ВСТУП

У цьому навчальному посібнику наведено матеріал, який є базовим для подальшого вивчення дисциплін, що пов'язані з криптографічним захистом інформації, секретними системами, захистом комп'ютерних систем та мереж, забезпеченням безпечного передавання інформації тощо.

Перший розділ містить описання основ теорії секретних систем, які вперше сформулював Клод Шеннон. Наведено математичну структуру секретних систем, зокрема способи зображення та приклади таких систем. Розглянуто основні шифри докомп'ютерного періоду, а також параметри, що використовуються для визначення теоретичної секретності. Особливу увагу приділено різним способам забезпечення практичної секретності в криптографічних системах.

У другому розділі розглянуто криптографічні протоколи, зокрема протоколи передавання інформації, цифрових підписів, встановлення достовірності, обміну ключами за допомогою симетричної криптографії та криптографії з відкритими ключами. Також наведено проміжні, розвинені та езотеричні протоколи, які використовуються в криптографії.

Наприкінці кожного розділу подано питання, за допомогою яких студенти зможуть перевіряти свої знання.