

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Навчальний посібник

У двох частинах

Частина 1

Основи технічного захисту інформації

Київ

Видавництво Ліра-К

2022

УДК 004.056.5 Т38

Авторський колектив:

БогущВ.М., Бровко В. Д., КобусО.С., КозюраВ.Д.

Рецензенти:

Мамченко С. М., доктор педагогічних наук, професор; Хорошко В.О., доктор технічних наук, професор

*Рекомендовано до друку редакційно-видавничою радою
Національної академії Служби безпеки України
протокол № 4 від 17 грудня 2021 р.*

Т38 Технічний захист інформації: Навч. погіб. в 2 ч. Ч. 1: Основи технічного захисту інформації / В.М.Богущ, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2022. - 286с.

У навчальному посібнику наведена систематизована сукупність відомостей, що забезпечує з'ясування понять захисту інформації з обмеженим доступом, як однієї з найважливіших сфер діяльності держави, опанування основними термінами та категоріями технічного захисту інформації на рівні їх тлумачення і відтворення для практичного застосування та втілення у процесі фахової та професійної діяльності із забезпечення національної безпеки в інформаційній сфері.

Розрахований на курсантів, слухачів та студентів закладів вищої освіти, які навчаються за всіма освітніми програмами спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності).

УДК 004.056.5

© Національна академія служби безпеки
України, 2022

©Богущ В.М., Бровко В.Д., Кобус О.С.,
В.Д.Козюра В.Д., 2022

ЗМІСТ

ВСТУП	8
ПЕРЕЛІК АБРЕВІАТУР	10
Розділ 1. Системний підхід до технічного захисту інформації	12
1.1. Основні положення системного підходу до технічного захисту інформації.....	12
1.2. Цілі, завдання і ресурси системи захисту інформації . .	15
1.3. Загрози безпеці інформації і засоби щодо їх попередження .	17
1.3.1. Основні властивості інформації як предмета захисту	17
1.3.2. Класифікація загроз безпеці інформації та інформаційних ресурсів	20
1.3.3. Класифікація джерел загроз інформації	25
1.3.4. Класифікація уразливостей безпеці.....	34
1.3.5. Класифікація актуальних загроз	37
1.3.6. Основні напрями захисту інформації та інформаційних ресурсів	37
Висновки	41
Питання та практичні завдання до розділу 1.....	42
Розділ 2. Основні положення концепції технічного захисту інформації	44
2.1. Концепція технічного захисту інформації в Україні . .	44
2.1.1. Загальні положення.....	44
2.1.2. Загрози безпеці інформації та стан її технічного захисту	45
2.1.3. Система технічного захисту інформації	47
2.1.4. Основні напрями державної політики у сфері технічного захисту інформації	50

2.2.	Основні положення концепції технічного захисту інформації на об'єкті інформаційної діяльності.....	54
2.2.1.	Принципи технічного захисту інформації на об'єкті інформаційної діяльності	54
2.2.2.	Принципи побудови системи захисту інформації	55
	Висновки	57
	Питання та практичні завдання до розділу 2	58
Розділ 3.	Характеристика інформації, що підлягає захисту	60
3.1.	Інформація та дані	60
3.2.	Форми адекватності інформації.....	63
3.3.	Міри інформації.....	65
3.4.	Якість інформації	70
3.5.	Види інформації, що підлягають захисту	72
3.5.1.	Основні властивості інформації як предмета захисту	72
3.5.2.	Демаскуючі ознаки об'єктів захисту.....	81
3.5.3.	Класифікація демаскуючих ознак об'єктів захисту	81
3.5.4.	Видові демаскуючі ознаки	83
3.5.5.	Демаскуючі ознаки сигналів	84
3.5.6.	Демаскуючі ознаки речовин	88
	Висновки	89
	Питання та практичні завдання до розділу 3	91
Розділ 4.	Загрози безпеці інформації	92
4.1.	Загальна характеристика загроз безпеці інформації . .	92
4.2.	Побічні електромагнітні випромінювання і наведення .	93
4.3.	Технічні канали витоку інформації.....	95
4.3.1.	Загальні відомості про канали технічного витоку інформації	95
4.3.2.	Акустичні канали витоку інформації	98
4.3.3.	Оптичні канали витоку інформації	99
4.3.4.	Радіоелектронні канали витоку інформації . . .	100
4.3.5.	Кіберканали витоку інформації	102
4.3.6.	Речовинні канали витоку інформації	103
4.4.	Способи доступу до джерел інформації	105
	Питання та практичні завдання до розділу 4	109

