МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Остапов С. Е.
Євсеєв С. П.
Король О. Г.

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Остапов С. Е.
Євсеєв С. П.
Король О. Г.

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник

Харків. Вид. ХНЕУ, 2013

УДК 004.056.5(076.5)
ББК 32.973я73
О-76

Рецензенти: докт. техн. наук, професор, зав. кафедри захисту інформації Національного університету “Львівська політехніка" *Дудикевич В. Б.;* докт. техн. наук, професор, зав, кафедри системного програмування Хмельницького національного університету *Поморова* О. *В.;* докт. техн. наук, проректор з наукової роботи та міжнародних зв’язків ПВНЗ “Буковинський університет’’ *Виклюк Я. І.*

Рекомендовано до видання рішенням вченої ради Харківського національного економічного університету.

Протокол № 6 від 21.01.2013 р.

Авторський колектив: докт. фіз.-мат. наук, професор Остапов С. Е. - вступ, розділи 1 - 3, 8, 9; канд. техн. наук, ст. наук, співробітник Євсеєв С. П. - розділи 4, 5, 7,10; викладач Король О. Г. - розділи 6, 11-13.

Остапов С. Е.

О-76 Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)

Розглянуто основи, сучасного захисту інформації в комп’ютерних системах, не пов'язаних із державною таємницею. Викладено основні поняття та визначення захисту інформації, формування політики безпеки, критерії оцінки захищеності комп’ютерних систем, основи криптографічного захисту інформації, захисту інформації від несанкціонованого доступу в сучасних операційних системах, а також описано комплексні системи захисту в корпоративних інформаційних системах.

Рекомендовано для студентів, які навчаються за напрямами "Комп’ютерна інженерія", "Програмна інженерія", “Інформатика" та “Комп’ютерні науки" всіх форм навчання, для студентів інших спеціальностей, де вивчається цикл навчальних дисциплін із захисту інформації, а також для самостійного опанування його основ.

ISBN 978-966-676-500-3

УДК 004.056.5(076.5)
ББК 32.973Я73

Зміст

Вступ 3
Розділ 1. Огляд безпеки системи 5
1.1. Основні поняття 5
1.2. Захист інформації та його основні завдання 6
1.2.1. Класифікація загроз для інформації та їх джерел 8
1.2.2. Основні задачі, які повинні вирішуватися системою комп'ютерної безпеки 11
1.2.3. Класифікація основних засобів протидії загрозам безпеки 11
1.3. Поняття про інформацію з обмеженим доступом. 12
1.4 Структура політики безпеки та її основні частини 14
1.5. Життєвий цикл розробки систем безпеки 18
1.5.1. Розробка профілю захисту і проекту безпеки об'єкта оцінки 18
1.5.2. Порядок розробки профілю захисту і проекту забезпечення безпеки 20
1.5.3. Структура і зміст профілю захисту 25
Контрольні запитання 27
Розділ 2. Механізми і політики розмежування прав доступу 28
2.1. TCSEC ("Оранжева книга") - перший стандарт у галузі оцінки захищеності комп'ютерних систем 28
2.1.1. Основні поняття Оранжевої книги 29
2.2. Common Criteria ("Загальні критерії") - європейський стандарт у галузі оцінки захищеності комп'ютерних систем 31
2.2.1. Функціональні вимоги безпеки 32
2.2.2. Вимоги довіри (гарантія безпеки) 35
2.2.3. Рівні оцінки довіри "Загальних критеріїв" 39
2.3. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу 41
Контрольні запитання 44
Розділ 3. Шифрування даних 45
3.1. Основні поняття роботи К. Шеннона "Теорія зв'язку в секретних системах" 46

3.2. Симетричні, асиметричні та комбіновані криптосистеми. їх переваги та недоліки 51
3.2.1. Симетричні криптосистеми 51
3.2.2. Асиметричні криптосистеми 55
3.3. Основні вимоги до сучасних криптосистем 58
3.4. Сітка Х.Фейстеля, її переваги та недоліки 63
3.5. Класифікація сучасних криптосистем та основні вимоги до них 65
3.6. Математичні основи асиметричної криптографії 70
Контрольні запитання 73
Розділ 4. Алгоритми з секретним ключем 74
4.1. DES (Data Encryption Standard) - стандарт шифрування даних США 1977 року 74
4.1.1. Принципи розробки 74
4.1.2. Шифрування. Початкова перстановка 76
4.1.3. Послідовність перетворень окремого раунду 77
4.1.4. Операція розгортання ключа 79
4.1.5. Операція розшифрування 81
4.1.6. Переваги та недоліки DES 82
4.2. Основні модифікації DES (3DES, DESX) 83
4.2.1. Потрійний DES 84
4.2.2. Алгоритм DESX 85
4.3. Алгоритм криптографічного перетворення ГОСТ 28147-89 86
4.4. Алгоритм Rijndael 89
4.5. Інші відомі блокові шифри 97
4.5.1. Алгоритм RC2 97
4.5.2. Алгоритм RC5 97
4.5.3. Алгоритм IDEA 98
4.5.4. Алгоритм SAFER 107
4.5.5. Алгоритм FEAL 107
4.5.6. Алгоритм Blowfish 107
4.6. Огляд алгоритмів українського конкурсу на сертифікований симетричний криптоалгоритм 109
4.6.1. Алгоритм RSB-32 110
4.6.2. Алгоритм "Мухомор" 115
4.6.3. Алгоритм ADE 119

