

В.М. Богуш
О.К. Юдін

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

WWW.MK-PRESS.COM

ББК 32.973

Б74

УДК 355.40

Рецензенти:

- Академік Академії зв'язку України, академік Міжнародної академії інформатизації асоційованого члену ООН, завідувач кафедрою УДАЗТ, д.т.н., професор Поляков П.Ф.
- Професор кафедри організації розслідування злочинів НАВСУ, к.ю.н., доц., полковник міліції Біленчук П.Д.

Рекомендовано Міністерством освіти і науки України як навчальний посібник за напрямом 1601 "Інформаційна безпека"

Богуш В. М., Юдін О. К.

Б74 Інформаційна безпека держави. — К.: "МК-Прес", 2005. — 432с., іл.

ISBN 966-8806-05-0

В книзі наведена систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. Визначене місце інформаційної безпеки в загальній системі національної безпеки, вплив дестабілізуючих факторів та інформаційних загроз на безпеку особистості, суспільства та держави, основи інформаційного протистояння та інформаційної боротьби, зміст і форми психологічних операцій та інформаційно-психологічної безпеки, а також загальні підходи до забезпечення безпеки інформаційних технологій. Детально розглядаються основні положення інформаційної безпеки України, способи та форми її забезпечення.

Призначається для студентів, що навчаються за усіма спеціальностями освітнього напрямку "Інформаційна безпека".

ББК 32.973

**Богуш Володимир Михайлович
Юдін Олександр Костянтинович**

Інформаційна безпека держави

Головний редактор: Ю. О. Шпак

Підписано до друку 06.09.2005. Формат 60 × 90 1/16. Папір газетний. Друк офсетний.

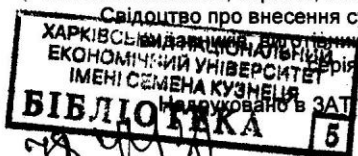
Ум. друк. л. 27. Обл.-вид. л. 25,8. Тираж 1000 екз. Замовлення № 5-1523

ПП Савченко Л.О., Україна, м.Київ, тел./ф.: (044) 517-73-77; e-mail: info@mk-press.com.

Свідчення про внесення суб'єкта видавничої справи до Державного реєстру

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Державна реєстрація ДК №51582 від 28.11.2003 р.



Надруковано в ЗАТ "ВІПОЛ". 03151, м. Київ, вул. Волинська, 60

ISBN 966-8806-05-0

© Богуш В. М., Юдін О. К. текст, ілюстрації, 2005

© "МК-Прес", оформлення, дизайн обкладинки, 2005

ЗМІСТ

Вступ.....	12
Перелік аббревіатур і скорочень	17
Українська мова	17
Англійська мова	17
Скорочення	18
Частина I. Сучасні основи інформаційної безпеки держави .19	
Розділ 1. Основи національної безпеки держави.....	20
1.1. Основні поняття національної безпеки	20
1.1.1. Визначення національної безпеки	20
1.1.2. Основні категорії теорії національної безпеки	21
Визначення теорії національної безпеки та перелік її основних категорій.....	21
Концепція національної безпеки.....	22
Національні інтереси держави	23
Загрози національній безпеці держави.....	23
Об'єкти національної безпеки	26
Принципи забезпечення національної безпеки	26
Методи та засоби забезпечення національної безпеки	26
Характеристики національної безпеки.....	27
1.1.3. Фактори та засоби забезпечення національної безпеки.....	27
Фактори забезпечення національної безпеки	27
Основні засоби забезпечення національної безпеки.....	29
1.2. Характеристика основних видів національної безпеки	30
1.2.1. Рівні та види національної безпеки	30
1.2.2. Політична безпека	31
1.2.3. Економічна безпека	32
1.2.4. Соціальна безпека	32
1.2.5. Воєнна безпека	33
1.2.6. Екологічна безпека	33
1.2.7. Науково-технологічна безпека	34
1.2.8. Забезпечення безпеки в інформаційній сфері.....	34
1.3. Система забезпечення національної безпеки в Україні.....	35
1.3.1. Визначення системи забезпечення національної безпеки	35
1.3.2. Функції системи забезпечення національної безпеки.....	36
1.3.3. Повноваження суб'єктів забезпечення національної безпеки	37
Розділ 2. Основні положення інформаційної безпеки.....	39
2.1. Поняття інформаційної безпеки.....	39
2.1.1. Визначення інформаційної безпеки.....	39
2.1.2. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері	40
2.1.3. Об'єкти та суб'єкти інформаційної безпеки	41
2.1.4. Види інформаційної безпеки.....	41
2.1.5. Концепція інформаційної безпеки держави.....	41