Розділ 5. Характеристика засобів технічної розвідки 111

5.1.	Загальні положення та класифікація технічної розвідки	111
5.1.1.	Загальне визначення технічної розвідки	111
5.1.2.	Класифікація технічної розвідки	112
5.2.	Структура системи технічної розвідки	115
5.3.	Загальна технологія добування інформації	117
5.4.	Класифікація технічних засобів добування інформації	123
5.5.	Можливості засобів технічної розвідки	128
5.6.	Технічні засоби розвідки	132
5.6.1.	Технічні засоби підслуховування	132
5.6.1.1.	Акустичні приймачі	133
5.6.1.2.	Закладні пристрої	146
5.6.1.3.	Лазерні засоби підслуховування	151
5.6.1.4.	Засоби високочастотного нав'язування	152
5.6.1.5.	Диктофони	153
5.6.2.	Засоби спостереження	154
5.6.2.1.	Засоби спостереження в оптичному діапазоні	155
5.6.2.2.	Засоби спостереження в інфрачервоному діапазоні	168
5.6.3.	Засоби спостереження в радіодіапазоні	170
5.6.4.	Засоби перехоплення сигналів	173
5.6.4.1.	Структура комплексу засобів перехоплення радіосигналів	173
5.6.4.2.	Антени	174
5.6.4.3.	Радіоприймачі	177
5.6.4.4.	Засоби технічного аналізу сигналів	183
5.6.4.5.	Засоби визначення координат джерел радіосигналів	185
5.6.4.6.	Індикація та реєстрація сигналів перехоплення	186
5.6.5.	Засоби перехоплення електричних та оптичних сигналів	186
5.6.5.1.	Засоби перехоплення електричних сигналів	187
5.6.5.2.	Засоби перехоплення оптичних сигналів	189
5.6.6.	Засоби добування інформації про речовини	191
5.7.	Сервіси та користувачі кіберпростору як об'єкти і суб'єкти кіберрозвідки	192
5.7.1.	Розвідка систем телекомунікацій	194
5.7.2.	Розвідка в мережах кіберпростору	196

5.7.3. Кіберрозвідка.....	197
Висновки	200
Питання та практичні завдання до РОЗДІЛУ 5.....	203
Розділ 6. Методи технічного захисту інформації	206
6.1. Фактори забезпечення захисту інформації ВІД загроз впливу	206
6.2. Фактори забезпечення захисту інформації від загроз витоку інформації	209
6.2.1. Умови утворення технічного каналу витоку інформації	209
6.2.2. Час і витрати на пошук носія з інформацією, що підлягає захисту	210
6.2.3. Ймовірність виявлення і розпізнавання носія ін- формації	210
6.3. Класифікація методів технічного захисту інформації .	215
6.3.1. Фізичний захист	216
6.3.2. Приховування інформації.....	217
6.3.2.1. Просторове приховування.....	217
6.3.2.2. Структурне приховування	219
6.3.2.3. Енергетичне приховування	226
6.3.3. Нейтралізація джерел небезпечних сигналів .	227
Висновки	227
Питання та практичні завдання до розділу 6	228
Розділ 7. Методи фізичного захисту інформації	229
7.1. Загальна характеристика об'єктів фізичного захисту .	229
7.2. Характеристика методів фізичного захисту інформації	230
7.2.1. Затримка зломисника чи іншого джерела загрози на час, більше часу нейтралізації загрози	231
7.2.2. Виявлення зломисника або джерела іншої загрози	233
7.2.3. Нейтралізація загроз впливу на джерело інформації ...	239
7.3. Модель шляху руху зломисника.....	240
7.3.1. Загальний опис моделі	240
7.3.2. Приклад роботи моделі.....	242
Висновки	244
Питання та практичні завдання до розділу 7	245

Розділ 8. Методи протидії спостереженню і підслухуван

ню	248
8.1. Методи протидії спостереженню	248
8.1.1. Методи протидії спостереженню в оптичному діапазоні	248
8.1.2. Методи протидії радіолокаційному та гідроакустичному спостереженню	257
8.2. Методи протидії підслухуванню	259
8.2.1. ^формаційне приховування мовної інформації в каналах зв'язку	259
8.2.2. Енергетичне приховування акустичного сигналу	263
8.2.3. Методи попередження несанкціонованого запису мовної інформації на диктофон	267
8.2.4. Методи придушення небезпечних сигналів аку- стоелектричних перетворювачів	269
Висновки	272
Питання та практичні завдання до розділу 7	274
ПРЕДМЕТНИЙ ПОКАЖЧИК ДО ЧАСТИНИ 1	276
ЛІТЕРАТУРА ДО ЧАСТИНИ 1	283

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 [23]: 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 [18], а також у забезпеченні безпеки об'єктів критичної інфраструктури [18; 24].

