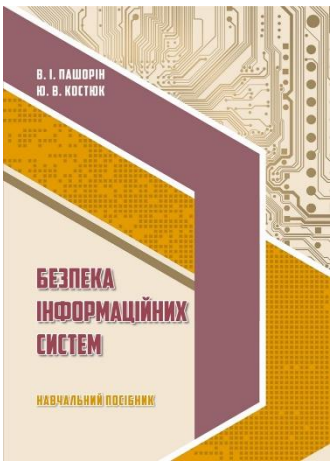

Пашорін В. І.

Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.

ISBN 978-966-918-101-5

У навчальному посібнику розглянуто сучасні напрями забезпечення безпеки інформаційно-телекомунікаційних систем. Викладено технічні, криптографічні, програмні методи і засоби захисту інформації. Формулюються проблеми вразливості сучасних інформаційно-телекомунікаційних систем, розглядаються питання захисту інформації в розподілених інформаційних системах, організаційно-правове забезпечення захисту інформації. Розглянуті загальні питання технологій збереження даних в єдиному інформаційному просторі та впровадженню функцій протидій кіберзлочинності, здатності організовувати та підтримувати комплекс заходів щодо забезпечення безпеки інформаційної та кібербезпеки, з урахуванням їхньої юридичної та економічної обґрунтованості, технічної реалізації, запобігання можливих зовнішніх впливів, імовірних загроз, а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, застосування технологій захисту інформаційно-телекомунікаційних систем.

Призначено для студентів галузі знань 12 «Інформаційні технології», аспірантів, що вивчають методи захисту інформації та безпеки інформаційних систем.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8

ВСТУП 9

Розділ 1. КІБЕРПРОСТІР ТА КІБЕРБЕЗПЕКА: КЛЮЧОВІ ПИТАННЯ ТА ВИЗНАЧЕННЯ 11

ГЛАВА 1. Безпека інформаційних систем в умовах функціонування глобальних мереж 11

1.1. Актуальність безпеки інформаційно-телекомунікаційних систем (ІТС)..... 12

1.2. Класифікація та властивості інформації 19

1.3. Основні терміни і визначення безпеки ІТС 24

ГЛАВА 2. Кібербезпека – складова частина безпеки ІТС 27

2.1. Кіберпростір і кібербезпека 27

2.2. Ключові питання кібербезпеки 34

2.3. Кіберзброя, кібертероризм і кібервійни 38

Контрольні запитання 42

Розділ 2. ВРАЗЛИВОСТІ ТА ЗАГРОЗИ ФУНКЦІОНУВАННЯ ІТС 43

ГЛАВА 3. Загрози інформації в ІТС 43
3.1. Загрози безпеки функціонування ІТС 43
3.2. Вразливості та вади захисту системи 48
3.3. Класифікація загроз безпеки 52
3.4. Основні навмисні загрози 60

ГЛАВА 4. Мережеві загрози 64
4.1.Сучасні мережеві загрози: інтернет-шахрайство 64
4.2. Сучасні мережеві загрози: крадіжка особистості 75
4.3. Загрози приватності при роботі в відкритих мережах 79
4.4. Соціальна інженерія 83
Контрольні запитання 91

Розділ 3. АТАКИ НА ІТС. ПОРУШНИКИ КІБЕРБЕЗПЕКИ 92

ГЛАВА 5. Атаки на інформаційні системи 92
5.1. Визначення атаки на ІТС 92
5.2. Фази атаки. Ланцюг кібервбивства 94
5.3. APT-атака 102

ГЛАВА 6. Класифікація та приклади атак на ІТС 106
6.1. Таксономія та приклади кібератак 106
6.2. Мережеві атаки. Застосування бот-мереж 114
6.3. Сучасні типові атаки на ІТС 123

ГЛАВА 7. Порушники безпеки 130
7.1. Порушники безпеки ІТС 130
7.2. Хакінг та етичний хакінг 138
Контрольні запитання 146

Розділ 4. ТЕОРІЯ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ІТС 147

ГЛАВА 8. Технології та методи захисту ІТС 147
8.1. Сучасні технології захисту інформаційних ресурсів 147
8.2. Основні методи забезпечення безпеки ІТС 150
8.3. Комплексне обстеження ІТС (аудит безпеки ІТС) 154

