

# ЗМІСТ

<b>ВСТУП</b>	<b>11</b>
<b>ПЕРЕЛІК АБРЕВІАТУР</b>	<b>13</b>
<b>I Основи технічного захисту інформації</b>	<b>15</b>
<b>Розділ 1. Системний підхід до технічного захисту інформації</b>	<b>16</b>
1.1. Основні положення системного підходу до технічного захисту інформації . . . . .	16
1.2. Цілі, завдання і ресурси системи захисту інформації . . . . .	18
1.3. Загрози безпеці інформації і засоби щодо їх попередження . . . . .	20
1.3.1. Основні властивості інформації як предмета захисту . . . . .	20
1.3.2. Класифікація загроз безпеці інформації та інформаційних ресурсів . . . . .	23
1.3.3. Класифікація джерел загроз інформації . . . . .	27
1.3.4. Класифікація уразливостей безпеки . . . . .	34
1.3.5. Класифікація актуальних загроз . . . . .	36
1.3.6. Основні напрями захисту інформації та інформаційних ресурсів . . . . .	37
Висновки . . . . .	39
Питання та практичні завдання до розділу 1 . . . . .	41
<b>Розділ 2. Основні положення концепції технічного захисту інформації</b>	<b>42</b>
2.1. Концепція технічного захисту інформації в Україні . . . . .	42
2.1.1. Загальні положення . . . . .	42
2.1.2. Загрози безпеці інформації та стан її технічного захисту . . . . .	43
2.1.3. Система технічного захисту інформації . . . . .	45
2.1.4. Основні напрями державної політики у сфері технічного захисту інформації . . . . .	47
2.2. Основні положення концепції технічного захисту інформації на об'єкті інформаційної діяльності . . . . .	50
2.2.1. Принципи технічного захисту інформації на об'єкті інформаційної діяльності . . . . .	50
2.2.2. Принципи побудови системи захисту інформації . . . . .	51
Висновки . . . . .	54
Питання та практичні завдання до розділу 2 . . . . .	54

<b>Розділ 3. Характеристика інформації, що підлягає захисту</b>	<b>55</b>
3.1. Інформація та дані . . . . .	55
3.2. Форми адекватності інформації . . . . .	58
3.3. Міри інформації . . . . .	59
3.4. Якість інформації . . . . .	63
3.5. Види інформації, що підлягають захисту . . . . .	65
3.5.1. Основні властивості інформації як предмета захисту . . . . .	65
3.5.2. Демаскуючі ознаки об'єктів захисту . . . . .	72
3.5.3. Класифікація демаскуючих ознак об'єктів захисту . . . . .	72
3.5.4. Видові демаскуючі ознаки . . . . .	73
3.5.5. Демаскуючі ознаки сигналів . . . . .	74
3.5.6. Демаскуючі ознаки речовин . . . . .	77
Висновки . . . . .	79
Питання та практичні завдання до розділу 3 . . . . .	80
<b>Розділ 4. Загрози безпеці інформації</b>	<b>81</b>
4.1. Загальна характеристика загроз безпеці інформації . . . . .	81
4.2. Побічні електромагнітні випромінювання і наведення . . . . .	82
4.3. Технічні канали витоку інформації . . . . .	83
4.3.1. Загальні відомості про канали технічного витоку інформації . . . . .	83
4.3.2. Акустичні канали витоку інформації . . . . .	87
4.3.3. Оптичні канали витоку інформації . . . . .	91
4.3.4. Радіоелектронні канали витоку інформації . . . . .	92
4.3.5. Кіберканали витоку інформації . . . . .	94
4.3.6. Речовинні канали витоку інформації . . . . .	95
4.4. Способи доступу до джерел інформації . . . . .	96
Питання та практичні завдання до розділу 4 . . . . .	99
<b>Розділ 5. Основні характеристики засобів технічної розвідки як джерел загроз</b>	<b>101</b>
5.1. Загальні положення та класифікація технічної розвідки . . . . .	101
5.1.1. Загальне визначення технічної розвідки . . . . .	101
5.1.2. Класифікація технічної розвідки . . . . .	102
5.2. Структура системи технічної розвідки . . . . .	105
5.3. Загальна технологія добування інформації . . . . .	106
5.4. Класифікація технічних засобів добування інформації . . . . .	111
5.5. Можливості засобів технічної розвідки . . . . .	114
5.6. Технічні засоби розвідки . . . . .	117
5.6.1. Технічні засоби підслуховування . . . . .	117
5.6.1.1. Акустичні приймачі . . . . .	119
5.6.1.2. Закладні пристрої . . . . .	130
5.6.1.3. Лазерні засоби підслуховування . . . . .	134
5.6.1.4. Засоби високочастотного нав'язування . . . . .	135
5.6.1.5. Диктофони . . . . .	136
5.6.2. Засоби спостереження . . . . .	137
5.6.2.1. Засоби спостереження в оптичному діапазоні . . . . .	138
5.6.2.2. Засоби спостереження в інфрачервоному діапазоні . . . . .	148