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, що 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 покажчик ключових термінів і понять. Ключові терміни і поняття технічного захисту інформації, які формулюються у основному тексті посібника та у словнику додаткових термінів і понять, виділені жирним шрифтом, а посилання на них — курсивом. 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 щиру вдячність рецензентам: доктору педагогічних наук наук, професору С. М. Мамченку та доктору технічних наук, професору В.О.Хорошку за змістовні зауваження та рекомендації, які безумовно сприяли покращенню книги.

ПЕРЕЛІК АБРЕВІАТУР

Україномовні

АТС - БД -	автоматична телефонна станція база даних база знань
БЗ - ДРР -	дешифрувально-розв'язувальна робота
ЕОТ - ЕПР -	електронно-обчислювальна техшка ефективна площа
ЕРС - ІТС -	розаювання електрорушшна сила
ЗТО - КА -	інформаційно-телекомунікаційна система зааб ТЕХНІЧНОЇ
КОПС - КПП	охорони космічний апарат
- МДН - НСД	комплекс охоронно-пожежної сигналізації
- ОС - ПВЧ -	контрольно-пропускний пункт
ПЗ - ПЗЗ -	метал-діелектрик-напівпровідник несанкціонований
ПКП -	доступ операційна система підсилювач високої частоти
ПЕМВН -	програмне забезпечення прилад із зарядовим зв'язком
ПЕОМ -	приймально-контрольний прилад
ПНБ - ПНЧ -	побічні електромагнітні випромінювання і наведення
ППЧ - ППС -	персональна електронно-обчислювальна машина
РЕЗ - РЛС -	прилад нічного бачення
СКУД - ТЗІ -	шдсилювач низької частоти
ТТХ -	підсилювач ПРОМІЖНОЇ частоти
	пульт централізованого спостереження
	радіоелектронний засіб
	радіолокаційна станція
	система контролю управління доступом
	ТЕХНІЧНИЙ захист інформації
	тактико-технічна характеристика

Англомовні

	ACOUSTic INTelligence
	Domain Name System
	Code Division Multiple Access
	Charge-Coupled Device
	COMmunications INTelligence
	Estimate of Adversary Sequence Interruption
ACOUSINT -	Enhanced Data rates for Global Evolution
DNS - CDMA -	ELectronic INTelligence
CCD - COMINT	International Organization for Standardization
- EASI - EDGE -	Metal Insulator-Semiconductor Field-Effect Transistor
ELINT - ISO -	NUCclear INTelligence
MISFET -	RADar INTelligence
NUCINT -	Wired Equivalent Privacy
RADINT - WEP	Wireless Local Area Network
- WLAN -	Wireless Metropolitan Area Networks
WMAN - WPA -	Wi-Fi Protected Access
WPAN -	Wireless Personal Area Network

Розділ 1

Системний підхід до технічного захисту інформації

1.1. Основні положення системного підходу до технічного захисту інформації

Сформувати уявлення про комплекс завдань щодо побудови системи технічного захисту Інформації, методів, заходів і засобів щодо її реалізації на об'єктах інформаційної діяльності організації найбільш доцільно на основі системного підходу [3; 26].

Системний підхід [systems approach] — це дослідження об'єкта або процесу за допомогою моделі, званою системою. Цей підхід передбачає найвищий рівень опису об'єкта дослідження — системний. Найнижчим рівнем є рівень опису параметрів об'єкта — параметричний. Між ними розташовуються структурний і функціональний рівні (рис. 1.1).

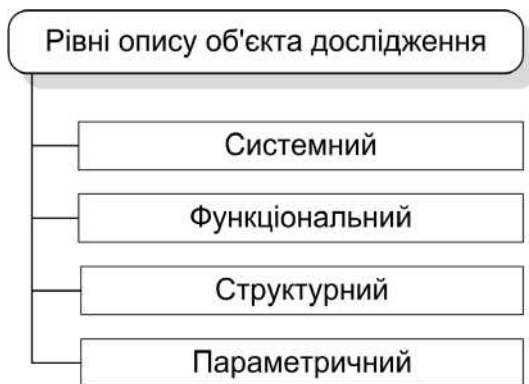


Рис. 1.1. Рівні опису об'єкта

Сутність системного підходу полягає в наступному:

- СУКУПНІСТЬ сил і засобів, ЯКІ забезпечують вирішення завдання, представляється у вигляді моделі, званою системою; система описується сукупністю параметрів;
- будь-яка система розглядається як підсистема більш складної системи, що впливає на структуру і функціонування розглянутої системи;
- будь-яка система має ієрархічну структуру, елементами і зв'язками якої не можна нехтувати без достатніх підстав;
- при аналізі системи необхідний облік зовнішніх і внутрішніх факторів, що впливають, прийняття рішень на основі частини з них без розгляду інших може привести до невірних результатів;
- властивості системи перевищують суму властивостей її елементів за рахунок якісно нових властивостей, відсутніх у її елементів — системних властивостей.

