

Зміст

Передмова	13
Частина I	
Забезпечення захисту інформації в інформаційно-комунікаційних системах	
Розділ 1. Базові поняття	18
1.1. Термінологія	18
1.1.1. Системи, в яких здійснюється захист інформації	18
1.1.2. Завдання захисту інформації	20
1.1.3. Загрози і вразливості	22
1.1.4. Комплексна система захисту інформації	23
1.1.5. Об'єкти захисту та їхні властивості	24
1.1.6. Розроблення й оцінювання захищених систем	26
1.2. Загрози безпеці інформації	27
1.2.1. Класифікація загроз	27
1.2.2. Перелік типових загроз безпеці	28
1.2.3. Класифікація атак	30
1.2.4. Методика класифікації загроз STRIDE	31
1.2.5. Модель загроз	32
1.3. Порушники	32
1.3.1. Визначення терміну «хакер»	32
1.3.2. Наслідки від дій порушників	33
1.3.3. Модель порушника	34
Висновки	35
Контрольні запитання та завдання	36
Розділ 2. Будова систем захисту інформації	37
2.1. Рівні інформаційно-комунікаційної системи	37
2.2. Функціональні сервіси безпеки і механізми, що їх реалізують	41
2.3. Основні підсистеми комплексу засобів захисту	45
2.3.1. Підсистема керування доступом	46
2.3.2. Підсистема ідентифікації й автентифікації	47
2.3.3. Підсистема аудита	48
2.3.4. Підсистема забезпечення цілісності	49
2.3.5. Криптографічна підсистема	49
Висновки	49
Контрольні запитання та завдання	50
Розділ 3. Основи криптографічних методів захисту інформації	51
3.1. Історична довідка	51
3.2. Основні поняття	52
3.3. Шифрування з ключем	54
3.3.1. Симетричне шифрування	54
3.3.2. Асиметричне шифрування	56
3.4. Поняття криптографічної системи	58
Висновки	60
Контрольні запитання та завдання	61

Розділ 4. Теоретичні основи захисту інформації	62
4.1. Загальні поняття теорії захисту інформації	62
4.2. Позначення, аксіоми та визначення	64
4.3. Основні типи політик безпеки	65
4.4. Математичні моделі безпеки.....	69
4.4.1. Моделі дискреційної політики безпеки.....	69
4.4.2. Моделі мандатної політики безпеки	73
Висновки	75
Контрольні запитання та завдання.....	76
Частина II	
Основні загрози безпеці інформації в інформаційно-комунікаційних системах	
Розділ 5. Типові вразливості систем і аналіз причин їх появи	78
5.1. Передумови виникнення вразливостей у комп'ютерних системах	78
5.2. Класифікація вад захисту	80
5.2.1. Класифікація вад захисту за причиною їх появи	80
5.2.2. Класифікація вад захисту за їх розміщенням у системі	81
5.2.3. Класифікація вад захисту за етапами їх появи	83
5.3. Класифікація помилок, що виникають у процесі програмної реалізації системи	87
5.4. Помилки переповнення буфера	89
5.4.1. Переповнення буфера у стеку.....	89
5.4.2. Переповнення буфера у статичній або динамічній пам'яті	92
5.4.3. Помилка переповнення в один байт.....	92
5.5. Помилки оброблення текстових рядків	93
5.5.1. Використання конвеєра	93
5.5.2. Переспрямування введення-виведення	95
5.5.3. Спеціальні символи.....	95
5.6. Люки	96
5.6.1. Режим debug у програмі sendmail	97
Висновки	97
Контрольні запитання та завдання.....	98
Розділ 6. Шкідливе програмне забезпечення	99
6.1. Класифікація шкідливого програмного забезпечення	99
6.2. Програмні закладки	102
6.2.1. Функції програмних закладок.....	102
6.2.2. Шпигунські програми	103
6.2.3. «Логічні бомби»	104
6.2.4. Люки — утиліти віддаленого адміністрування.....	104
6.2.5. Несанкціонована робота з мережею	106
6.2.6. Інші програмні закладки.....	107
6.3. Комп'ютерні віруси	109
6.3.1. Файлові віруси	110
6.3.2. Завантажувальні віруси	112
6.3.3. Макровіруси	114
6.3.4. Скриптові віруси.....	115
6.3.5. Захист від комп'ютерних вірусів.....	116

