

351.746.1(477)
Ф66

В. В. Домарєв

СИСТЕМА СИТУАЦІЙНОГО УПРАВЛІННЯ



Теорія, методологія, рекомендації

В. В. Домарєв

**СИСТЕМА
СИТУАЦІЙНОГО УПРАВЛІННЯ**

Теорія, методологія, рекомендації

Київ
Знання України
2017

УДК [004.056+007.51](477)

Д66

Домарєв В. В.

Д66 Система ситуаційного управління: Теорія, методологія, рекомендації / В. В. Домарєв. - Київ : Знання України, 2017. - 347 [1] с. - Бібліогр.: с. 346-347.

ISBN 978-966-316-414-4

Книга присвячена питанням удосконалення процесів гарантування національної безпеки шляхом створення та впровадження системи ситуаційного управління - системи реагування на кризові ситуації. Методологія ситуаційного управління розглядається як складова системи забезпечення національної безпеки України. Запропоновано вирішення проблеми неузгодженості експертно-аналітичного забезпечення процесів прийняття управлінських рішень на державному рівні шляхом застосування єдиної методики обробки інформаційних потоків. Висвітлено теоретичні і практичні питання реалізації системного та процесного підходу до створення нових методів ситуаційного управління безпекою. Розраховано на широке коло читачів.

УДК [004.056+007.51](477)

ISBN 978-966-316-414-4

© Домарєв В. В., 2017

*ПРИСВЯЧУЮ
моїй родині та однодумцям, які підтримували мене
морально та матеріально під час роботи над книгою.*

*СПОДІВАЮСЬ,
що наші патріотичні бажання
оптимізувати процеси управління безпекою
стануть у пригоді для покращення могутності
нашої держави та знайдуть практичне використання.*

*ЩИРО ДЯКУЮ
друзям, колегам та знайомим, які без зайвого пафосу
забезпечили можливість видання цієї книги.
Також вдячний опонентам і недругам, які своєю
протидією та небажанням вислухати спонукали мене
до пошуку будь-яких можливостей довести
особисте бачення проблем ситуаційного управління
та висловити думки щодо можливих шляхів їх вирішення.*

Зміст

ПЕРЕЛІК СКОРОЧЕНЬ.....	12
1. ВСТУП: ВИПАДКОВА ЗАКОНОМІРНІСТЬ АБО ЗАКОНОМІРНА ВИПАДКОВІСТЬ.....	14
1.1. Методологія ситуаційного управління - складова процесів гарантування національної безпеки України.....	15
1.2. Актуальність впровадження систем ситуаційного управління.....	16
1.3. Безпека інформаційних технологій - проблемна складова ССУ.....	17
1.4. Наукові аспекти проектування багаторівневих систем ситуаційного управління.....	19
1.5. Практична цінність запропонованих науково-методичних підходів	20
1.6. Висновки.....	22
2. КОНЦЕПТУАЛЬНО-МЕТОДОЛОГІЧНІ ПІДХОДИ ГАРАНТУВАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ.....	24
2.1. Актуальність оновлення системи забезпечення національної безпеки.....	26
2.2. Основні категорії, що складають зміст теорії національної безпеки.....	28
2.3. Базові концептуально-методологічні підходи щодо гарантування національної безпеки.....	29
2.4. Визначення системи забезпечення національної безпеки.....	31
2.5. Основні функції та завдання системи забезпечення національної безпеки.....	35
2.6. Висновки.....	36
3. УНІВЕРСАЛЬНА ЛОГІКО-ЛІНГВІСТИЧНА МАТРИЧНА МОДЕЛЬ БЕЗПЕКИ.....	38
3.1. Актуальність матричної моделі національної безпеки.....	42
3.2. Типова логіко-лінгвістична матрична модель безпеки.....	44
3.3. Матрична модель системи забезпечення національної безпеки.....	46
3.4. Компонента «СКЛАДОВІ» логіко-лінгвістичної матричної моделі безпеки.....	48
3.5. Компонента «ФУНКЦІЇ» логіко-лінгвістичної матричної моделі безпеки.....	48
3.6. Компонента «СФЕРИ» логіко-лінгвістичної матричної моделі безпеки.....	49
3.7. Універсальна матриця системи забезпечення національної безпеки.....	53
3.8. Моделювання ситуацій та процесів реагування СЗНБ.....	57
3.9. Системно-процесний підхід матричної моделі СЗНБ.....	58
3.10. Використання теорії нечіткості для моделювання процесів гарантування національної безпеки.....	58
3.11. Висновки.....	60
4. СКЛАДОВІ ЛОГІКО-ЛІНГВІСТИЧНОЇ МОДЕЛІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ.....	62
4.1. Законодавча та нормативно-методична база системи забезпечення національної безпеки.....	63

