ПЕРЕДМОВА

Інтенсивний розвиток методів прикладної криптології привів до створення широкого спектра систем та засобів криптографічного захисту інформації та інформаційних ресурсів, які ґрунтуються на теорії чисел, методах алгебри, проективної геометрії та дискретної математики.

Курс “Спеціальні розділи математики” – складова частина математики, в якій вивчають математичні засоби дослідження дискретних процесів і систем.

Навчальний посібник підготовлено на підставі лекцій та практичних занять із дисципліни “Спеціальні розділи математики”, яку викладають студенти Львівської політехніки.

Мета видання – ознайомити читача з основними поняттями та моделями теорії чисел, алгебри, полів Галуа та групових операцій на еліптичних кривих.

Зміст посібника, який обмежено такими основними темами дисципліни як базові поняття теорії чисел, алгебраїчні структури, конгруенції, поля Галуа, групові операції на еліптичних кривих, відповідає типовій програмі півріччного курсу освітньо-кваліфікаційного рівня бакалавра галузі знань “Інформаційні технології”, спеціальності “Кібербезпека” та спеціалізації “Безпека інформаційних та комунікаційних систем”.

Навчальний посібник складається із шести розділів, які умовно поділені на три частини.

Перша частина посібника (розділи 1–4) містить теоретичний матеріал із названих тем і є вступною для спеціальних дисциплін.

У другій частині (розділ 5) подано методи розв’язування типових прикладів із тем, розглянутих у першій частині. Ця частина є допоміжною для самостійного розв’язування задач з індивідуальних завдань, які містяться у третій частині посібника (розділ 6).

Розділ 6 містить 12 комплексних завдань для самостійного виконання студентами та необхідні пояснення до них.

Матеріал посібника викладено на доступному рівні для випускника середньої школи.

Посібник може бути використано як теоретичний довідник для розв’язування задач із розглянутих тем та як збірник задач для виконання індивідуальних завдань.