6.4. Мережні хробаки	117
6.4.1. Класифікація мережних хробаків.....	118
6.4.2. Хробак Морріса.....	121
6.4.3. Сучасні мережні хробаки.....	126
6.5. «Троянські коні».....	127
6.5.1. Соціальна інженерія	128
6.5.2. Класифікація «троянських коней»	129
6.5.3. Шпигунські троянські програми	130
6.5.4. Троянські інсталютори	131
6.5.5. «Троянські бомби».....	131
6.6. Спеціальні хакерські утиліти	132
6.6.1. Засоби здійснення віддалених атак.....	133
6.6.2. Засоби створення шкідливого програмного забезпечення	134
6.6.3. Створення засобів атак	135
Висновки	138
Контрольні запитання та завдання.....	140

Частина III

Нормативні документи з оцінювання захищеності інформації

Розділ 7. Розвиток стандартів безпеки	142
7.1. Призначення стандартів інформаційної безпеки	142
7.2. Стандарти, орієнтовані на застосування військовими та спецслужбами	143
7.2.1. «Критерії оцінювання захищених комп'ютерних систем» Міністерства оборони США	144
7.2.2. Інтерпретація і розвиток TCSEC	149
7.2.3. Керівні документи Державної технічної комісії при Президенті Російської Федерації.....	150
7.3. Стандарти, що враховують специфіку вимог захисту в різних системах	151
7.3.1. Європейські критерії безпеки інформаційних технологій	151
7.4. Стандарти, що використовують концепцію профілю захисту.....	155
7.4.1. Концепція профілю захисту	155
7.4.2. Федеральні критерії безпеки інформаційних технологій США.....	156
Висновки	157
Контрольні запитання та завдання.....	158
Розділ 8. Нормативно-правова база України	159
8.1. Законодавча і нормативна база захисту інформації в Україні.....	159
8.1.1. Закон України «Про захист інформації в інформаційно- телекомунікаційних системах»	160
8.1.2. Нормативні документи системи технічного захисту інформації	160
8.2. Оцінювання захищеності інформації, яку обробляють у комп'ютерних системах.....	161
8.2.1. Особливості термінології.....	161
8.2.2. Критерії захищеності інформації в комп'ютерних системах від несанкціонованого доступу	162
8.2.3. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності інформації в комп'ютерних системах	169

8.3. Керівні документи з вимогами до захисту інформації в інформаційних системах певних типів	170
8.3.1. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2	170
8.3.2. Вимоги до захисту інформації веб-сторінки від несанкціонованого доступу	172
Висновки	173
Контрольні запитання та завдання	174
Розділ 9. Міжнародний стандарт ISO/IEC 15408	175
9.1. Основні відомості	175
9.2. Базові поняття	177
9.3. Розроблення IT-продукту та його кваліфікаційний аналіз	180
9.3.1. Загальні положення	180
9.3.2. Оцінювання об'єкта за «Загальною методологією»	181
9.3.3. Матеріали, необхідні для проведення кваліфікаційного аналізу	182
9.3.4. Три етапи здійснення кваліфікаційного аналізу	182
9.4. Структура основних документів «Загальних критеріїв»	182
9.4.1. Профіль захисту	182
9.4.2. Завдання з безпеки	185
Висновки	188
Контрольні запитання та завдання	188

