

ЗМІСТ

Зміст	3
Передмова	9
Розділ 1. Основні поняття та визначення в галузі інформаційної безпеки	11
1.1. Державна політика України в галузі інформаційної безпеки	11
1.1.1. Інформаційна безпека та її місце в системі національної безпеки України	11
1.1.2. Державна політика інформаційної безпеки та її здійснення в законодавстві України.....	15
1.1.3. Органи забезпечення інформаційної безпеки та захисту інформації	17
1.2. Інформація як об'єкт захисту	19
1.2.1. Поняття інформації та її властивості.....	19
1.2.2. Загрози інформації.....	24
1.2.3. Модель порушника	27
1.2.4. Підготовчі дії порушника перед несанкціонованим доступом до інформації.....	31
1.2.5. Методи та види несанкціонованого доступу. Методи захисту від несанкціонованого доступу	33
Контрольні питання до розділу 1	38
Список літератури до розділу 1	39
Розділ 2. Математичні основи криптології	40
2.1. Елементи теорії множин	40
2.1.1. Відображення	40
2.1.2. Основні поняття і визначення	42
2.2. Елементи теорії чисел.....	48
2.2.1. Ділення з остачею.....	48
2.2.2. Найбільший спільний дільник і взаємно прості числа	49
2.2.3. Прості числа	50
2.2.4. Алгоритм Евкліда.....	51
2.2.5. Лінійні діофантові рівняння з двома невідомими.....	52
2.2.6. Основна теорема арифметики	54
2.3. Теорія порівнянь	55
2.3.1. Означення й найпростіші властивості	56
2.3.2. Повна та зведена системи лишків	58
2.3.3. Теорема Ейлера	60
2.3.4. Мала теорема Ферма	61
2.3.5. Порівняння першого степеня	63
2.3.6. Китайська теорема про лишки	66
2.3.7. Порівняння другого степеня. Символ Лежандра.....	68
2.3.8. Алгоритми перевіряння чисел на простоту	71
2.3.9. Порівняння будь-якого степеня за простим модулем.....	74
2.3.10. Порівняння будь-якого степеня за складним модулем	76
2.4. Алгоритми та їхня складність.....	80
2.4.1. Задачі й алгоритми	81
2.4.2. Асимптотичні позначення.....	84

2.4.3. Рандомізація, імовірнісні алгоритми.....	87
2.4.4. Односторонні функції.....	90
2.4.5. Функції з секретом.....	93
2.5. Алгоритми виконання операцій із довгими числами	95
2.5.1. Розміщення в пам'яті комп'ютера довгих чисел та аналіз типів даних для виконання арифметичних операцій з ними	95
2.5.2. Здійснення алгоритму множення довгого числа на коротке.....	98
2.5.3. Множення довгих чисел із використанням стовпчика.....	99
2.5.4. Алгоритм швидкого множення.....	100
2.5.5. Множення з використанням швидкого перетворення Фур'є	101
2.5.6. Застосування швидкого перетворення Фур'є для обчислення згортки $a \otimes b$	103
2.5.7. Обмеження швидкого перетворення Фур'є множення	104
2.5.8. Використання швидкого перетворення Хартлі для обчислення згортки.....	105
2.5.9. Порівняльна характеристика алгоритмів множення довгих чисел	108
2.6. Елементи теорії еліптичних кривих	109
2.6.1. Способи побудови еліптичних кривих	109
2.6.2. Композиція точок еліптичних кривих	110
2.6.3. Властивості множини точок на еліптичній кривій.....	114
2.6.4. Криптографічні операції на еліптичній кривій.....	115
Контрольні питання до розділу 2	115
Список літератури до розділу 2.....	117
Розділ 3. Криптологія	118
3.1. Історія криптології	118
3.2. Основні поняття та визначення криптології	124
3.3. Класичні криптосистеми та їхній криптоаналіз.....	131
3.3.1. Шифри простої заміни.....	131
3.3.2. Гомофонний шифр заміни	134
3.3.3. Поліграмні шифри	135
3.3.4. Поліалфавітні криптосистеми.....	137
3.3.5. Шифри перестановки.....	140
3.3.6. Кількаразове шифрування	142
3.3.7. Роторні шифрувальні машини	143
3.4. Афінні шифри.....	144
3.5. Поточкові симетричні шифри	147
3.6. Блокові симетричні шифри	155
3.6.1. Методи конструювання сучасних блокових симетричних шифрів	155
3.6.2. Стандарт блокового симетричного шифрування DES.....	158
3.6.3. Шифр ГОСТ 28147-89.....	169
3.6.4. Стандарт блокового симетричного шифрування AES.....	171
3.6.5. Національний стандарт блокового симетричного шифрування ДСТУ 7624:2014	179
3.7. Асиметричні криптосистеми.....	191
3.7.1. Криптосистема на основі телефонного довідника.....	193
3.7.2. Головоломки Меркла	194
3.7.3. Важкооборотні функції	195

