



**Захист інформації  
в мережах  
передачі даних**

**Юдін О.К.  
Корченко О.Г.  
Конахович Г.Ф.**

УДК 004.056.5 (0758)

ББК з 880-021я7

Ю 163

**Рецензенти:**

- **Новіков О.М.** – заступник голови Науково-методичної ради МОН України, проф., доктор техн. наук, директор фізико-технічного інституту НТУУ “КПІ”(Київський політехнічний інститут)
- **Стасюк О.І.** – проф., доктор техн. наук, Державний економіко-технологічний університет транспорту
- **Рудницький В.М.** – проф., доктор техн. наук, Черкаський державний технологічний університет

*Гриф МОН України. Лист № 1.4/18.Г-1 від 08.01.09 р.*

Ю 163 **Юдін О.К., Корченко О.Г., Конахович Г.Ф.**

Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.

**ISBN 978-966-97108-6-4**

У підручнику систематизовано викладено основні методи та поняття побудови інформаційно-комунікаційних систем та мереж на основі багаторівневих моделей, сучасних процесів передачі і обробки даних. Детально проведено класифікацію методів та засобів несанкціонованого доступу до інформаційних ресурсів. Викладено основи теорії передачі даних в системах бездротового зв'язку на базі новітніх технологій розширення спектру, а також представлено принципи побудови та режими роботи бездротових систем та мереж. Визначені принципи захисту інформації в інформаційних системах та мережах за допомогою криптографічних методів, приведені методи та технології практичного застосування криптографічних алгоритмів та протоколів, а також загальні поняття криптографічного аналізу. Представлено основні принципи захисту інформації в системах та мережах передачі даних за допомогою стеганографічних методів й алгоритмів. Визначені мета і завдання, сутність методів та засобів захисту інформації від несанкціонованого доступу, а також принципи організації систем захисту бездротових мереж.

Широко викладено технології та методи захисту інформації від руйнівних програмних впливів. Визначено роль та місце нормативно-правового та організаційного забезпечення інформаційної безпеки з урахуванням вітчизняних та міжнародних стандартів.

Підручник призначено для студентів технічних спеціальностей вищих навчальних закладів, аспірантів, наукових та інженерно-технічних працівників з напрямом інформаційної безпеки.

ISBN 978-966-97108-6-4

© Юдін О.К., 2009

© Корченко О.Г., 2009

© Конахович Г.Ф., 2009

© ТОВ «НВП»ІНТЕРСЕРВІС», 2009

784 717

# ЗМІСТ

<b>ВСТУП</b> .....	6
<b>Розділ 1. ОСНОВНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ</b> .....	8
1.1. Визначення інформаційної безпеки .....	8
1.2. Загрози інформаційним ресурсам ІКСМ .....	10
1.3. Побудова моделі порушника .....	14
1.4. Основні положення щодо методів і засобів забезпечення інформаційної безпеки .....	21
1.5. Основні характеристики інформаційної системи, як об'єкта захисту .....	30
1.6. Атаки на інформаційні ресурси системи. Класифікація .....	38
1.7. Основні принципи та рівні захисту інформаційних систем .....	56
<b>Розділ 2. ІНФОРМАЦІЙНІ СИСТЕМИ ПЕРЕДАЧІ ДАНИХ</b> .....	64
2.1. Основні положення .....	64
2.2. Модель взаємодії відкритих систем OSI .....	72
2.3. Розробка інформаційних систем передачі даних .....	86
2.4. Багаторівнева технологія серверної взаємодії .....	97
2.5. Принципи взаємодії Web- навігаторів .....	107
2.6. Розподілена обробка інформації на основі мігруючих програм .....	110
2.7. Організація системи доступу до баз даних .....	116
2.8. Перспективи розвитку систем серверної взаємодії .....	121
<b>Розділ 3. БЕЗДРОТОВІ СИСТЕМИ ПЕРЕДАЧІ ДАНИХ</b> .....	126
3.1. Основи теорії передачі даних в бездротових мережах .....	127
3.2. Види модуляції в системах бездротового зв'язку .....	134
3.3. Технології розширення спектру бездротових мереж .....	139
3.4. Методи доступу до ресурсів інформаційного середовища .....	147
3.5. Методи завадостійкого кодування в каналах бездротового зв'язку .....	154
3.6. Принципи побудови та режими роботи систем та мереж бездротового зв'язку .....	158
3.7. Супутникові інформаційні системи передачі даних .....	174
3.8. Множинний доступ до інформаційних ресурсів .....	185
<b>Розділ 4. СИСТЕМИ ПЕРЕДАЧІ МОВНОЇ ІНФОРМАЦІЇ</b> .....	207
4.1. Характеристики безперервних джерел та одержувачів повідомлень .....	208