Частина IV

Захист інформації на рівні операційної системи

Розділ 10. Апаратне забезпечення засобів захисту	190
10.1. Завдання апаратного захисту	190
10.2. Підтримка керування пам'яттю	191
10.2.1. Віртуальні адреси	191
10.2.2. Віртуальна пам'ять	191
10.2.3. Трансляція адрес	194
10.3. Підтримка керування процесами	196
10.4. Особливості архітектури процесорів Intel x86	198
10.4.1. Регістри процесорів x86	199
10.4.2. Селектори та дескриптори сегментів і сторінок	203
10.5. Керування оперативною пам'яттю	208
10.5.1. Сегментний розподіл пам'яті	208
10.5.2. Сегментно-сторінковий розподіл пам'яті	213
10.6. Керування задачами	213
10.6.1. Виклик процедур	214
10.6.2. Виклик задач	216
10.6.3. Привілейовані команди	218
Висновки	218
Контрольні запитання та завдання	219
Розділ 11. Захищені операційні системи	221
11.1. Загрози безпеці операційних систем	221
11.1.1. Сканування файлової системи	221
11.1.2. Викрадення ключової інформації	222
11.1.3. Добирання паролів	223

11.1.4. Збирання сміття.....	223
11.1.5. Перевищення повноважень	224
11.1.6. Програмні закладки	225
11.1.7. «Жадібні» програми	225
11.2. Поняття захищеної операційної системи	225
11.2.1. Підходи до побудови захищених операційних систем.....	225
11.2.2. Принципи створення захищених систем.....	226
11.2.3. Адміністративні заходи захисту	227
11.2.4. Політика безпеки	229
11.3. Типова архітектура комплексу засобів захисту операційних систем	231
11.3.1. Основні функції КЗЗ	231
11.3.2. Розмежування доступу.....	232
11.3.3. Ідентифікація, автентифікація й авторизація	235
11.3.4. Аудит	237
Висновки	238
Контрольні запитання та завдання.....	239
Розділ 12. Засоби захисту в операційній системі UNIX	241
12.1. Історія створення UNIX.....	241
12.2. Архітектура системи.....	243
12.3. Безпека UNIX	246
12.3.1. Модель безпеки системи UNIX	246
12.3.2. Підсистема ідентифікації й автентифікації.....	246
12.3.3. Підсистема розмежування доступу.....	249
12.3.4. Підсистема реєстрації	252
12.4. Адміністрування засобів безпеки UNIX.....	253
12.4.1. Особливості адміністрування.....	253
12.4.2. Утиліти безпеки	254
12.4.3. Характерні вразливості системи UNIX.....	257
Висновки	258
Контрольні запитання та завдання.....	260
Розділ 13. Засоби захисту в операційній системі Windows	261
13.1. Основні відомості про систему	261
13.1.1. Стисло про історію створення системи	261
13.1.2. Відповідність вимогам стандартів безпеки	262
13.2. Архітектура системи.....	263
13.2.1. Основні концепції	263
13.2.2. Компоненти системи захисту.....	264
13.3. Розмежування доступу	266
13.3.1. Основні принципи реалізації системи розмежування доступу	266
13.3.2. Суб'єкти доступу Windows	266
13.3.3. Об'єкти доступу Windows.....	268
13.3.4. Стандарти настроювання прав доступу.....	269
13.3.5. Ідентифікація й автентифікація	270
13.3.6. Реалізація дискреційного керування доступом	272
13.4. Аудит.....	285
13.5. Аналіз причин уразливостей системи Windows	286
Висновки	288
Контрольні запитання та завдання.....	289

Розділ 14. Системи оброблення конфіденційної інформації	291
14.1. Обґрунтування застосування захищених ОС.....	291
14.2. Система Trusted Solaris.....	292
14.2.1. Основні характеристики середовища Trusted Solaris.....	292
14.2.2. Керування доступом у середовищі Trusted Solaris.....	294
14.2.3. Окреме зберігання позначеної мітками інформації у середовищі Trusted Solaris.....	299
14.2.4. Адміністрування безпеки у середовищі Trusted Solaris.....	301
14.3. Операційна система Фенікс.....	303
14.3.1. Архітектура системи.....	304
14.3.2. Засоби захисту.....	307
14.3.3. Дискреційна модель ієрархічного керування.....	308
14.3.4. Засоби керування доступом.....	310
14.3.5. Перегляд протоколу аудита.....	311
14.3.6. Програмні інтерфейси системи.....	311
14.3.7. Застосування операційної системи Фенікс.....	312
Висновки.....	312
Контрольні запитання та завдання.....	313

