

ЗМІСТ

Передмова.....	3
Розділ 1. Вступ. Основні поняття безпеки. Конфіденційність, цілісність та доступність даних. Класифікація загроз. Сервіси та механізми захисту....	5
1.1. Основні поняття безпеки даних	7
1.2. Порушення, механізми і служби захисту.....	9
Контрольні запитання	17
Розділ 2. Традиційне шифрування. Модель традиційного шифрування. Криптографія і криптоаналіз. Класична техніка шифрування: підстановки і перестановки	18
2.1. Традиційне шифрування. Модель традиційного шифрування	18
2.2. Криптографія і криптоаналіз.....	21
2.3. Стеганографія.....	28
2.4. Підстановочні і перестановочні шифри.....	28
2.5. Просте XOR.....	34
2.6. Одноразові блокноти	36
2.7. Комп'ютерні алгоритми	39
Контрольні запитання	39
Розділ 3. Потокові і блокові шифри. Дифузія і конфузія. Шифр Файстеля. Диференційний та лінійний криптоаналіз. Принципи побудови блокових шифрів	40
3.1. Потокові та блокові шифри.....	40
3.2. Шифр Файстеля.....	43
3.3. Дифузія і конфузія	44
3.4. Структура шифру Файстеля.....	45
3.5. Диференційний та лінійний криптоаналіз	51
3.6. Принципи побудови блокових шифрів	52
Контрольні запитання	54
Розділ 4. Стандарт шифрування даних (DES). Критерії, що їх покладено в основу конструкції DES. Алгоритми “Подвійний” та “Потрійний” DES.....	55
4.1. Стандарт шифрування даних (DES).....	55
4.2. Шифрування DES.....	57
4.3. Дешифрування DES.....	64
4.4. “Подвійний” DES	70
4.5. “Потрійний” DES із двома ключами	72
4.6. “Потрійний” DES із трьома ключами.....	72
Контрольні запитання	73
Розділ 5. Режими роботи блокових шифрів. Проблема та схеми розподілу ключів симетричного шифрування.....	74

5.1. Режим електронної шифрувальної книги	74
5.2. Режим зчеплення шифрованих блоків	77
5.3. Режим шифрованого зворотного зв'язку	79
5.4. Режим зворотного зв'язку по виходу	81
5.5. Розподіл ключів.....	82
Контрольні запитання	94
Розділ 6. Генерування випадкових чисел. Використання та джерела	
випадкових чисел. Генератори псевдовипадкових чисел.....	95
6.1. Генерування випадкових чисел	95
6.2. Генератори псевдовипадкових чисел	97
Контрольні запитання	104
Розділ 7. Криптографія з відкритим ключем.	
Принципи побудови криптосистем з відкритим ключем	105
7.1. Принципи побудови криптосистем з відкритим ключем	106
7.2. Застосування криптосистем з відкритим ключем	113
Контрольні запитання	117
Розділ 8. Алгоритм RSA	
8.1. Опис алгоритму.....	118
8.2. Шифрування й дешифрування.....	121
8.3. Захищеність алгоритму RSA.....	125
Контрольні запитання	130
Розділ 9. Порівняння основних характеристик симетричних	
та асиметричних алгоритмів.....	131
9.1. Дослідження характеристик криптостійкості алгоритму	
симетричного шифрування DES	131
9.2. Дослідження основних характеристик алгоритму	
симетричного шифрування RC5.....	138
9.3. Порівняння швидкодії програмної реалізації алгоритмів	
симетричного (DES) та асиметричного (RSA) шифрування.....	146
Контрольні запитання	150
Розділ 10. Управління ключами і схема Діффі–Хеллмана	
10.1. Управління ключами	151
10.2. Розподіл секретних ключів за допомогою системи	
з відкритим ключем	157
10.3. Обмін ключами за схемою Діффі-Хеллмана	161
Контрольні запитання	165
Розділ 11. Аутентифікація повідомлень і функції хешування.	
Вимоги та функції аутентифікації.....	166
11.1. Вимоги аутентифікації.....	166

11.2. Функції аутентифікації.....	167
11.3. Код автентичності повідомлення.....	174
Контрольні запитання	181
Розділ 12. Коди автентичності повідомлень та функції хешування	182
12.1. Коди автентичності повідомлень.....	182
12.2. Функції хешування	186
12.3. Захист функцій хешування і кодів автентичності повідомлень	192
Контрольні запитання	193
Розділ 13. Алгоритми хешування. Алгоритм HMAC.....	194
13.1. HMAC.....	194
Контрольні запитання	200
Розділ 14. Цифрові підписи та протоколи аутентифікації. Вимоги до цифрового підпису. Стандарт цифрового підпису DSS	201
14.1. Цифрові підписи.....	201
14.2. Стандарт цифрового підпису DSS	206
Контрольні запитання	209
Розділ 15. Протоколи аутентифікації. Взаємна та одностороння аутентифікація	210
15.1. Взаємна аутентифікація.....	210
15.2. Одностороння аутентифікація	219
Контрольні запитання	221
Розділ 16. Програмна реалізація криптографічних алгоритмів. Використання криптографічних функцій Microsoft CryptoAPI в прикладному ПЗ	222
16.1. Будова і можливості Crypto API	222
16.2. Криптопровайдери	225
16.3. Контейнери ключів	229
16.4. Алгоритми	231
16.5. Сертифікати	232
16.6. Базові функції	232
Контрольні запитання	238
Розділ 17. Методи та засоби створення захищеного програмного забезпечення. Поняття про безпечний цикл розробки ПЗ (SDL).....	239
17.1. Поняття аудиту безпеки програмного коду	239
17.2. Поняття про безпечний цикл розробки ПЗ Microsoft (SDL)	246
Контрольні запитання	248
Список літератури.....	249
Алфавітний покажчик	251