ГЛАВА 9. Теоретичні аспекти захисту ІТС 157
9.1. Моделі безпеки ІТС 157
9.2. Особливості сучасних ІТС, з точки зору безпеки 161
9.3. Принципи побудови систем безпеки 163
9.4. Архітектурна безпека 166
Контрольні запитання 169

Розділ 5. ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ЗАХИСТ ВІД РУЙНУЮЧИХ ПРОГРАМНИХ ДІЙ 170

ГЛАВА 10. Комп'ютерні віруси: класифікація та характеристика 170
10.1. Поняття та класифікація шкідливого програмного забезпечення 170
10.2. Поняття та класифікація комп'ютерних вірусів 176
10.3. Коротка характеристика вірусів 181

ГЛАВА 11. Шкідливе програмне забезпечення 185
11.1. Мережеві хробаки 185
11.2. Троянські програми 191
11.3. Спеціальні шкідливі програми 197

ГЛАВА 12. Захист від шкідливого програмного забезпечення 208
12.1. Методи виявлення шкідливих програм 208
12.2. Типи і характеристики антивірусних програм 211
12.3. Технологія Whitelisting і антивірусні хмари 218
Контрольні запитання 221

Розділ 6. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІТС 222

ГЛАВА 13. Закони, нормативні документи і стандарти 222
13.1. Законодавство України по забезпеченню кібербезпеки 222
13.2. Нормативні документи системи технічного захисту інформації 225
13.3. Стандарти інформаційної безпеки. Стандарт TCSEC 228
13.4. Поняття кіберзлочинності. Класифікація кіберзлочинів 232

ГЛАВА 14. Міжнародні стандарти 237
14.1. Класи безпеки комп'ютерних систем 237
14.2. Міжнародні стандарти серії ISO 27000 240
Контрольні запитання 247

Розділ 7. АДМІНІСТРАТИВНЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІТС 248

ГЛАВА 15. Політика безпеки 248
15.1. Організаційний захист 248
15.2. Склад і структура політики безпеки 253
15.3. Зразок спеціалізованої політики безпеки допустимого використання . 258

ГЛАВА 16. Процедури політики безпеки 261
16.1. Процедури реалізації політики безпеки 261
16.2. Оновлення ПЗ та зниження привілеїв 269

ГЛАВА 17. Управління ризиками 275
17.1. Ризики безпеки ІТС 275
17.2. Типові витрати на забезпечення безпеки ІТС 281
Контрольні запитання 287

Розділ 8. ІНЖЕНЕРНО-ТЕХНІЧНИЙ ЗАХИСТ ІТС 288

ГЛАВА 18. Технічні канали витоку інформації..... 288
18.1. Загальна характеристика інженерно-технічних засобів безпеки 288
18.2. Фізичний захист..... 290
18.3. Технічні канали витоку інформації 293

ГЛАВА 19. Економічна розвідка і принципи захисту від неї..... 305
19.1. Технічні засоби економічної розвідки 305
19.2. Принципи захисту від економічної розвідки..... 312
Контрольні запитання..... 317

Розділ 9. ПРОГРАМНО-АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІТС 318

ГЛАВА 20. Ідентифікація і автентифікація 318
20.1. Загальна характеристика програмних засобів безпеки ІТС 318
20.2. Ідентифікація, автентифікація та авторизація в ІТС 321
20.3. Види автентифікації суб'єктів в ІТС..... 325
20.4. Парольна автентифікація 327
20.5. Автентифікація на основі PIN-коду..... 330

ГЛАВА 21. Види автентифікації..... 332
21.1. Апаратна автентифікація 332
21.2. Автентифікація за допомогою біометричних даних..... 340
21.3. Автентифікація на основі цифрових сертифікатів 346
21.4. Централізовані системи автентифікації. Концепція єдиного логічного входу..... 348
Контрольні запитання..... 353

Розділ 10. УПРАВЛІННЯ ДОСТУПОМ І АУДИТ ІТС..... 355

ГЛАВА 22. Управління доступом..... 355
22.1. Поняття і технології управління доступом 355
22.2. Дискреційна модель розмежування доступу..... 358
22.3. Мандатна модель розмежування доступу 361

ГЛАВА 23. Управління доступом і реєстрація подій в системі..... 364
23.1. Рольова модель розмежування доступу 364
23.2. Реєстрація подій і аудит 367
Контрольні запитання..... 371

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ 372