4.2. Компресія мовних сигналів .....	220
4.3. Статистичні характеристики мовних повідомлень .....	232
4.4. Параметрична компресія мовних сигналів .....	235
4.5. Системи передачі безперервних повідомлень за допомогою дискретних сигналів.....	242
4.6. Пакетна передача мови .....	247
4.7. Статистичне ущільнення .....	262
4.8. Протокол X.25 .....	265
4.9. Протокол Frame Relay.....	271
4.10. Організація мереж на базі технологій ATM .....	279
4.11. Загальні принципи IP – телефонії.....	289

## **Розділ 5. СИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ**

<b>ІНФОРМАЦІЇ</b> .....	299
5.1. Історичні відомості .....	299
5.2. Базові поняття криптографії.....	305
5.3. Шифрування в каналах зв'язку .....	319
5.4. Цифровий підпис.....	322
5.5. Базові алгоритми з використанням ключів .....	326
5.6. Засоби криптографічного захисту інформаційно-комунікаційних систем .....	350

## **Розділ 6. СТЕГАНОГРАФІЧНІ СИСТЕМИ ЗАХИСТУ**

<b>ІНФОРМАЦІЇ</b> .....	373
6.1. Моделі та задачі систем стеганографічного шифрування.....	376
6.2. Структурна схема і математична модель типової стеганосистеми .....	380
6.3. Протоколи стеганографічних систем .....	390
6.4. Принципи стеганографічного аналізу .....	397
6.5. Основні етапи практичного стеганоаналізу.....	402
6.6. Пропускна здатність каналів передачі приховуваних даних .....	423
6.7. Стеганографічні методи приховування даних і їх реалізація .....	448

## **Розділ 7. МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ**

7.1. Основні принципи політики безпеки .....	462
7.2. Класичні моделі систем захисту інформаційних ресурсів. Оцінка ефективності .....	467
7.3. Програмно-апаратні комплекси міжмережного захисту інформаційних ресурсів.....	504

7.4. Концепція трьох «А». Аутентифікація. Авторизація. Аудит. ....	525
7.5 Структурні моделі організації систем безпеки корпоративних мереж.....	542
7.6. Несанкціонований доступ до інформаційних ресурсів бездротових мереж.....	557
<b>Розділ 8. ЗАХИСТ ІНФОРМАЦІЙНІЙ ВІД РУЙНІВНИХ ПРОГРАМНИХ ВПЛИВІВ .....</b>	<b>566</b>
8.1 Задачі захисту програмного забезпечення. Класифікація загроз.....	566
8.2 Класифікація комп'ютерних вірусів .....	574
8.3 Методи та засоби захисту програмного забезпечення.....	595
8.4 Методи боротьби з вірусами.....	601
8.5 Захист ПЗ від реасемблерів та налагоджувачів .....	612
8.6 Системний підхід до захисту ПЗ.....	628
<b>Розділ 9. КОНЦЕПЦІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА БАЗІ МІЖНАРОДНИХ ТА ВІТЧИЗНЯНИХ СТАНДАРТІВ .....</b>	<b>636</b>
9.1 Загальні положення щодо організації технічного захисту інформації у ІКСМ.....	638
9.2 Розробка технічної політики безпеки інформаційних ресурсів ІКСМ.....	641
9.3 Критерії оцінки захищеності інформації від несанкціонованого доступу .....	649
9.4 Методика оцінки захищеності інформації в АТС.....	655
9.5 Захист інформаційних ресурсів на базі міжнародних стандартів ISO/IEC.....	657
9.6 Основні заходи забезпечення безпеки інформаційних мереж.....	669
9.7 Організація управління доступом .....	676
9.8 Заходи забезпечення конфіденційності .....	689
9.9 Цілісність системного програмного забезпечення .....	693
9.10 Управління безперервністю бізнесу.....	695
<b>СПИСОК ЛІТЕРАТУРИ .....</b>	<b>700</b>