5.6.3.	Засоби спостереження в радіодіапазоні . . . . .	150
5.6.4.	Засоби перехоплення сигналів . . . . .	152
5.6.4.1.	Структура комплексу засобів перехоплення радіо- сигналів . . . . .	152
5.6.4.2.	Анени . . . . .	153
5.6.4.3.	Радіоприймачі . . . . .	156
5.6.4.4.	Засоби технічного аналізу сигналів . . . . .	162
5.6.4.5.	Засоби визначення координат джерел радіосигналів . . . . .	162
5.6.4.6.	Індикація та реєстрація сигналів перехоплення . . . . .	163
5.6.5.	Засоби перехоплення електричних та оптичних сигналів . . . . .	163
5.6.5.1.	Засоби перехоплення електричних сигналів . . . . .	164
5.6.5.2.	Засоби перехоплення оптичних сигналів . . . . .	166
5.6.6.	Засоби добування інформації про речовини . . . . .	166
5.7.	Сервіси та користувачі кіберпростору як об'єкти і суб'єкти кібер- розвідки . . . . .	168
5.7.1.	Розвідка систем телекомунікацій . . . . .	170
5.7.2.	Розвідка в мережах інфраструктури кіберпростору . . . . .	171
5.7.3.	Кіберрозвідка . . . . .	172
	Висновки . . . . .	174
	Питання та практичні завдання до розділу 5 . . . . .	177
<b>Розділ 6.</b>	<b>Методи технічного захисту інформації</b>	<b>179</b>
6.1.	Фактори забезпечення захисту інформації від загроз впливу . . . . .	179
6.2.	Фактори забезпечення захисту інформації від загроз витоку інфор- мації . . . . .	181
6.2.1.	Умови утворення технічного каналу витоку інформації . . . . .	181
6.2.2.	Час і витрати на пошук носія з інформацією, що підлягає захисту . . . . .	182
6.2.3.	Ймовірність виявлення і розпізнавання носія інформації . . . . .	182
6.3.	Класифікація методів технічного захисту інформації . . . . .	186
6.3.1.	Фізичний захист . . . . .	187
6.3.2.	Приховування інформації . . . . .	188
6.3.2.1.	Просторове приховування . . . . .	188
6.3.2.2.	Структурне приховування . . . . .	190
6.3.2.3.	Енергетичне приховування . . . . .	195
6.3.3.	Нейтралізація джерел небезпечних сигналів . . . . .	195
	Висновки . . . . .	196
	Питання та практичні завдання до розділу 6 . . . . .	196
<b>Розділ 7.</b>	<b>Методи фізичного захисту інформації</b>	<b>198</b>
7.1.	Загальна характеристика об'єктів фізичного захисту . . . . .	198
7.2.	Характеристика методів фізичного захисту інформації . . . . .	199
7.2.1.	Затримка зловмисника чи іншого джерела загрози на час, більше часу нейтралізації загрози . . . . .	199
7.2.2.	Виявлення зловмисника або джерела іншої загрози . . . . .	201
7.2.3.	Нейтралізація загроз впливу на джерело інформації . . . . .	205
7.3.	Модель шляху руху зловмисника . . . . .	206