3.7.4. Ранцеві криптосистеми	196
3.7.5. Алгоритм RSA	201
3.7.6. Бінарний алгоритм піднесення до степеня	205
3.7.7. Криптосистема Рабіна	207
3.7.8. Система Ель-Гамала	208
3.8. Асиметричні криптосистеми на еліптичних кривих	209
3.9. Альтернативна криптографія	212
3.10. Елементи криптоаналізу	220
3.10.1. Типи розкриття	221
3.10.2. Криптоаналіз класичних алгоритмів	223
3.10.3. Криптоаналіз симетричних шифрів	226
3.10.4. Криптоаналіз асиметричних шифрів	232
3.10.5. Силкові методи криптоаналізу	238
3.10.6. Криптоаналіз за побічними каналами	239
3.10.7. Нові методи криптоаналізу	243
Контрольні питання до розділу 3	247
Список літератури до розділу 3	249
Розділ 4. Стеганографія	251
4.1. Стеганографічні системи	251
4.1.1. Сфери застосування стеганографії	251
4.1.2. Атаки на стеганографічні системи та протидія їм	253
4.1.3. Пропускна здатність каналів приховуваного передавання повідомлень	257
4.1.4. Оцінювання стійкості стеганографічних систем	259
4.2. Методи стеганографії	260
4.2.1. Приховування даних у нерухомих цифрових зображеннях, відеофайлах та аудіофайлах	260
4.2.2. Текстова стеганографія	263
4.2.3. Практичне застосування стеганографії	264
Контрольні питання до розділу 4	271
Список літератури до розділу 4	271
Розділ 5. Ідентифікація. автентифікація. санкціонований доступ	272
5.1. Автентифікація	272
5.1.1. Основні визначення (термінологія)	272
5.1.2. Ідентифікація та автентифікація об'єктів	273
5.1.3. Системи захисту цілісності даних	275
5.1.4. Задачі автентифікації	278
5.2. Класифікація систем автентифікації за ступенем стійкості	279
5.2.1. Поняття безумовно безпечних кодів автентифікації	280
5.3. Криптографічні хеш-функції	284
5.3.1. Алгоритм MD5	285
5.3.2. Алгоритм SHA	291
5.3.3. Алгоритм SHA3	293
5.3.4. Застосування функції хешування в криптографії	296
5.3.5. Хеш-функції, що використовують симетричні блокові алгоритми	297
5.3.6. Хеш-функція ГОСТ	299

5.3.7. Функція хешування “Купина” – національний стандарт України ДСТУ 7564:2014	300
5.3.8. Коды автентифікації повідомлень, що використовують функції хешування із ключем.....	306
5.3.9. SVC-MAC.....	308
5.4. Протоколи автентифікації	308
5.4.1. Автентифікація джерела даних	309
5.4.2. Автентифікація сутності	309
5.4.3. Атаки на протоколи автентифікації	311
5.4.4. Основні протоколи автентифікації	312
5.4.5. Стратегія “виклик – відгук”	312
5.4.6. Мітки часу	314
5.4.7. Взаємна автентифікація.....	315
5.4.8. Автентифікація із залученням довіреного посередника.....	316
5.4.9. Типові атаки на протоколи автентифікації	319
5.4.10. Протокол автентифікації Kerberos	320
Контрольні питання до розділу 5	325
Список літератури до розділу 5.....	325
Розділ 6. Безпека інформаційних систем.....	327
6.1. Захист інформації в каналах електрозв’язку.....	328
6.1.1. Види та принципи побудови каналів електрозв’язку, телекомунікаційних систем та мереж	328
6.1.2. Засоби несанкціонованого доступу до інформації в абонентських телефонних лініях.....	330
6.1.3. Методи виявлення та боротьби із засобами несанкціонованого доступу до інформації в абонентських телефонних лініях у робочому стані	334
6.1.4. Засоби несанкціонованого доступу до інформації, що використовують радіолінії.....	336
6.1.5. Виявлення засобів несанкціонованого доступу до інформації, що використовують радіолінії.....	338
6.1.6. Методи несанкціонованого доступу до інформації та методи боротьби з ним у волоконно-оптичних лініях зв’язку	343
6.2. Інформаційна безпека в мережах коміркового зв’язку	346
6.2.1. Функціональна та просторова структура мереж коміркового зв’язку	346
6.2.2. Захист від несанкціонованого доступу	351
6.2.3. Захист від підслуховування.....	352
6.2.4. Конфіденційність локалізації абонента	353
6.2.5. Особливості забезпечення конфіденційності в мережах CDMA.....	354
6.2.6. Ідентифікація апаратури абонента	355
6.3. Інформаційна безпека комп’ютерних мереж	356
6.3.1. Види комп’ютерних мереж та основи їх функціонування	356
6.3.2. Інциденти інформаційної безпеки.....	360
6.3.3. Принципи організації безпеки комп’ютерних мереж.....	364
6.3.4. Методи та засоби забезпечення вимог політики безпеки комп’ютерної мережі.....	367
6.3.5. Підвищення рівня інформаційної безпеки за допомогою маршрутизаторів	371

