сергій Едуардович, д.ф.м.н., проф.,

Дата і місце народження: 1957, Чернівці, Україна

Освіта: Чернівський державний університет, 1980.

Посада: завідувач кафедри програмного забезпечення комп'ютерних систем Чернівецького національного університету імені Юрія Федьковича

Кола наукових інтересів: інформаційна безпека, криптографія на основі клітинних автоматів.

Публікації: автор понад 150 наукових публікацій, з них: 6 монографій, понад 100 наукових статей, понад 20 навчальних посібників.

ORCID: <https://orcid.org/0000-0002-4139-4152>.

Scopus Author ID: 6602744324

E-mail: sergey.ostapov@gmail.com



Свєсєєв Сергій Петрович, д.т.н., с.н.с.,

Дата і місце народження: 1969, Хардизьк, Донецька обл.

Освіта: Харківський військовий університет, 2002.

Посада: завідувач кафедри кібербезпеки та інформаційних технологій Харківського національного економічного університету.

Кола наукових інтересів: захист банківських інформаційних ресурсів в АБС, криптографія.

Публікації: автор понад 250 наукових публікацій, з них: 5 монографій, 119 наукових статей, 32 патента на корисну модель, 23 навчальних посібника.

ORCID: <https://orcid.org/0000-0003-1647-6444>

Scopus Author ID: 57190440690

E-mail: serhii.vevseiev@hneu.net



Король Ольга Григорівна, к.т.н., доц.,

Дата і місце народження: 1981, Джанкой, АР Крим.

Освіта: Харківський економічний університет, 2006.

Посада: доцент кафедри кібербезпеки та інформаційних технологій Харківського національного економічного університету.

Кола наукових інтересів: захист банківських інформаційних ресурсів в АБС

Публікації: автор понад 130 наукових публікацій, з них: 3 монографії, 58 наукових статей, 8 патентів, 14 навчальних посібника

ORCID: <https://orcid.org/0000-0002-8733-9984>

Scopus Author ID: 57190440690

E-mail: korol.olha2015@gmail.com

Вища освіта в Україні

Видавництво "Новий Світ – 2000"



• • , • • , • •

2- ,

« -2000»

2024

.....	7
1.	9
1.1.	9
1.2.	10
1.3.	17
1.4.	18
1.5.	23
2.	33
2.1. TCSEC (« ») -	33
2.2. CommonCriteria (« ») -	36
2.3. 2.5-004-99 «»	47
3.	52
3.1. « »	53
3.2.	58
3.3.	66
3.4.	67
3.5.	73
3.6.	79
4.	83
4.1. DES (Data Encryption Standard) - 1977	83
4.2. DES (3DES, DESX).....	93
4.3. 28147-89	96
4.4. Rijndael.....	99
4.5.	107
4.6.	119
4.7. (, , CFB, OFB,).....	138

4.8.			153
5.			160
5.1.	RSA,		160
5.2.			168
6.			171
6.1.			171
6.2.	MD.....		192
6.3.	SHA-1, SHA-2.....		202
6.4.	SHA-3.....		208
7.			229
7.1.	(RSA),		229
7.2.			231
7.3.	DSA.....		261
7.4.	34.10-94 34.10-2001		263
7.5.	4145.....		266
8.			281
8.1.			283
8.2.			284
8.3.			288
8.4.			291
9.			293
9.1.			293
9.2.			298
10.			306
10.1.			306
10.2.			325
10.3.			329
10.4.			333
10.5.			335
11.			369

11.1.	369
11.2.	380
11.3.	383
12.	397
12.1.	397
12.2.	402
12.3.	404
12.4.	410
12.5.	415
13.	429
13.1.	429
13.2.	435
13.3.	Windows.....	436
13.4.	Windows Linux.....	454
	466
	468
	1	469
	2.....	510
	3.....	537
	4.....	548
	5.....	558
	6.....	563
	7.....	569
	8.....	572
	9.....	578
	10	584
	591
	11	592
	12.....	603
	13.....	610
	14.....	615
	15.....	618

16.....	628
17.....	633
18.....	636
19.....	638
.....	641
20.....	642
21.....	647
22.....	651
23.....	654
24.....	664
25.....	669
.....	673