Частина V

Захист інформації в розподілених системах

Розділ 15. Основи безпеки інформації в комп'ютерних мережах	316
15.1. Основні відомості про комп'ютерні мережі.....	316
15.1.1. Відкриті системи.....	317
15.1.2. Модель взаємодії відкритих систем.....	317
15.1.3. Стеки протоколів.....	319
15.2. Інтернет.....	321
15.2.1. Організація.....	321
15.2.2. Адресація.....	322
15.2.3. Маршрутизація.....	326
15.3. Загрози безпеці інформації у мережах.....	329
15.4. Безпека взаємодії відкритих систем.....	330
15.4.1. Сервіси безпеки.....	331
15.4.2. Специфічні механізми безпеки.....	333
15.4.3. Універсальні механізми безпеки.....	336
15.4.4. Керування безпекою.....	338
15.4.5. Подальший розвиток міжнародних стандартів.....	340
Висновки.....	340
Контрольні запитання та завдання.....	342
Розділ 16. Безпека мережних протоколів Інтернету	343
16.1. Протоколи прикладного рівня.....	343
16.1.1. Протокол Telnet.....	344
16.1.2. Протокол FTP.....	349
16.1.3. Мережні служби UNIX.....	356
16.2. Транспортні протоколи.....	359
16.2.1. Протокол UDP.....	360
16.2.2. Протокол TCP.....	361

16.3. Протокол IP	369
16.3.1. Призначення й можливості протоколу IPv4	369
16.3.2. Атаки на протокол IPv4, пов'язані з адресацією	372
16.3.3. Атаки, що ґрунтуються на помилках оброблення фрагментованих пакетів	373
16.3.4. Можливості, закладені у протокол IPv6	378
16.4. Протокол маршрутизації BGP	380
16.4.1. Особливості протоколу	380
16.4.2. Модель загроз	384
16.4.3. Механізми захисту	388
16.4.4. Рішення з безпеки	389
16.4.5. Оцінювання захищеності	391
16.5. Протоколи керування мережею	393
16.5.1. Протокол ICMP	393
16.5.2. Протокол SNMP	403
Висновки	408
Контрольні запитання та завдання	410
Розділ 17. Безпека прикладних служб Інтернету	412
17.1. Система електронної пошти	412
17.1.1. Архітектура системи електронної пошти	413
17.1.2. Формат повідомлення електронної пошти	416
17.1.3. Протокол SMTP	417
17.1.4. Протокол POP3	419
17.1.5. Протокол IMAP4	421
17.1.6. Загрози, пов'язані з використанням електронної пошти	422
17.1.7. Анонімне відсилання електронної пошти	426
17.1.8. Атаки через систему електронної пошти	427
17.2. Веб-служба	430
17.2.1. Принципи веб-технології	430
17.2.2. Протокол HTTP	433
17.2.3. Динамічні сторінки	439
17.2.4. Уразливості серверного програмного забезпечення	441
17.2.5. Уразливості у сценаріях	443
17.2.6. SQL-ін'єкція	447
17.2.7. Міжсайтовий скриптинг	450
17.2.8. Захист сервера від атак	453
17.2.9. Атака на клієнта	454
17.2.10. Безпека Java	457
Висновки	460
Контрольні запитання та завдання	461
Розділ 18. Засоби захисту в розподілених інформаційно-комунікаційних системах	463
18.1. Архітектура захищених мереж	463
18.1.1. Протидія прослуховуванню трафіку	463
18.1.2. Сегментація мережі	464
18.1.3. Резервування мережного обладнання і каналів зв'язку	465