2.2. Загрози інформаційній безпеці	42
2.2.1. Дестабілізуючі фактори інформаційної безпеки	42
2.2.2. Класифікація загроз інформаційній безпеці	43
Ієрархічна класифікація загроз інформаційній безпеці	44
2.2.3. Джерела загроз інформаційній безпеці	45
Джерела загроз інформаційній безпеці особистості	45
Джерела загроз інформаційній безпеці суспільства	46
Джерела загроз інформаційній безпеці держави	47
2.3. Методи і засоби забезпечення інформаційної безпеки	48
2.3.1. Основні принципи забезпечення інформаційної безпеки	48
2.3.2. Система забезпечення інформаційної безпеки держави	50
2.3.3. Основні форми і способи забезпечення інформаційної безпеки держави	50
Розділ 3. Основи інформаційного протиборства	53
3.1. Основні поняття інформаційного протиборства	53
3.1.1. Визначення поняття “інформаційне протиборство”	53
3.1.2. Інформаційна війна	53
3.1.3. Інформаційний тероризм	55
3.1.4. Інформаційна злочинність	56
3.1.5. Інформаційне протиборство як форма забезпечення інформаційної безпеки	56
3.2. Основні поняття інформаційної війни	57
3.2.1. Визначення інформаційної війни	57
3.2.2. Концепція інформаційної війни	58
3.2.3. Органи інформаційної війни	58
3.3. Основні форми інформаційної війни	59
3.3.1. Визначення форм інформаційної війни	59
3.3.2. Основні форми інформаційної війни на державному рівні	59
3.3.3. Основні форми інформаційної війни на воєнному рівні	61
3.3.4. Необхідні умови для досягнення інформаційної переваги	63
3.4. Інформаційна зброя в інформаційній війні	64
3.4.1. Визначення, особливості та сфера застосування інформаційної зброї	64
3.4.2. Інформаційна зброя воєнного застосування	65
3.4.3. Інформаційна зброя воєнного та невоєнного застосування	66
Засоби ураження комп'ютерних інформаційних систем	66
Засоби ураження (впливу) на людей та їхню психіку	75
3.4.4. Особливості, що характеризують основні риси застосування інформаційної зброї	76
3.5. Основи теорії інформаційної боротьби	77
3.5.1. Зміст теорії інформаційної боротьби	77
Основні визначення теорії інформаційної боротьби	77
Закони та закономірності інформаційної боротьби	80
Принципи інформаційної боротьби	81
3.5.2. Заходи інформаційної боротьби	82
3.5.3. Способи інформаційної боротьби	85
Визначення способів інформаційної боротьби	85
Наступальні способи інформаційної боротьби	85

Оборонні способи інформаційної боротьби	88
3.5.4. Форми ведення інформаційної боротьби	88
3.5.5. Методологія оцінки ефективності інформаційної боротьби	91
Розділ 4. Психологічна війна та інформаційно-психологічна	
безпека держави.....	94
4.1. Основні поняття психологічної війни	94
4.1.1. Поняття психологічної війни	94
4.1.2. Цілі та завдання психологічної війни	95
4.1.3. Види та закономірності психологічних впливів	97
Види психологічних впливів	97
Механізм реалізації психологічного впливу	99
Закономірності психологічного впливу	100
4.2. Основи психологічних операцій	102
4.2.1. Зміст психологічних операцій	102
4.2.2. Ефективність психологічного впливу в психологічній	
операції	104
Сприйняття психологічного впливу	105
Засвоєння психологічного впливу	107
4.2.3. Органи та засоби проведення психологічних операцій	108
4.3. Технології психологічної війни	109
4.3.1. Основні характеристики об'єктів психологічної війни	109
Визначення об'єктів психологічної війни	109
Національно-психологічні особливості об'єктів психологічної	
війни	110
Індивідуально-особистісні особливості об'єктів психологічної	
війни	110
Групова належність об'єктів психологічної війни	111
Особливості морально психологічного стану об'єктів	
психологічної війни	112
4.3.2. Методика вивчення об'єктів психологічної війни	113
Основні принципи вивчення об'єктів психологічної війни	113
Процес вивчення об'єктів психологічної війни	114
Основні методи вивчення об'єктів психологічної війни	115
4.3.3. Форми психологічної війни	117
Усне мовлення	118
Психологічний вплив друкованими засобами	120
Психологічний вплив образотворчими засобами	124
Психологічний вплив через радіо та телебачення	124
4.4. Методи впливу в психологічній війні	126
4.4.1. Переконуючий психологічний вплив	126
Визначення та характеристика переконуючого психологічного	
впливу	126
Вплив джерела інформації	127
Вплив змісту інформації	128
Вплив ситуації інформування	131
Основні принципи здійснення переконуючого впливу	132
4.4.2. Навіюючий психологічний вплив	134