7.3.1.	Загальний опис моделі . . . . .	206
7.3.2.	Приклад роботи моделі . . . . .	208
	Висновки . . . . .	211
	Питання та практичні завдання до розділу 7 . . . . .	211
<b>Розділ 8. Методи протидії спостереженню і підслухуванню</b>		<b>213</b>
8.1.	Методи протидії спостереженню . . . . .	213
8.1.1.	Методи протидії спостереженню в оптичному діапазоні . . . . .	213
8.1.2.	Методи протидії радіолокаційному та гідроакустичному спостереженню . . . . .	221
8.2.	Методи протидії підслухуванню . . . . .	222
8.2.1.	Інформаційне приховування мовної інформації в каналах зв'язку . . . . .	222
8.2.2.	Енергетичне приховування акустичного сигналу . . . . .	226
8.2.3.	Методи попередження несанкціонованого запису мовної інформації на диктофон . . . . .	228
8.2.4.	Методи придушення небезпечних сигналів акустоелектричних перетворювачів . . . . .	230
	Висновки . . . . .	233
	Питання та практичні завдання до розділу 8 . . . . .	234
<b>II Організаційно-технічне та методичне забезпечення технічного захисту інформації</b>		<b>236</b>
<b>Розділ 9. Організація технічного захисту інформації</b>		<b>237</b>
9.1.	Завдання і структура державної системи технічного захисту інформації . . . . .	237
9.1.1.	Державна служба спеціального зв'язку та захисту інформації України . . . . .	237
9.1.2.	Ліцензування діяльності в галузі захисту інформації . . . . .	238
9.1.3.	Експертиза в галузі технічного захисту інформації . . . . .	239
9.1.4.	Державний контроль . . . . .	241
9.1.5.	Основні завдання з кіберзахисту . . . . .	244
9.2.	Завдання і структура системи технічного захисту інформації в організаціях . . . . .	246
9.2.1.	Загальні положення . . . . .	246
9.2.2.	Нормативно-правова база захисту інформації в організації . . . . .	247
9.2.3.	Нормативні документи системи технічного захисту інформації . . . . .	248
	Висновки . . . . .	249
	Питання та практичні завдання до розділу 9 . . . . .	249
<b>Розділ 10. Розробка типових заходів технічного захисту інформації</b>		<b>250</b>
10.1.	Основні організаційні і технічні заходи . . . . .	250
10.2.	Контроль ефективності технічного захисту інформації . . . . .	252
10.3.	Рекомендації щодо моделювання системи технічного захисту інформації . . . . .	255

10.3.1. Алгоритм проектування (удосконалення) системи технічного захисту інформації . . . . .	255
10.3.2. Моделювання об'єктів захисту . . . . .	257
10.3.3. Моделювання загроз інформації . . . . .	258
10.3.4. Рекомендації щодо оцінки показників ефективності захисту	261
10.4. Рекомендації щодо виявлення технічних каналів витоку інформації	261
10.4.1. Загальні положення щодо виявлення технічних каналів витоку інформації . . . . .	261
10.4.2. Рекомендації щодо проведення спеціальних перевірок з виявлення технічних каналів витоку інформації . . . . .	263
10.4.3. Рекомендації щодо проведення спеціальних обстежень виділених приміщень з виявлення технічних каналів витоку інформації . . . . .	267
10.4.4. Основні рекомендації щодо проведення спеціальних досліджень з виявлення технічних каналів витоку інформації . .	275
10.5. Методичні рекомендації щодо вибору заходів технічного захисту інформації . . . . .	281
10.5.1. Методичні рекомендації щодо організації фізичного захисту джерел інформації . . . . .	281
10.5.1.1. Рекомендації щодо підвищення укріпленості інженерних конструкцій . . . . .	281
10.5.1.2. Вибір технічних засобів охорони . . . . .	282
10.5.2. Рекомендації щодо попередження витоку інформації . . . .	282
10.5.2.1. Типові заходи щодо захисту інформації від спостереження . . . . .	282
10.5.2.2. Типові заходи щодо захисту інформації від підслуховування . . . . .	283
10.5.2.3. Типові заходи щодо захисту інформації від перехоплення . . . . .	284
10.5.2.4. Рекомендації щодо «чистки» приміщень від закладних пристроїв . . . . .	284
10.5.2.5. Заходи щодо захисту інформації при роботі з мобільними пристроями . . . . .	285
10.5.2.6. Заходи щодо захисту інформації від витоку по речовинному каналу . . . . .	286
10.5.3. Заходи щодо організації захисту інформації від несанкціонованого доступу при її обробці та зберіганні в інформаційних системах . . . . .	286
10.5.4. Заходи щодо встановлення рівнів безпеки та механізмів безпеки приміщень надавачів електронних довірчих послуг . .	300
Висновки . . . . .	304
Питання та практичні завдання до розділу 10 . . . . .	306

