004.056.5
Є25

Євсеєв С. П.
Йохов О. Ю.
Король О. Г.

ГЕШУВАННЯ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

монографія

Євсеєв С. П.
Йохов О. Ю.
Король О. Г.

ГЕШУВАННЯ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Монографія

Харків. Вид. ХНЕУ, 2013

УДК 004.631.54
ББК 32,973
Є25

Рецензенти: докт. техн. наук, професор кафедри безпеки інформаційних технологій Національного авіаційного університету *Хорошко В.* О., докт. техн. наук, професор, головний науковий співробітник Науково-дослідного центру службово-бойової діяльності Академії внутрішніх військ МВС України *Морозов О. О.*

Рекомендовано до видання рішенням вченої ради Харківського національного економічного університету.
Протокол № 6 від 21.01.2013 р.

Авторський колектив: канд. техн. наук, ст. наук, співробітник Євсеєв С. П. - розділи 1, 3, 5; канд. техн. наук, ст. наук, співробітник Йохов О Ю. - вступ, п 4.1, п. 4.2; викладач Король О Г. - розділ 2, п. 4.3, п. 4,4.

Євсеєв С. П.
Є25 Гешування даних в інформаційних системах : монографія / С. П. Євсеєв, О. Ю. Йохов, О. Г. Король. – Х. : Вид. ХНЕУ. 2013 – 312 с. (Укр. мов.)

Викладено загальні поняття та положення в галузі захисту інформації щодо механізмів забезпечення автентичності даних і цифрового підпису. Досліджено методи формування геш-функцій на основі безключових та ключових геш-функцій і використання універсальних класів. Розглянуто результати міжнародних криптографічних конкурсів у сфері гешування. Розкрито теоретичні основи й методи побудови кодів автентичності повідомлень для,забезпечення автентичності та цілісності даних в інформаційних системах.

Рекомендовано для викладачів, наукових та інженерно-технічних співробітників у галузі захисту інформації та інформаційних систем, а також для ад'юнктів, аспірантів і студентів старших курсів відповідних спеціальностей.

ISBN 978-966-676-629-1

УДК 004.631.54
ББК 32,973

© Євсеєв С. П.
Йохов О. Ю.
Король О. Г.
2013

Зміст

Вступ..... 3
Розділ 1. Загальні поняття та положення у галузі захисту інформації.. 5
1.1. Основні терміни та визначення галузі захисту інформації..... 5
1 2 Сучасні загрози безпеки..... 14
1.3. Послуги та механізми захисту інформації (ISO 7498, ISO/IEC 10181) 21
Розділ 2. Механізми забезпечення цілісності та автентичності інформації 32
2.1. Електронний цифровий підпис..... 32
2.2. Коди автентифікації повідомлень..... 76
2.3. Коди детектування маніпуляцій..... 84
Розділ 3. Функції гешування інформації..... 88
3.1. Визначення та загальні вимоги до функцій гешування..... 88
3.2. Ітеративні геш-функції..... 92
3.3 Безкпючове гешування..... 95
3.3.1. На основі блокових шифрів..... 97
3.3.2. На основі модулярної арифметики..... 110
3.3.3. Спеціалізовані геш-функції..... 117
3.4. Ключове гешування..... 138
3.4.1. На основі блочних шифрів..... 141
3.4.2. На основі безкпючових геш-функцій..... 173
Розділ 4. Універсальне гешування..... 194
4.1. Визначення та загальні властивості універсального гешування 194
4.2. Універсальне гешування на основі лінійно-блокових кодів..... 203
4.3. Універсальне гешування на основі модулярних перетворень..... 216
4.4. Каскадні схеми універсального гешування..... 228
Розділ 5. Результати міжнародних криптографічних конкурсів
у галузі гешування..... 252
5.1. Результати конкурсу NESSIE в галузі гешування інформації..... 252
5.1.1 Колізійно-стійкі функції гешування Whirpool та SHA-256,
SHA-384, SHA-512..... 258
5.1.2 Коди автентифікації повідомлень UMAC, TTMAC, EMAC, HMAC..... 263
5.2. Результати конкурсу SHA-3..... 274
5.2.1. BLAKE (Jean-PhilippeAumasson)..... 277
5.2.2. Grostl (LarsRamkildKnudsen)..... 282
5.2.3. JH (HongjunWu)..... 289
5.2.4. Keccak (JoanDaemen)..... 289
5.2.5 Skein..... 290
Висновки..... 300
Використана література..... 301