Визначення, характеристика та класифікація навіюючих впливів.....	134
Навіюваність.....	136
Опірність навіюванню.....	137
Модель навіюючого впливу.....	138
Основні способи та прийоми специфічного навіювання.....	139
Основні способи та прийоми неспецифічного навіювання.....	140
4.5. Особливі способи та прийоми психологічної війни.....	143
4.5.1. Дезінформування.....	143
4.5.2. Маніпулювання свідомістю.....	144
4.5.3. Розповсюдження чуток та міфів.....	146
4.6. Основи забезпечення інформаційно-психологічної безпеки держави.....	148
4.6.1. Основні положення.....	148
4.6.2. Основи інформаційно-психологічної безпеки держави.....	150
Основні поняття інформаційно-психологічної безпеки.....	150
Принципи безпеки у психосфері.....	152
Потенційні джерела загроз.....	152
Загрози інформаційно-психологічній безпеці держави.....	153
Основні завдання державної політики в галузі забезпечення інформаційно-психологічної безпеки.....	155
Об'єкти інформаційно-психологічного захисту.....	155
4.6.3. Основні напрями діяльності державної системи забезпечення інформаційно-психологічної безпеки.....	156
Функції державної системи забезпечення інформаційно-психологічної безпеки.....	156
Структура державної системи забезпечення інформаційно-психологічної безпеки.....	157
Сили та засоби інформаційно-психологічної безпеки.....	157
Ліцензування в галузі забезпечення інформаційно-психологічної безпеки.....	158
Сертифікація засобів і методів неусвідомлюваного інформаційного впливу.....	159
Експертиза з метою забезпечення інформаційно-психологічної безпеки (психоекологічна експертиза).....	159
Контроль за забезпеченням інформаційно-психологічної безпеки.....	160
Розділ 5. Основи державної інформаційної політики.....	161
5.1. Основні положення державної інформаційної політики.....	161
5.1.1. Визначення державної інформаційної політики.....	161
5.1.2. Поняття про програму входження держави в інформаційне суспільство.....	163
5.2. Основні напрями національної інформаційної політики.....	163
5.2.1. Основні напрями національної інформаційної політики у сфері суспільних відносин.....	164
5.2.2. Основні напрями національної інформаційної політики в економічній сфері.....	164

5.2.3. Основні напрями національної інформаційної політики в організаційній сфері.....	165
5.3. Державна політика забезпечення інформаційної безпеки.....	165
5.3.1. Основні поняття політики забезпечення інформаційної безпеки держави.....	165
5.3.2. Основні загрози інформаційній безпеці держави.....	167
5.3.3. Організаційний напрям протидії загрозам у сфері інформаційної безпеки.....	167
5.3.4. Захист прав і свобод людини та громадянина.....	168
5.3.5. Розвиток матеріально-технічної бази системи інформаційної безпеки особи, держави та суспільства.....	169
5.3.6. Науково-практична робота щодо забезпечення інформаційної безпеки.....	169
5.3.7. Вдосконалення нормативно-правової бази забезпечення загальнодержавної системи інформаційної безпеки.....	170
Частина II. Основи безпеки інформаційних технологій.....	171
Розділ 6. Інформаційні системи та технології як об'єкти інформаційної безпеки.....	172
6.1. Види та властивості інформації як предмета захисту.....	172
6.1.1. Інформація та дані.....	172
6.1.2. Форми адекватності інформації.....	173
6.1.3. Міри інформації.....	174
Класифікація мір.....	174
Синтаксична міра інформації.....	174
Семантична міра інформації.....	176
Прагматична міра інформації.....	177
6.1.4. Якість інформації.....	177
6.1.5. Основні властивості інформації як предмета захисту.....	179
Доступність інформації.....	179
Цінність, цілісність і конфіденційність інформації.....	180
Цінність і ціна інформації.....	181
Залежність цінності інформації від часу.....	182
Вплив копіювання на ціну інформації.....	183
Види інформації, що підлягають захисту.....	183
6.2. Інформаційні системи як об'єкти захисту.....	186
6.2.1. Загальні відомості про інформаційні системи.....	186
Визначення інформаційної системи.....	186
Типові процеси в інформаційній системі.....	187
6.2.2. Структура інформаційної системи.....	188
Підсистеми забезпечення інформаційної системи.....	188
Інформаційне забезпечення.....	189
Технічне забезпечення.....	190
Математичне і програмне забезпечення.....	191
Організаційне забезпечення.....	192
Правове забезпечення.....	192
6.2.3. Класифікація інформаційних систем.....	193
Класифікація за ступенем автоматизації.....	193