6.4. Атаки на інформаційні та програмно-технічні ресурси комп'ютерної мережі.....	373
6.4.1. Види атак	373
6.4.2. Виявлення атак на ресурси комп'ютерної мережі	378
6.5. Захист приватної мережі від зовнішнього втручання	381
6.5.1. Забезпечення доступу користувачів приватної мережі до ресурсів мережі Інтернет	381
6.5.2. Захист інформаційних ресурсів за допомогою міжмережевих екранів та створення DMZ	385
6.6. Особливості забезпечення безпеки корпоративних мереж	390
6.6.1. Особливості будови та захисту корпоративних сховищ даних	390
6.6.2. Забезпечення безпеки в мережах Wi-Fi.....	396
6.7. Основи технології віртуальних приватних мереж	407
6.7.1. Основні поняття й функції мережі VPN.....	407
6.7.2. Варіанти побудови віртуальних захищених каналів	412
6.7.3. Засоби забезпечення безпеки VPN	414
6.7.4. Класифікація мереж VPN	417
6.8. Протоколи захисту інформації на канальному рівні моделі OSI	421
6.8.1. Принцип роботи протоколу PPTP	422
6.8.2. Протоколи L2F і L2TP	425
6.9. Протоколи захисту даних на мережевому рівні моделі OSI	427
6.9.1. Компоненти IPSec	428
6.9.2. Режими та функції протоколів AH і ESP.....	432
6.9.3. Алгоритми автентифікації та шифрування в IPSec	438
6.9.4. Протокол управління криптоключами IKE.....	441
6.9.5. Режими та схеми застосування IPSec	444
6.9.6. Переваги застосування засобів безпеки IPSec.....	447
6.10. Протоколи захисту даних на сеансовому рівні моделі OSI.....	447
6.10.1. Протоколи SSL / TLS	448
6.10.2. Протокол SOCKS	450
6.11. Протоколи захисту даних на прикладному рівні моделі OSI.....	454
6.11.1. Управління ідентифікацією та доступом.....	455
6.11.2. Функціонування системи управління доступом.....	456
Контрольні питання до розділу 6.....	459
Список літератури до розділу 6	461
Розділ 7. Захист програмного забезпечення в інформаційних системах.....	463
7.1. Актуальність	463
7.2. Безпека програмного забезпечення	463
7.3. Життєвий цикл програмного забезпечення	464
7.4. Загрози безпеці програмного забезпечення.....	468
7.4.1. Загальна характеристика	468
7.4.2. Комп'ютерні віруси	469
7.4.3. Алгоритмічні та програмні закладки.....	472
7.5. Захист програмного забезпечення від загроз	473
7.5.1. Експлуатаційна безпека програмного забезпечення	473
7.5.2. Адаптивна безпека інформаційних систем	476
7.5.3. Юридичний та технічний захист програмного забезпечення	484

7.5.4. Захист програмного забезпечення від комп'ютерних вірусів	485
7.5.5. Захист програмного забезпечення від упродовження програмних закладок	488
7.5.6. Захист програмного забезпечення від несанкціонованого копіювання	492
7.5.7. Захист програмного забезпечення від несанкціонованого доступу	493
7.6. Оцінювання рівня безпеки програмного забезпечення	496
Контрольні питання до розділу 7	498
Список літератури до розділу 7	499
Розділ 8. Інформаційна безпека підприємств та організацій.	
Системи інформаційної безпеки	500
8.1. Інформаційна безпека підприємств та організацій	500
8.1.1. Модель багаторівневого захисту інформаційних систем підприємств та організацій	500
8.1.2. Засоби забезпечення інформаційної безпеки підприємств та організацій	503
8.1.3. Правові, організаційні та технологічні засоби захисту інформації	505
8.1.4. Фізичний захист об'єктів підприємств та організацій	506
8.1.5. Апаратні засоби захисту та збереження інформації	510
8.1.6. Програмні засоби захисту інформації	513
8.2. Безпека інформації на об'єктах підприємств та організацій	516
8.2.1. Канали витоку інформації в інформаційних системах підприємств та організацій	516
8.2.2. Забезпечення безпеки інформації на об'єктах підприємств та організацій	521
8.3. Системи інформаційної безпеки	527
8.3.1. Система охоронної сигналізації	528
8.3.2. Система пожежної сигналізації	534
8.3.3. Система автоматичного пожежогасіння	538
8.3.4. Система контролю й управління доступом	539
8.3.5. Система відеоспостереження	540
8.3.6. Система протидії економічному шпигунству	542
8.3.7. Система безпеки інформаційної системи	542
8.3.8. Система захисту інформації	544
8.3.9. Система збирання й опрацювання інформації	547
8.4. Створення системи інформаційної безпеки	548
8.4.1. Концепція створення захищених інформаційних систем	548
8.4.2. Етапи створення системи інформаційної безпеки	551
8.4.3. Науково-дослідне розроблення системи інформаційної безпеки	551
8.4.4. Моделювання системи інформаційної безпеки	554
8.4.5. Вибір показників ефективності та критеріїв оптимальності системи інформаційної безпеки	559
8.4.6. Підходи до оцінювання ефективності системи інформаційної безпеки	560
8.4.7. Проектування системи інформаційної безпеки	562
Контрольні питання до розділу 8	564
Список літератури до розділу 8	565
Предметний покажчик	567