

В. Ю. Ковтун, С. П. Євсєєв, І. В. Аксьонова

004.056.5
К 56

КІБЕРБЕЗПЕКА ТА НОВІТНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник



Видавництво ПП «Новий Світ-2000»



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

В. Ю. Ковтун, С. П. Євсєєв, І. В. Аксьонова

**КІБЕРБЕЗПЕКА ТА
НОВІТНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ**

Навчальний посібник
для бакалаврів і магістрів
спеціальностей 125 «Кібербезпека та захист інформації»,
256 «Національна безпека (за окремими сферами забезпечення і видами
діяльності)», 257 «Управління інформаційною безпекою»
денної та заочної форм навчання

Рекомендовано Вченою радою НТУ «ХПІ»

Харків – НТУ «ХПІ»
Львів – Видавництво ПП «Новий Світ – 2000»
2024

УДК 004.056.5(075) + 004.421.5(075)
К 56

Рецензенти:

*І. Р. Опірський, д.т.н., проф., завідувач кафедри захисту інформації
Національного університету «Львівська політехніка»;*

*К. В. Молодецька, д.т.н., проф. кафедри менеджменту організацій
Києво-Могилянської бізнес школи, Національний університет
«Києво- Могилянська академія».*

*Рекомендовано Вченою радою НТУ «ХПІ» як навчальний посібник для
бакалаврів і магістрів спеціальностей 125 «Кібербезпека та захист
інформації», 256 «Національна безпека (за окремими сферами
забезпечення і видами діяльності)», 257 «Управління інформаційною
безпекою» денної та заочної форм навчання,
протокол № 9 від 29.11.2024 року*

Ковтун В. Ю., Євсєєв С. П., Аксьонова І. В.

К 56 Кібербезпека та новітні технології захисту інформації :
навчальний посібник / В. Ю. Ковтун, С. П. Євсєєв, І. В. Аксьонова. –
Харків, – Львів : «Новий Світ – 2000», 2024. – 285 с.

ISBN 978-966-418-505-6

Розглянуто теоретичні основи інформаційної безпеки, криптографії та криптоаналізу. Представлено базовий функціонал аналізу випадкових та псевдовипадкових послідовностей. Також розглянуті поняття симетричного та асиметричного криптоаналізу на підставі блокових та поточкових шифрів. Наведено принципи криптоперетворення в групах точок еліптичних кривих, описано криптоаналіз хеш-функцій. Розглянуто задачі факторизації та дискретного логарифмування. Наведено лабораторний практикум, який містить лабораторні роботи з методичними рекомендаціями до їх виконання.

Призначено для студентів вищих навчальних закладів III-IV рівня акредитації, які навчаються за спеціальностями 125 - «Кібербезпека та захист інформації», 256 - «Національна безпека (за окремими сферами забезпечення і видами діяльності)» та 257 - «Управління інформаційною безпекою» денної та заочної форм навчання, які вивчають дисципліну «Основи криптографічного захисту», а також всім, хто цікавиться питаннями безпеки та захисту інформації.

Іл. 46. Табл. 21. Бібліогр. 32 назв.

УДК 004.056.5(075) + 004.421.5(075)

© Ковтун В. Ю., Євсєєв С. П., Аксьонова І. В., 2024
© Національний технічний університет
«Харківський політехнічний інститут», 2024
© Видавництво ПП «Новий Світ - 2000»,
ФООП ПічаС. В., 2024

