

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

004.056
0-76

Кібербезпека: сучасні технології захисту

Навчальний посібник



Видавництво "Новий Світ – 2000"



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний економічний університет
імені Семена Кузнеця

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

КІБЕРБЕЗПЕКА: СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ

Навчальний посібник

«Новий Світ-2000»
Львів
2019

УДК 004.056.5(076.5)

**Рекомендовано до видання рішенням вченої ради
Харківського національного економічного університету**

Рецензенти;

Дудикевич В. Б. докт. техн. наук, професор, зав. кафедри захисту інформації
Національного університету "Львівська політехніка";

Поморова О. В. докт. техн. наук, професор, зав. кафедри системного
програмування Хмельницького національного університету;

Виклюк Я. І. докт. техн. наук, проректор з наукової роботи та міжнародних
зв'язків ПВНЗ "Буковинський університет".

Автори: доктор фізико-математичних наук, професор С. Е. Остапов (вступ, розділи 1 - 3, 8, 9); доктор технічних наук, старший науковий співробітник С. П. Євсеєв (розділи 4, 5, 7, 10); кандидат технічних наук О. Г. Король (розділи 6, 11 - 13).

Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Львів; «Новий Світ- 2000», 2019. – 678 с.

У пропонованому виданні викладені основи сучасного захисту інформації в комп'ютерних системах, не пов'язаних з державною таємницею. Посібник складається з теоретичного матеріалу та лабораторного практикуму. У теоретичній частині висвітлено основні поняття й подані визначення, які стосуються захисту інформації, формування політики безпеки. Розглянуто критерії оцінки захищеності комп'ютерних систем, основи криптографічного захисту інформації, захист інформації від несанкціонованого доступу в сучасних операційних системах, описано комплексні системи захисту в корпоративних інформаційних системах.

Для студентів, які навчаються за галуззю 12 - «Інформаційні технології» всіх форм навчання, інших спеціальностей, де вивчається цикл дисциплін захисту інформації, а також для самостійного опанування його основами.

ISBN 978-617-7519-44-6

© Остапов С. Е., Євсеєв С. П., Король О. Г., 2019

© «Новий Світ-2000, ФОП Піча С. В., 2019

ЗМІСТ

Вступ	7
Розділ 1. Огляд безпеки системи.....	9
1.1. Основні поняття.....	9
1.2. Захист інформації та його головні завдання.....	10
1.3. Поняття про інформацію з обмеженим доступом.....	17
1.4. Структура політики безпеки та її основні частини.....	18
1.5. Життєвий цикл розробки систем безпеки.....	23
Розділ 2. Механізми і політики розмежування прав доступу.....	33
2.1. TCSEC («Оранжева книга») - перший стандарт у галузі оцінки захищеності комп'ютерних систем.....	33
2.2. CommonCriteria («Загальні критерії») - європейський стандарт у галузі оцінки захищеності комп'ютерних систем.....	36
2.3. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу».....	47
Розділ 3. Шифрування даних.....	52
3.1. Основні поняття праці К.Шеннона «Теорія зв'язку в секретних системах».....	53
3.2. Симетричні, асиметричні та комбіновані криптосистеми. їх переваги та недоліки.....	58
3.3. Основні вимоги до сучасних криптосистем.....	66
3.4. Сітка Х.Фейстеля, її переваги та недоліки.....	67
3.5. Класифікація сучасних криптосистем.....	73
3.6. Математичні основи асиметричної криптографії.....	79
Розділ 4. Алгоритми із секретним ключем.....	83
4.1. DES (Data Encryption Standard) - стандарт шифрування даних США 1977 року.....	83
4.2. Основні модифікації DES (3DES, DESX).....	93
4.3. Алгоритм криптографічного перетворення ГОСТ 28147-89	96
4.4. Алгоритм Rijndael.....	99
4.5. Інші відомі блокові шифри.....	107
4.6. Огляд алгоритмів українського конкурсу на сертифікований симетричний криптоалгоритм.....	119
4.7. Основні режими роботи симетричних алгоритмів (ECB, CBC, CFB, OFB, режим генерування імітовставки).....	138