Ефективність реалізації системного підходу на практиці залежить від уміння фахівця виявляти і об'єктивно аналізувати все різноманіття факторів і зв'язків досить складного об'єкта дослідження, яким є, наприклад, організація як об'єкт захисту.

Необхідною умовою такого вміння є наявність у фахівця так званого системного мислення, що формується в результаті відповідного навчання та практики вирішення завдань, що слабо формалізуються.

Системне мислення [systems thmkmng] — це форма мислення, що характеризує здатність людини на несвідомому рівні вирішувати завдання дедуктивними методами. Ці методи стосовно до технічного захисту інформації передбачають:

- чітку постановку задачі, що включає визначення тематичних питань інформації та її джерел як об'єктів захисту, виявлення загроз цій інформації та формулювання цілей і завдань захисту інформації;
- розробку принципів і шляхів вирішення завдання;
- розробку методів вирішення завдань;
- створення програмного, технічного та методичного забезпечення вирішення завдань.

Системне мислення — це найважливіша якість не тільки фахівця із захисту інформації, а й будь-якого організатора і керівника. Якщо керівник не може швидко виявити фактори, що впливають на те чи інше рішення, і оцінити їх вагу, то невраховані або необґрунтовано відкинуті фактори постійно будуть про себе нагадувати. Такий керівник перетворюється на борця з ним же створюваними проблемами.

Якщо системний підхід характеризує концептуальні погляди на шляхи вирішення завдань, що слабо формалізуються, то основу їх вирішення становить системний аналіз.

Системний аналіз [system analysis] — 1) Аналіз об'єкта дослідження як сукупності елементів, що утворюють систему. У наукових дослідженнях він передбачає оцінку поведінки об'єкта як системи з усіма факторами, які впливають на його функціонування. Системний аналіз можна здійснювати у відповідності до етапів системного аналізу. Кінцевим результатом системного аналізу є побудова моделі системи і розробка пропозицій з її удосконалення або зміни. 2) Аналіз призначення системи, яку передбачається проектувати, і встановлення множини вимог, яким вона повинна відповідати. Єдиної методики системного аналізу у наукових дослідженнях поки що немає. У практиці досліджень він застосовується з використанням таких методик:

- процедур теорії дослідження операцій, яка дає змогу дати кількісну оцінку об'єктам дослідження;
- аналізу систем дослідження об'єктів в умовах невизначеності;
- системотехніки, яка включає проектування і синтез складних систем у процесі дослідження їхнього функціонування.

Відповідно до вимог системного підходу сукупність взаємопов'язаних елементів, функціонування яких спрямоване на забезпечення безпеки інформації, утворює систему захисту інформації.

Такими елементами є люди, інженерні конструкції і технічні засоби, що забезпечують захист інформації незалежно від їх приналежності до інших систем.

Ядро системи захисту утворюють сили і засоби, основними

функціями яких є забезпечення інформаційної безпеки. Однак вони становлять лише частину сил і засобів системи захисту інформації.

Наприклад, в систему захисту інформації входять не тільки структурні підрозділи (служба безпеки, відділ режиму і секретності 1-й відділ тощо), призначені для захисту інформації, але й всі співробітники організації, зобов'язані в міру своєї відповідальності забезпечувати захист інформації. Отже, вони також є елементами системи захисту інформації організації. І якщо який-небудь співробітник організації порушить правила поведінки з секретними документами, то можливий величезний збиток, незважаючи на бездоганну роботу інших елементів системи захисту.

Отже, структура (елементи та їх взаємозв'язок) системи захисту інформації держави, відомства, організації пронизує структуру держави, відомства, організації.

1.2. Цілі, завдання і ресурси системи захисту інформації

Цілі являють собою очікувані результати функціонування системи захисту інформації, а завдання те, що треба зробити для того, щоб система могла забезпечити досягнення поставлених цілей (рис. 1.2) [26].

Можливість вирішення завдань залежить від ресурсу, що виділяється на захист інформації.

Ресурс включає в себе людей, що вирішують завдання захисту інформації, фінансові, технічні та інші засоби, що витрачаються на захист інформації.

Входами системи захисту інформації є загрози інформації, а виходами — заходи, які треба застосувати для запобігання реалізації загроз або зниження їх до допустимого рівня.

Нарешті, заходи, дії і технології, що визначають заходи захисту, відповідні загрозам, утворюють процес.

Основною метою технічного захисту інформації є забезпечення її безпеки, при якій ризик зміни, знищення або розкрада-