

ЗМІСТ

ПЕРЕДМОВА	6
ЛЕКЦІЙНИЙ МАТЕРІАЛ	8
Традиційна і електронна комерція	8
Типи електронної комерції	12
B2B-комерція	12
B2C-комерція	12
C2C-комерція	13
P2P-комерція	13
Платіжна система	14
Інтернет-банкінг	17
Безпека електронної комерції	19
Анонімність платежів	19
Аутентифікація учасників інформаційного обміну	20
Забезпечення конфіденційності та цілісності інформації	21
Забезпечення доступності сервісів у режимі 24/7	21
Забезпечення неможливості відмови від укладених документів	21
Загрози з боку покупця	25
Загрози з боку продавця	27
Структура внутрішньоплатіжної системи комерційного банку	32
B2B-комерція. Системи електронного обміну даними	36
Система EDIFACT	39
Безпека ЕОД-систем	43
First Virtual: безпека без шифрування	46
Захищені протоколи	49
Протоколи iKP	49
Протокол SSL/TLS	52
Протокол SET	62
Архітектура SET	64
Технологія OAEP	68
Метод подвійного підпису	70
Повідомлення SET	72
Переваги і недоліки SET. Порівняння з TLS	73
Безпека банківських платіжних карток	76
З історії карток	76
Код Луна	79
Структура магнітної смужки	80

Смарт-карти	84
Карткові операційні системи.....	89
Атаки на смарт-карти.....	89
Електронні підписи та інфраструктури.....	95
Стандартизація та сертифікація в галузі інформаційної безпеки	95
Цифровий підпис	104
MDC-коди	136
MAC-коди	150
Удосконалений алгоритм UMAC	154
Поняття про криптовалюти	201
Алгоритм ЕЦП на еліптичних кривих	202
Електронний цифровий підпис ECDSA.....	204
Функція хешування SHA-2.....	205
Організація транзакцій в BitCoin.....	207
Поняття про Blockchain.....	210
Поняття про майнінг	215
ЛАБОРАТОРНИЙ ПРАКТИКУМ.....	218
Лабораторна робота № 1. Вивчення системи захисту інформації GnuPG та Kleopatra.....	218
Теоретична частина.....	218
Практична частина.	226
Контрольні запитання та завдання	226
Лабораторна робота № 2. Вивчення системи захисту даних VeraCrypt 1.24.	227
Теоретична частина.....	227
Практична частина	232
Контрольні запитання та завдання	233
Лабораторна робота № 3. Дослідження захисту інформації у спрощених EDI-системах.....	234
Теоретична частина.....	234
Практична частина	238
Контрольні запитання та завдання	239
Лабораторна робота № 4. Розробка системи «Банкоматик».....	240
Теоретична частина.....	240
Практична частина	245
Контрольні запитання та завдання	247

Лабораторна робота № 5. Використання електронних гаманців у системах електронної торгівлі	249
Теоретична частина.....	249
Практична частина	250
Контрольні запитання та завдання	254
Лабораторна робота № 6. Вивчення захисту повідомлень у протоколі SET	255
Теоретична частина.....	255
Практична частина	259
Контрольні запитання та завдання	259
Лабораторна робота № 7. Розробка навчальної криптовалюти. Генерування користувачів та транзакцій.....	260
Теоретична частина.....	260
Практична частина	262
Контрольні запитання та завдання	262
Лабораторна робота № 8. Розробка навчальної криптовалюти. Майнінг.....	264
Теоретичні відомості.....	264
Практична частина	265
Контрольні запитання та завдання	266
Список використаної літератури	267
Додатки.....	272