4.8. Сучасні потокові шифри, їх переваги та недоліки.....	153
Розділ 5. Алгоритми з публічним ключем.....	160
5.1. Алгоритм RSA, його криптостійкість і швидкість роботи.....	160
5.2. Алгоритм Ель Гамалія, його безпека та криптостійкість.....	168
Розділ 6. Протоколи автентифікації.....	171
6.1. Поняття про хешувальні алгоритми, їх призначення, вимоги до них.....	171
6.2. Алгоритми сімейства MD.....	192
6.3. Алгоритми SHA-1, SHA-2.....	202
6.4. Огляд алгоритмів хешування конкурсу SHA-3.....	208
Розділ 7. Цифрові підписи.....	229
7.1. Поняття про цифровий підпис (на прикладі RSA), вимоги до нього.....	229
7.2. Основні алгоритми електронного цифрового підпису.....	231
7.3. Федеральний стандарт цифрового підпису DSA.....	261
7.4. Стандарти ЕЦП ГОСТ Р 34.10-94 та ГОСТ Р 34.10-2001	263
7.5. Український алгоритм ЕЦП ДСТУ 4145.....	266
Розділ 8. Основні види атак, принципи криптоаналізу.....	281
8.1. Класифікація атак на симетричні криптоалгоритми.....	283
8.2. Класифікація атак на асиметричні криптоалгоритми.....	284
8.3. Диференціальний криптоаналіз.....	288
8.4. Лінійний криптоаналіз.....	291
Розділ 9. Основні напрямки розвитку сучасної криптографії.....	293
9.1. Нові асиметричні алгоритми на основі еліптичних кривих.....	293
9.2. Проблеми генерування випадкових та псевдовипадкових послідовностей.....	298
Розділ 10. Механізми та протоколи керування ключами в інфраструктурах публічних ключів інформаційної системи.....	306
10.1. Основні положення керування ключами. Життєвий цикл криптографічного ключа.....	306
10.2. Керування ключами на основі симетричних методів.....	325
10.3. Керування ключами на основі асиметричних методів.....	329
10.4. Безпека керування ключами.....	333
10.5. Структура та призначення Інфраструктури публічних ключів	335
Розділ 11. Методи та пристрої забезпечення інформаційно'	
безпеки	369

11.1. Основні принципи захисту інформації при підключені до мережі Інтернет.....	369
11.2. Захист інформації за допомогою міжмережевих екранів.....	380
11.3. Захист інформації на мережевому рівні.....	383
Розділ 12. Моделі захисту. Захист пам'яті.....	397
12.1. Аналіз умов функціонування та загроз інформації в комп'ютерних системах і мережах.....	397
12.2. Побудова моделі загроз у сучасних КСМ.....	402
12.3. Побудова моделі порушника в сучасних КСМ.....	404
12.4. Організація захисту пам'яті в ПК.....	410
12.5. Засоби захисту пам'яті персонального комп'ютера.....	415
Розділ 13. Використання паролів і механізмів контролю за доступом.....	429
13.1. Формальні моделі доступу. Дискреційний та мандатний доступ до інформації.....	429
13.2. Аналіз захищеності сучасних операційних систем.....	435
13.3. Підсистема захисту в ОС Windows.....	436
13.4. Порівняння архітектури Windows та Linux.....	454
Лабораторний практикум.....	466
Лабораторні роботи базового рівня.....	468
Лабораторна робота № 1.....	469
Лабораторна робота № 2.....	510
Лабораторна робота № 3.....	537
Лабораторна робота № 4.....	548
Лабораторна робота № 5.....	558
Лабораторна робота № 6.....	563
Лабораторна робота № 7.....	569
Лабораторна робота № 8.....	572
Лабораторна робота № 9.....	578
Лабораторна робота № 10.....	584
Лабораторні роботи середнього рівня.....	591
Лабораторна робота №11.....	592
Лабораторна робота №12.....	603
Лабораторна робота №13.....	610
Лабораторна робота №14.....	615
Лабораторна робота №15.....	618

Лабораторна робота №16.....	628
Лабораторна робота №17.....	633
Лабораторна робота №18.....	636
Лабораторна робота №19.....	638
Лабораторні роботи підвищеного рівня.....	641
Лабораторна робота №20.....	642
Лабораторна робота №21	647
Лабораторна робота №22.....	651
Лабораторна робота №23.....	654
Лабораторна робота №24.....	664
Лабораторна робота №25.....	669
Список використаної літератури.....	673