<b>Розділ 11. Основні рекомендації щодо технічного захисту інформації в кабінеті керівника організації</b>	<b>308</b>
11.1. Моделювання кабінету керівника організації як об'єкта захисту . .	308

11.1.1.	Обґрунтування вибору кабінету як об'єкта захисту . . . . .	308
11.1.1.1.	Характеристика інформації, що захищається в кабінеті керівника . . . . .	309
11.1.2.	План кабінету як об'єкта захисту . . . . .	312
11.2.	Моделювання загроз інформації в кабінеті керівника . . . . .	313
11.2.1.	Моделювання загроз впливу на джерела інформації . . . . .	314
11.2.2.	Моделювання технічних каналів витоку інформації . . . . .	317
11.2.2.1.	Моделювання оптичних каналів витоку інформації . . . . .	317
11.2.2.2.	Моделювання акустичних каналів витоку інформації . . . . .	319
11.2.2.3.	Моделювання радіоелектронних каналів витоку інформації . . . . .	320
11.3.	Нейтралізація загроз інформації в кабінеті керівника організації . . . . .	323
11.3.1.	Заходи щодо запобігання проникнення зловмисника до джерел інформації . . . . .	323
11.3.2.	Захист інформації в кабінеті керівника від спостереження . . . . .	324
11.3.3.	Заходи щодо захисту мовної інформації від підслуховування . . . . .	325
	Висновки . . . . .	327
	Питання та практичні завдання до розділу 11 . . . . .	328

## **Розділ 12. Типовий підхід до побудови системи технічного захисту інформації організації 329**

12.1.	Структура системи технічного захисту інформації . . . . .	329
12.2.	Підсистема фізичного захисту джерел інформації . . . . .	330
12.2.1.	Загальні відомості про підсистему фізичного захисту . . . . .	330
12.2.2.	Структура системи контролю і управління доступом . . . . .	331
12.2.3.	Підкомплекс виявлення джерел загроз . . . . .	332
12.2.4.	Підкомплекс спостереження . . . . .	335
12.2.5.	Підкомплекс нейтралізації . . . . .	335
12.3.	Підсистема технічного захисту інформації від її витоку . . . . .	337
12.3.1.	Комплекс захисту інформації від спостереження . . . . .	337
12.3.2.	Комплекс захисту інформації від підслуховування . . . . .	338
12.3.3.	Комплекс захисту інформації від перехоплення . . . . .	338
12.3.4.	Попередження витоку речовинними каналами . . . . .	339
12.4.	Управління силами і засобами технічного захисту інформації . . . . .	339
12.5.	Класифікація засобів технічного захисту інформації . . . . .	341
	Висновки . . . . .	343
	Питання та практичні завдання до розділу 12 . . . . .	343

## **Розділ 13. Засоби інженерного захисту та технічної охорони об'єктів 344**

13.1.	Засоби інженерного захисту інформації . . . . .	344
13.1.1.	Огорожа території . . . . .	344
13.1.2.	Огорожа будівель і приміщень . . . . .	345
13.1.2.1.	Двері і ворота . . . . .	345
13.1.2.2.	Замки . . . . .	345
13.1.2.3.	Вікна . . . . .	347
13.1.2.4.	Металеві шафи, сейфи і сховища . . . . .	348
13.1.3.	Засоби систем управління доступом та контролю доступу . . . . .	350