Класифікація інформаційних систем за характером використання інформації.....	194
Класифікація інформаційних систем за сферою застосування.....	194
6.2.4. Основні характеристики інформаційної системи як об'єкта захисту.....	195
6.3. Інформаційні технології та проблеми їхньої безпеки.....	197
6.3.1. Визначення інформаційної технології.....	197
6.3.2. Співвідношення інформаційної технології та інформаційної системи.....	198
6.3.3. Класифікація та види інформаційних технологій.....	198
Традиційна та нова інформаційна технологія.....	198
Інформаційна технологія управління.....	199
Програмна інформаційна технологія.....	200
Інформаційна технологія доступу до ресурсів.....	201
Основні тенденції розвитку інформаційних технологій.....	201
6.3.4. Основні проблеми безпеки інформаційних технологій.....	203
Розділ 7. Основи безпеки інформаційних ресурсів.....	207
7.1. Загрози безпеці інформації та інформаційних ресурсів.....	207
7.1.1. Загальні положення.....	207
7.1.2. Збитки як категорія класифікації загроз.....	208
7.1.3. Класифікація загроз безпеці інформації.....	209
7.1.4. Класифікація джерел загроз.....	210
7.1.5. Ранжирування джерел загроз.....	213
7.1.6. Класифікація уразливостей безпеці.....	216
7.1.7. Ранжирування уразливостей.....	217
7.1.8. Класифікація актуальних загроз.....	219
7.2. Основні напрями забезпечення безпеки інформації та інформаційних ресурсів.....	219
7.2.1. Основні визначення.....	219
7.2.2. Правовий захист.....	220
7.2.3. Організаційний захист.....	227
Загальні положення організаційного захисту.....	227
Особливості організаційного захисту комп'ютерних інформаційних систем та мереж.....	229
Служба, захисту інформації.....	230
7.2.4. Інженерно-технічний захист.....	233
Загальні положення інженерно-технічного захисту.....	233
Фізичні засоби захисту.....	234
Системи контролю доступу.....	239
Апаратні засоби захисту.....	241
Програмні засоби захисту.....	244
Криптографічні засоби захисту.....	249
7.3. Архітектура захисту інформації в мережах телекомунікацій.....	254
7.3.1. Архітектура відкритих систем.....	254
7.3.2. Загрози в архітектурі відкритих мереж.....	257
7.3.3. Процедури захисту.....	258
7.3.4. Сервісні служби захисту.....	259
7.3.5. Реалізація захисту.....	262

Розділ 8. Критерії безпеки інформаційних технологій	264
8.1. Загальні відомості про вимоги та критерії оцінки безпеки інформаційних технологій	264
8.1.1. Основні поняття про стандарти інформаційної безпеки	264
8.1.2. Критерії безпеки комп'ютерних систем	264
8.1.3. Європейські критерії безпеки інформаційних технологій	265
8.1.4. Федеральні критерії безпеки інформаційних технологій	266
8.1.5. Канадські критерії безпеки комп'ютерних систем	267
8.2. Основні положення загальних критеріїв безпеки інформаційних технологій	268
8.2.1. Мета розробки, основні положення та склад "Загальних критеріїв"	268
8.2.2. Потенційні загрози безпеці та типові завдання захисту	270
8.2.3. Політика безпеки	271
8.2.4. Продукт інформаційних технологій	272
8.2.5. Профіль захисту	272
8.2.6. Проект захисту	275
8.3. Функціональні вимоги до засобів захисту	279
8.3.1. Загальна характеристика функціональних вимог безпеки	279
8.3.2. Класи функціональних вимог безпеки	282
Аудит	282
Захист інформації	283
Ідентифікація та автентифікація	286
Керування безпекою	288
Контроль доступу до системи	289
Контроль за використанням ресурсів	290
Конфіденційність роботи в системі	290
Криптографія	291
Надійність засобів захисту	292
Причетність до прийому/передавання	294
Пряма взаємодія	295
8.4. Вимоги гарантій засобів захисту	295
8.4.1. Загальна характеристика вимог гарантій безпеки	295
8.4.2. Класи вимог гарантій безпеки	297
Керування проектом	297
Дистрибуція	298
Розробка	298
Документація	300
Процес розробки	300
Тестування	301
Аналіз захисту	302
8.4.3. Рівні гарантій безпеки	303
Визначення рівнів гарантій	303
Функціональне тестування	303
Структурне тестування	304
Методичне тестування та перевірка	306
Методична розробка, тестування та аналіз	307
Напівформальні методи розробки та тестування	309

