

Міністерство освіти і науки, молоді та спорту України
Харківський національний університет імені В. Н. Каразіна

В. І. Єсін
О. О. Кузнецов
Л. С. Сорока

Безпека інформаційних систем і технологій

Навчальний посібник

Рекомендовано Міністерством освіти і науки, молоді та спорту України
як навчальний посібник для студентів вищих навчальних закладів,
які навчаються за напрямками підготовки
«Безпека інформаційних і комунікаційних систем»

Харків – 2013

УДК 004.056
ББК 32.973.202 я73
Е 83

Рецензенти:

Горбенко І. Д. – доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Харківського національного технічного університету радіоелектроніки;

Краснобаєв В. А. – доктор технічних наук, професор кафедри автоматизації та комп'ютерних технологій Харківського національного технічного університету сільського господарства;

Потій О. В. – доктор технічних наук, доцент, начальник кафедри радіолокаційних систем пунктів управління повітряних сил Харківського університету повітряних сил імені І. М. Кожедуба.

*Рекомендовано Міністерством освіти і науки, молоді та спорту України
як навчальний посібник для студентів вищих навчальних закладів,
які навчаються за напрямками підготовки
«Безпека інформаційних і комунікаційних систем»
(Лист № 1/11-871 від 30 січня 2013 р.)*

Єсін В. І.

Е 83 **Безпека інформаційних систем і технологій : навчальний посібник [для студентів вищих навчальних закладів, які навчаються за напрямками підготовки «Безпека інформаційних і комунікаційних систем»] / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с. ISBN 978-966-623-927-6**

У навчальному посібнику розглядаються сучасні напрями забезпечення безпеки інформаційних систем і технологій. Викладаються технічні, криптографічні, програмні методи і засоби захисту інформації. Формулюються проблеми вразливості сучасних інформаційних систем і технологій, розглядаються питання захисту інформації в розподілених інформаційних системах, організаційно-правове забезпечення захисту інформації.

Посібник призначений для студентів вищих навчальних закладів, які навчаються за напрямками підготовки «Безпека інформаційних і комунікаційних систем».

**УДК 004.056
ББК 32.973.202 я73**

ISBN 978-966-623-927-6

© Харківський національний університет імені В. Н. Каразіна, 2013
© Єсін В. І., Кузнецов О. О., Сорока Л. С., 2013
© Будник О. В., макет обкладинки, 2013

Зміст

<i>Вступ</i>	10
I. Основи безпеки інформації	11
<i>Розділ 1. Роль інформації в сучасному світі та необхідність її захисту</i>	11
1.1. Інформація, її значення і необхідність захисту в сучасних умовах.....	11
1.2. Підробка документів.....	25
<i>Розділ 2. Загрози безпеці інформаційних систем</i>	29
2.1. Випадкові загрози.....	30
2.2. Навмисні загрози.....	31
2.3. Класифікації загроз.....	35
<i>Розділ 3. Канали просочування інформації</i>	41
3.1. Характеристика основних каналів просочування інформації.....	41
3.2. Канали просочування інформації в процесі експлуатації ЕОМ.....	59
<i>Розділ 4. Загрози безпеці програмного забезпечення</i>	66
4.1. Загрози безпеці програмного забезпечення інформаційних систем.....	66
4.2. Загальна характеристика та класифікація шкідливих програм.....	70
II. Методи й засоби захисту інформації в інформаційних системах	110
<i>Розділ 5. Захист інформації від випадкових загроз</i>	110
5.1. Класифікація методів захисту інформації від випадкових загроз.....	110
5.2. Характеристика методів і засобів захисту інформації.....	110
<i>Розділ 6. Технічні методи й засоби захисту інформації</i>	123
6.1. Класифікація технічних засобів захисту.....	123
6.2. Характеристика методів і засобів захисту.....	123
<i>Розділ 7. Захист інформації від несанкціонованого доступу</i>	146
7.1. Принципи захисту інформації від несанкціонованого доступу.....	146
7.2. Методи ідентифікації та автентифікації користувачів.....	150
<i>Розділ 8. Криптографічні методи захисту інформації</i>	167
8.1. Основні поняття та історія криптографії.....	167
8.2. Шифр заміни.....	174
8.3. Шифр перестановки.....	182
8.4. Шифр Вернама й проблема практичного використання абсолютно стійкого шифру.....	186
8.5. Класифікація шифрів.....	192
8.6. Коротка характеристика шифрів з ключем.....	193
8.7. Симетрична криптографія.....	199