4.6.4. Алгоритм "Калина" 121
4.6.5. Алгоритм "Лабіринт" 123
4.7. Основні режими роботи DES (ECB, CBC, CFB, OFB, режим генерування імітовставки) 126
4.7.1. Шифрування в режимі Electronic Code Book, ECB 126
4.7.2. Шифрування в режимі Cipher Block Changing, CBC 128
4.7.3. Шифрування в режимі Electronic Feedback, CFB 131
4.7.4. Шифрування в режимі Output Feedback, OFB 136
4.7.5. Шифрування в режимах удосконаленого OFB і PCBC 139
4.8. Сучасні потокові шифри, їх переваги та недоліки 139
4.8.1. Регістри зсуву зі зворотним зв'язком 140
4.8.2. Алгоритм A5 143
4.8.3. RC4 143
4.8.4. SEAL 144
Контрольні запитання 145
Розділ 5. Алгоритми з відкритим ключем 146
5.1. Алгоритм RSA, його криптостійкість та швидкість роботи 146
5.1.1. Безпека та швидкодія RSA 149
5.2. Алгоритм Ель-Гамаля, його безпека та криптостійкість 153
5.2.1. Криптостійкість системи Ель-Гамаля 154
Контрольні запитання 155
Розділ 6. Протоколи автентифікації 156
6.1. Поняття про гешувальні алгоритми, їх призначення, вимоги до них 156
6.1.1. Колізійно-стійкі функції гешування Whirpool та SHA-256, SHA-384, SHA-512 176
6.2. Алгоритми сімейства MD 204
6.3. Алгоритми SHA-1, SHA-2 215
6.4. Огляд алгоритмів гешування конкурсу SHA-3 219
Контрольні запитання 235
Розділ 7. Цифрові підписи 236
7.1. Поняття про цифровий підпис (на прикладі RSA), вимоги до нього 236
7.2. Основні алгоритми електронного цифрового підпису 238
7.3. DSA 265
7.4. Стандарти ЕЦП ГОСТ Р 34.10 та ГОСТ Р 34.10-2001 267

7.5. Український алгоритм ЕЦП ДСТУ 4145 270
Контрольні запитання 283
Розділ 8. Основні види атак, принципи криптоаналізу 284
8.1. Класифікація атак на симетричні криптоалгоритми 285
8.2. Класифікація атак на асиметричні криптоалгоритми 287
8.3. Диференціальний криптоаналіз 290
8.4. Лінійний криптоаналіз 293
Контрольні запитання 294
Розділ 9. Основні напрями розвитку сучасної криптографії 295
9.1. Нові асиметричні алгоритми на основі еліптичних кривих 295
9.1.1. Еліптичні криві 295
9.2. Математичні моделі нелінійних вузлів замін у термінах булевої алгебри 300
9.3. Проблеми генерування випадкових та псевдовипадкових послідовностей 308
9.3.1. Вимоги до генераторів випадкових та псевдовипадкових послідовностей 308
9.3.2. Криптографічно стійкі генератори псевдовипадкових послідовностей 312
Контрольні запитання 314
Розділ 10. Механізми та протоколи керування ключами в (PKI) інформаційної системи 315
10.1. Основні положення керування ключами. Життєвий цикл криптографічного ключа 315
10.2. Керування ключами на основі симетричних методів 332
10.3. Керування ключами на основі асиметричних методів 336
10.4. Безпека керування ключами 339
10.5. Структура та призначення PKI 341
10.5.1. Структура 341
10.5.2. Компоненти і сервіси інфраструктури відкритих ключів 342
10.5.3. Сервіси PKI 345
10.5.4. Архітектура і топологія PKI 348
10.5.5. Стандарти і специфікації PKI 357
10.5.6. Управління сертифікатами 360
Контрольні запитання 371

Розділ 11. Методи та пристрої забезпечення захисту і безпеки 372
11.1. Основні принципи захисту інформації при підключені до мережі Інтернет 372
11.2. Захист інформації за допомогою міжмережних екранів 383
11.3. Захист інформації на мережному рівні 385
11.3.1. Протокол IPSec 385
11.3.1.1. Забезпечення цілісності та автентичності даних в IP-мережах з використанням протоколу AH (IPSec) 391
11.3.1.2. Забезпечення конфіденційності, цілісності та автентичності даних у IP-мережах з використанням протоколу ESP (IPSec) 393
11.3.1.3. Застосування протоколів AH і ESP в транспортному і тунельний режимах 394
11.3.2. Протокол SSL 397
11.3.3. Протокол TLS 398
Контрольні запитання 398
Розділ 12. Моделі захисту. Захист пам’яті 399
12.1. Аналіз умов функціонування та загроз інформації в комп’ютерних системах та мережах 399
12.2. Побудова моделі загроз у сучасних комп’ютерних мережах та системах 404
12.3. Побудова моделі порушника у сучасних сучасних комп'ютерних мережах та системах 407
12.4. Організація захисту пам’яті в ПК 413
12.4.1. Організація захисту пам’яті в ЕОМ 414
12.5. Засоби захисту памяті в персональній ЕОМ 418
Контрольні запитання 432
Розділ 13. Використання паролів і механізмів контролю за доступом 433
13.1. Формальні моделі доступу. Дискреційний та мандатний доступ до інформації 433
13.1.1. Дискреційна модель доступу 434
13.1.2. Мандатна модель доступу 435
13.2. Аналіз захищеності сучасних операційних систем 439
13.3. Підсистема захисту в ОС Windows 440
13.4. Порівняння архітектури Windows та Linux 456
Контрольні запитання 466
Використана література 467