13.1.4. Картки . . . . .	352
13.2. Засоби технічної охорони об'єктів . . . . .	354
13.2.1. Засоби виявлення зловмисників і пожежі . . . . .	354
13.2.1.1. Сповіщувачі . . . . .	354
13.2.1.2. Контактні сповіщувачі . . . . .	356
13.2.1.3. Акустичні сповіщувачі . . . . .	357
13.2.1.4. Мікрохвильові сповіщувачі . . . . .	357
13.2.1.5. Інші сповіщувачі . . . . .	358
13.2.2. Засоби контролю і управління засобами охорони . . . . .	359
13.2.3. Засоби телевізійної охорони . . . . .	360
13.2.4. Засоби освітлення . . . . .	361
13.3. Засоби нейтралізації загроз . . . . .	362
Висновки . . . . .	363
Питання та практичні завдання до розділу 13 . . . . .	364
<b>Розділ 14. Засоби протидії спостереженню і підслухуванню</b>	<b>366</b>
14.1. Основні види та характеристики засобів протидії спостереженню . . . . .	366
14.1.1. Засоби протидії спостереженню в оптичному діапазоні . . . . .	366
14.1.2. Засоби протидії радіолокаційному спостереженню . . . . .	371
14.1.3. Засоби протидії гідроакустичному спостереженню . . . . .	372
14.2. Основні види та характеристики засобів протидії підслухуванню . . . . .	373
14.2.1. Засоби звукоізоляції та звукопоглинання акустичного сигналу	373
14.2.2. Засоби попередження витоку інформації за допомогою закладних підслуховуючих пристроїв . . . . .	379
14.2.2.1. Класифікація засобів виявлення та локалізації закладних підслуховуючих пристроїв . . . . .	380
14.2.2.2. Апаратура радіоконтролю . . . . .	380
14.2.2.3. Нелінійні локатори . . . . .	388
14.2.2.4. Металодетектори . . . . .	390
14.2.2.5. Рентгенівські апарати . . . . .	392
14.2.2.6. Технічні засоби придушення сигналів закладних пристроїв . . . . .	392
Висновки . . . . .	394
Питання та практичні завдання до розділу 14 . . . . .	395
<b>Розділ 15. Засоби попередження витоку інформації через побічні електромагнітні випромінювання і наведення</b>	<b>397</b>
15.1. Засоби придушення небезпечних сигналів . . . . .	398
15.2. Екранування електромагнітних полів . . . . .	401
15.3. Попередження витоку інформації колами електроживлення і заземлення . . . . .	405
Висновки . . . . .	407
Питання та практичні завдання до розділу 15 . . . . .	408

---

<b>СЛОВНИК ДОДАТКОВИХ ТЕРМІНІВ І ПОНЯТЬ</b>	<b>409</b>
<b>ОДИНИЦІ ВИМІРЮВАННЯ</b>	<b>442</b>
<b>ПРЕДМЕТНИЙ ПОКАЖЧИК</b>	<b>461</b>
<b>ЛІТЕРАТУРА</b>	<b>474</b>



## ВСТУП

Навчальний посібник відображає сучасні погляди на стан розвитку теорії і практики технічного захисту інформації з обмеженим доступом.

Причому, основні визначення дисципліни сформульовані відповідно до законодавчих актів України [53]:

- технічний захист інформації — це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особистості, суспільства і держави;
- система технічного захисту інформації — це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та матеріально-технічна база.

Особливого значення технічний захист інформації набуває як один із основних напрямів кіберзахисту в системах забезпечення кібербезпеки [48], а також у забезпеченні безпеки об'єктів критичної інфраструктури [48; 106].

У **першій частині** посібника наведені основні положення системного підходу щодо захисту інформації, загальних концептуальних підходів щодо побудови системи технічного захисту інформації в державі і в організації, характеристик інформації як предмета захисту, загроз безпеці інформації та методів технічного захисту інформації.

У **другій частині** посібника розглядаються особливості організаційного та методичного забезпечення системи технічного захисту інформації, основи побудови системи і основних підсистем технічного захисту інформації, що включає: типовий підхід до побудови системи технічного захисту інформації організації, який включає застосування засобів технічної охорони об'єктів, засобів протидії спостереженню і підслухуванню, засобів попередження витоку інформації через побічні електромагнітні випромінювання і наведення.

Посібник містить також словники додаткових термінів і понять, одиниць вимірювання та показчик ключових термінів і понять. Ключові тер-

міни і поняття технічного захисту інформації, які формулюються у основному тексті посібника та у словнику додаткових термінів і понять, виділені жирним шрифтом. Наведені також англійські еквіваленти термінів і понять, а також їхня етимологія, тобто визначення походження слова шляхом співставлення його зі спорідненими словами тієї або іншої мови. Це дозволяє досить докладно окреслити предметну частину технічного захисту інформації та використовувати посібник як тлумачний словник.

Автори висловлюють щирю вдячність рецензентам: доктору педагогічних наук, професору С. М. Мамченку та доктору технічних наук, професору В. О. Хорошку за змістовні зауваження та рекомендації, які безумовно сприяли покращенню книги.

Особливу вдячність автори висловлюють генеральному директору науково-впроваджувальної фірми «Криптон» О. Й. Куляниці за плідні дискусії та цінні поради, що сприяли появі посібника та формуванню його змісту.