Напівформальні методи верифікації розробки та тестування ..	310
Формальні методи верифікації розробки та тестування	312
8.5. Шляхи і перспективи застосування “Загальних критеріїв”	314
Розділ 9. Основи управління інформаційною безпекою	316
9.1. Стандарти менеджменту інформаційної безпеки та їх основні положення	316
9.2. Політика інформаційної безпеки організації	319
9.2.1. Визначення політики інформаційної безпеки організації ..	319
9.2.2. Концепція інформаційної безпеки в організації	321
9.2.3. Аналіз та оцінка ризиків	322
9.3. Основні правила інформаційної безпеки організації	323
9.3.1. Правила побудови системи забезпечення інформаційної безпеки	323
Вибір варіанту побудови системи забезпечення інформаційної безпеки	323
Оцінювання витрат на СЗІБ	324
Визначення вимог до заходів, методів та засобів захисту	324
Вибір основних рішень з забезпечення безпеки інформації ..	324
9.3.2. Організація проведення відновлювальних робіт і забезпечення неперервного функціонування об'єктів організації та організації в цілому	326
9.3.3. Правила розмежування доступу користувачів та процесів до ресурсів інформаційної сфери організації	327
9.3.4. Документальне оформлення політики безпеки	328
9.4. Система менеджменту інформаційної безпеки та її оцінка	329
Частина III. Забезпечення інформаційної безпеки України ..331	
Розділ 10. Інформаційна безпека України	332
10.1. Національні інтереси України в інформаційній сфері та шляхи їх забезпечення	332
10.2. Загрози інформаційній безпеці України	335
10.3. Джерела загроз інформаційній безпеці України	338
10.4. Стан інформаційної безпеки України	340
10.5. Завдання із забезпечення інформаційної безпеки України ..	341
Розділ 11. Методи та заходи забезпечення інформаційної безпеки України	343
11.1. Загальні методи забезпечення інформаційної безпеки України	343
11.2. Особливості забезпечення інформаційної безпеки України в різних сферах громадського життя	345
11.2.1. Забезпечення інформаційної безпеки України в сфері економіки	346
11.2.2. Забезпечення інформаційної безпеки України в сфері внутрішньої політики	348
11.2.3. Забезпечення інформаційної безпеки України в сфері зовнішньої політики	349
11.2.4. Забезпечення інформаційної безпеки України у галузі науки та техніки	352

11.2.5. Забезпечення інформаційної безпеки України у сфері духовного життя.....	354
11.2.6. Забезпечення інформаційної безпеки України у загально-державних інформаційних і телекомунікаційних системах.....	356
11.2.7. Забезпечення інформаційної безпеки України у сфері оборони	359
11.2.8. Забезпечення інформаційної безпеки України у правоохоронній і судовій сферах.....	362
11.2.9. Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій	363
11.3. Міжнародне співробітництво України в галузі забезпечення інформаційної безпеки	365
Розділ 12. Система та політика забезпечення інформаційної безпеки України.....	367
12.1. Основні функції системи забезпечення інформаційної безпеки України	367
12.2. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України	368
12.3. Основні положення політики забезпечення інформаційної безпеки України	371
12.4. Першочергові заходи щодо реалізації політики забезпечення інформаційної безпеки України	373
Словник додаткових термінів і понять.....	375
Б.....	376
В.....	378
Г.....	381
Д.....	382
Е.....	385
З.....	385
І.....	388
К.....	389
Л.....	392
М.....	393
Н.....	396
О.....	396
П.....	398
Р.....	403
С.....	405
Т.....	408
У.....	409
Ф.....	410
Х.....	410
Ц.....	410
Ч.....	410
Ш.....	411
Я.....	411
Показчик ключових термінів і понять	412
Бібліографія.....	427