8.7.1. Основи будови поточкових шифрів.....	199
8.7.2. Лінійні реєстри зсуву.....	207
8.7.3. Нелінійні поточкові шифри.....	211
8.7.4. Основи блокового шифрування.....	213
8.7.5. Режими блокового шифрування.....	218
8.7.5.1. Режим електронної кодової книги.....	218
8.7.5.2. Режим зчеплення блоків шифртексту.....	222
8.7.5.3. Режим зворотного зв'язку по шифртексту.....	227
8.7.5.4. Режим зворотного зв'язку по виходу.....	231
8.7.6. Мережі Фейстеля.....	234
8.7.7. Стандарт шифрування DES.....	242
8.7.8. Стандарт шифрування ГОСТ.....	247
8.7.9. Шифр TEA.....	249
8.7.10. Шифр IDEA.....	250
8.7.11. Відкритий конкурс США на криптостандарт блокового шифрування та його результати.....	253
8.7.11.1. Шифр MARS.....	256
8.7.11.2. Шифр RC6.....	265
8.7.11.3. Шифр Serpent.....	268
8.7.11.4. Шифр TwoFish.....	269
8.7.11.5. Шифр RIJNDAEL.....	271
8.7.12. Європейський криптопроект NESSIE.....	283
8.7.13. Національний конкурс із розробки стандарту симетричного блокового криптоалгоритму України.....	284
8.7.13.1. Симетричний блоковий криптографічний алгоритм «Калина».....	284
8.7.13.2. Симетричний блоковий криптографічний алгоритм «Мухомор».....	313
8.7.13.3. Симетричний блоковий криптографічний алгоритм «Лабіринт».....	332
8.7.13.4. Симетричний блоковий криптографічний алгоритм RSB-32.....	350
8.7.13.5. Симетричний блоковий криптографічний алгоритм ADE.....	361
8.8. Асиметрична криптографія.....	396
8.8.1. Основні принципи асиметричної криптографії.....	396
8.8.2. Схема асиметричного шифрування RSA.....	400
8.8.3. Схема асиметричного шифрування Рабіна.....	404
8.8.4. Схема асиметричного шифрування Ель Гамалія.....	405
8.8.5. Електронний цифровий підпис.....	408
8.9. Основні типи криптоаналітичного розкриття.....	411

8.9.1. Методи криптоаналізу.....	417
8.10. Стійкість криптографічних систем.....	433
8.11. Управління криптографічними ключами.....	436
8.11.1. Генерація ключів.....	437
8.11.2. Зберігання ключів.....	439
8.11.3. Розподіл ключів.....	444
8.11.4. Депонування ключів.....	456
<i>Розділ 9. Програмні методи й засоби захисту.....</i>	<i>461</i>
9.1. Програмне забезпечення та інформаційна безпека.....	461
9.1.1. Основні механізми інформаційної безпеки програмного забезпечення.....	461
9.1.2. Контроль життєвого циклу програмного забезпечення.....	466
9.1.3. Захист програмного забезпечення.....	470
9.2. Захист від шкідливого програмного забезпечення.....	481
9.2.1. Методи та засоби захисту від шкідливого програмного забезпечення.....	481
9.2.2. Організація системи антивірусного захисту.....	505
<i>Розділ 10. Захист інформації в розподілених інформаційних системах.....</i>	<i>514</i>
10.1. Міжмережні екрани	515
10.2. Технологія VPN.....	525
10.3. Сканери уразливості.....	530
<i>Розділ 11. Організаційно-правове забезпечення захисту інформації.....</i>	<i>539</i>
11.1. Основні міжнародні стандарти інформаційної безпеки.....	539
11.1.1. Вимоги до безпеки інформаційних систем у США.....	540
11.1.2. Вимоги до безпеки інформаційних систем у Росії.....	544
11.1.3. Відомі міжнародні стандарти інформаційної безпеки.....	549
11.1.4. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, введені в дію в Україні.....	566
11.2. Організаційні заходи щодо захисту інформації.....	572
<i>Додаток</i>	<i>582</i>
<i>Глосарій.....</i>	<i>616</i>
<i>Список використаної літератури.....</i>	<i>625</i>
