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

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. Євсеєв, 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., Євсеєв С. П., Аксьонова І. В.

К 56 **Кібербезпека та новітні технології захисту інформації :** навчальний посібник / В. Ю. Ковтун, С. П. Євсеєв, 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 потокових 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)

ISBN 978-966-418-505-6

ЗМІСТ