ISBN 978-966-418-505-6

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1.ОСНОВИ ТЕОРІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....	5
1.1. Розвідка та канали поширення інформації.....	5
1.2. Канали несанкціонованого отримання інформації.....	9
1.3.Захист даних: основні поняття та визначення.....	13
1.4. Вступ до криптографії та криптоаналізу.....	19
Контрольні запитання до розділу.....	25
РОЗДІЛ 2. ВИПАДКОВІ ТА ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ.....	27
2.1. Випадкові числа. Генератори випадкових чисел та псевдовипадкових послідовностей.....	27
2.2. Криптографічно надійні датчики випадкових чисел. Методи отримання справжніх випадкових чисел.....	36
2.3. Статистичні тести.....	45
Контрольні запитання до розділу.....	50
РОЗДІЛ 3. СИМЕТРИЧНІ КРИПТОСИСТЕМИ БЛОКЧЕЙНУ: AES	52
3.1. Характеристика симетричних криптосистем.....	52
3.2. Опис симетричної криптосистеми блокчейн AES	57
3.2.1. Шифрування та дешифрування.....	59
3.2.2. Особливості реалізації стандарту шифрування AES.....	64
Контрольні запитання до розділу.....	75
РОЗДІЛ 4. СИМЕТРИЧНІ БЛОКОВІ КРИПТОСИСТЕМИ: ГОСТ 28147-8977	
4.1. Опис симетричної блокової криптосистеми ГОСТ 28147-89.....	77
4.2. Логіка побудови шифру і структура ключової інформації ГОСТ.....	79
4.3. Обговорення криптографічних алгоритмів ГОСТ.....	95
Контрольні запитання до розділу.....	100
РОЗДІЛ 5. СИМЕТРИЧНІ КРИПТОСИСТЕМИ: ПОТОКОВІ ШИФРИ	101
5.1. Криптосистеми з симетричним потоком.....	101
5.2. Інші режими блокового шифру.....	112
5.3. Показники потокового шифру.....	115
Контрольні запитання до розділу.....	123
РОЗДІЛ 6. ВВЕДЕННЯ ДО КРИПТОАНАЛІЗУ. КРИПТОАНАЛІЗ СИМЕТРИЧНИХ КРИПТОСИСТЕМ: БЛОКОВІ ШИФРИ.....	125
6.1. Основні поняття криптоаналізу.....	125
6.2. Універсальні методи криптоаналізу.....	131
6.3. Методи криптоаналізу симетричних криптосистем.....	140
Контрольні запитання до розділу.....	150
РОЗДІЛ 7. КРИПТОАНАЛІЗ СИМЕТРИЧНИХ КРИПТОСИСТЕМ: ПОТОКОВІ ШИФРИ. КРИПТОАНАЛІЗ ЧЕРЕЗ ПОБІЧНІ КАНАЛИ.....	152
7.1. Методи криптоаналізу поточкових шифрів.....	152
7.2. Криптоаналіз на сторонньому каналі	157
7.3. Використання нових технологій у криптоаналізі.....	161
Контрольні запитання до розділу.....	169
РОЗДІЛ 8. АСИМЕТРИЧНІ КРИПТОСИСТЕМИ.....	170

8.1. Вступ в асиметричні криптосистем».....	170
8.2. Криптосистема RSA.....	175
8.3. Криптосистема Ель-Гамала.....	178
8.4. Односпрямовані хеш-функції.....	179
Контрольні запитання до розділу.....	189
РОЗДІЛ 9. КРИПТОПЕРЕТВОРЕННЯ В ГРУПАХ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ.....	190
9.1. Групи та скінченні поля.....	190
9.2. Еліптична крива. Криптографія з еліптичною кривою.....	194
9.3. Метрики операцій на еліптичній кривій	196
9.4. Афінні та проективні основи.....	199
Контрольні запитання до розділу.....	205
РОЗДІЛ 10. КРИПТОАНАЛІЗ АСИМЕТРИЧНИХ КРИПТОСИСТЕМ.....	206
10.1. Криптоаналіз хеш-функцій.....	206
10.2. Метод «зустріч посередині». Розв’язання задачі факторизації.....	209
10.3. Розв’язання задачі дискретного логарифма.....	214
Контрольні запитання до розділу.....	220
ЛАБОРАТОРНИЙ ПРАКТИКУМ.....	222
РЕКОМЕНДОВАНА ЛІТЕРАТУРА.....	267
ДОДАТКИ.....	270