18.2. Міжмережні екрани	466
18.2.1. Можливості міжмережних екранів	467
18.2.2. Рівні реалізації	468
18.2.3. Особливості персональних брандмауерів	471
18.2.4. Недоліки міжмережного екрана.....	472
18.3. Системи виявлення атак	474
18.3.1. Можливості систем виявлення атак.....	474
18.3.2. Різні типи систем виявлення атак.....	475
18.3.3. Інформаційні джерела	477
18.3.4. Аналіз подій у системах виявлення атак.....	480
18.3.5. Відповідні дії систем виявлення атак.....	482
18.4. Додаткові інструментальні засоби.....	484
18.4.1. Системи аналізу й оцінювання вразливостей	484
18.4.2. Перевірка цілісності файлів	488
Висновки	489
Контрольні запитання та завдання	490
Розділ 19. Передавання інформації через захищені мережі	491
19.1. Захист інформації, що передається відкритими каналами зв'язку	491
19.2. Віртуальні захищені мережі	492
19.2.1. Різні види віртуальних захищених мереж	492
19.2.2. Проблеми побудови віртуальних захищених мереж.....	493
19.3. Рівні реалізації віртуальних захищених мереж	495
19.3.1. Захист віртуальних каналів на сеансовому рівні	495
19.3.2. Захист віртуальних каналів на мережному рівні	499
19.3.3. Захист віртуальних каналів на каналному рівні	505
19.4. Вимоги нормативної бази до реалізації віртуальних захищених мереж в Україні	508
Висновки	509
Контрольні запитання та завдання	510

Частина VI

Створення, введення в дію та супроводження захищених систем

Розділ 20. Створення комплексної системи захисту інформації.....	512
20.1. Порядок проведення робіт зі створення комплексної системи захисту інформації	512
20.1.1. Структура комплексної системи захисту інформації	513
20.1.2. Створення комплексної системи захисту інформації.....	513
20.2. Вимоги до комплексної системи захисту інформації та політика безпеки....	515
20.2.1. Обґрунтування потреби у створенні системи захисту	515
20.2.2. Обстеження середовищ функціонування інформаційно- телекомунікаційних систем.....	515
20.2.3. Визначення й аналіз можливих загроз безпеці	517
20.2.4. Розроблення політики безпеки	521
20.2.5. Перелік вимог до захищеної системи	529
20.3. Розроблення технічного завдання на створення комплексної системи захисту інформації.....	531
20.4. Створення і впровадження комплексної системи захисту інформації	535
20.4.1. Розроблення проекту	535

20.4.2. Введення комплексної системи захисту інформації в дію та оцінювання захищеності інформації в інформаційно-телекомунікаційних системах	538
20.4.3. Супроводження комплексної системи захисту інформації	541
Висновки	541
Контрольні запитання та завдання	543
Розділ 21. Кваліфікаційний аналіз засобів і систем захисту інформації	544
21.1. Вимоги до кваліфікаційного аналізу	544
21.2. Організація державної експертизи	545
21.2.1. Положення про державну експертизу.....	545
21.2.2. Рекомендації з оформлення програм і методик проведення експертизи комплексної системи захисту інформації	546
21.3. Сертифікація засобів технічного захисту інформації.....	549
Висновки	552
Контрольні запитання та завдання.....	552
Розділ 22. Супроводження комплексної системи захисту інформації	553
22.1. «Типове положення про службу захисту інформації в автоматизованій системі»	553
22.1.1. Загальні положення	554
22.1.2. Завдання та функції служби захисту інформації	555
22.1.3. Права й обов'язки служби захисту інформації	558
22.1.4. Взаємодія служби захисту інформації з іншими підрозділами та із зовнішніми організаціями	560
22.1.5. Штатний розклад і структура служби захисту інформації	561
22.1.6. Організація заходів служби захисту інформації та їх фінансування	562
22.2. Рекомендації щодо структури та змісту Плану захисту інформації в автоматизованій системі	563
22.2.1. Завдання захисту інформації в АС	564
22.2.2. Класифікація інформації, що обробляють в АС	565
22.2.3. Компоненти АС і технології оброблення інформації	566
22.2.4. Загрози інформації в АС	567
22.2.5. Політика безпеки інформації в АС.....	567
22.2.6. Календарний план робіт із захисту інформації в АС	567
22.3. ISO/IEC 27002 «Інформаційні технології — Методики безпеки — Практичні правила управління безпекою інформації»	568
22.3.1. Загальні відомості про стандарт	568
22.3.2. Структура й основний зміст стандарту.....	569
22.3.3. Інші стандарти серії 27000	581
Висновки	582
Контрольні запитання та завдання.....	583
Список скорочень	584
Література та посилання	594