4.1.1.	<i>Місце процесів формування законодавчої бази СЗНБ у матриці національної безпеки</i>	67
4.1.2.	<i>Структура керівних документів СЗНБ</i>	68
4.2.	Структура органів (суб'єктів) національної безпеки.....	70
4.2.1.	<i>Місце процесів формування структури органів СЗНБ у матриці національної безпеки</i>	72
4.2.2.	<i>Суб'єкти СЗНБ</i>	73
4.2.3.	<i>Сектор безпеки і оборони України</i>	75
4.3.	Заходи політики гарантування національної безпеки.....	77
4.4.	Комплекси засобів, форм та методів гарантування національної безпеки.....	83
4.5.	Висновки.....	87
5.	ФУНКЦІЇ ЛОГІКО-ЛІНГВІСТИЧНОЇ МОДЕЛІ СЗНБ.....	88
5.1.	Визначення переліку об'єктів небезпеки.....	90
5.1.1.	<i>Місце процесів визначення об'єктів (ресурсів) небезпеки у матриці національної безпеки</i>	91
5.1.2.	<i>Об'єкти національної безпеки</i>	94
5.2.	Приклад формування переліку об'єктів, важливих для національної безпеки.....	94
5.3.	Оцінка, аналіз, прогнозування загроз національної безпеки.....	96
5.3.1.	<i>Місце процесів виявлення та оцінка загроз (впливів) у матриці національної безпеки</i>	98
5.3.2.	<i>Загрози національній безпеці держави</i>	98
5.4.	Приклад формування переліку загроз у сферах національної безпеки.....	99
5.5.	Аналіз ризиків національної безпеки.....	102
5.5.1.	<i>Місце процесів оцінки ризиків у матриці національної безпеки</i>	104
5.5.2.	<i>Логіко-лінгвістична матрична модель оцінки ризику</i>	105
5.6.	Формування вимог (характеристик) СЗНБ.....	106
5.7.	Ухвалення управлінських рішень з питань гарантування безпеки.....	109
5.7.1.	<i>Місце процесів прогнозування, планування та ухвалення управлінських рішень у матриці національної безпеки</i>	111
5.7.2.	<i>Система стратегічного аналізу і прогнозування у сферах гарантування національної безпеки</i>	113
5.7.3.	<i>Процес експертно-аналітичної підтримки ухвалення управлінських рішень</i>	115
5.8.	Реалізація заходів гарантування національної безпеки та контроль виконання рішень.....	117
5.9.	Оцінка ефективності СЗНБ України.....	121
5.9.1.	<i>Місце процесів оцінки ефективності СЗНБ у матриці національної безпеки</i>	123
5.9.2.	<i>Методи оцінки показників ефективності СЗНБ</i>	124
5.9.3.	<i>Оцінка стану національної безпеки</i>	125
5.9.4.	<i>Оцінка ефективності функціонування СЗНБ</i>	126
5.9.5.	<i>Система показників ефективності СЗНБ</i>	127
5.9.6.	<i>Оцінка ефективності СЗНБ з використанням методів нечіткої логіки</i>	132
5.10.	Висновки.....	136

6.	ТЕОРІЯ СИТУАЦІЙНОГО УПРАВЛІННЯ.....	138
6.1.	Визначення ситуаційного управління.....	140
6.2.	Визначення управлінської ситуації.....	142
6.3.	Принципи ситуаційного управління.....	143
6.4.	Сучасні технології ситуаційного управління.....	144
6.5.	Системно-процесний підхід у ситуаційному управлінні.....	146
6.6.	Методологія системно-процесного підходу.....	148
6.7.	Методологія ситуаційного аналізу.....	149
	6.7.1. <i>Етапи ситуаційного аналізу</i>	150
	6.7.2. <i>Методи ситуаційного аналізу</i>	151
6.8.	Висновки.....	152
7.	СИСТЕМА СИТУАЦІЙНОГО УПРАВЛІННЯ.....	154
7.1.	Поняття та визначення системи ситуаційного управління.....	159
	7.1.1. <i>Ситуаційне управлінське рішення</i>	161
	7.1.2. <i>Типи кризових ситуацій</i>	162
	7.1.3. <i>Етапи життєвого циклу ССУ</i>	162
	7.1.4. <i>Методи та засоби забезпечення живучості ССУ</i>	163
7.2.	Системно-процесний підхід до ситуаційного управління.....	164
7.3.	Мета функціонування ССУ.....	165
7.4.	Функції ССУ.....	166
7.5.	Завдання ССУ.....	167
7.6.	Загальні вимоги до ССУ.....	169
7.7.	Ієрархічні рівні ССУ.....	170
	7.7.1. <i>Стратегічний рівень управління</i>	171
	7.7.2. <i>Галузевий рівень управління</i>	171
	7.7.3. <i>Регіональний рівень управління</i>	172
	7.7.4. <i>Оперативний рівень управління</i>	172
	7.7.5. <i>Комунікаційний рівень управління</i>	173
7.8.	Моніторинг стану національної безпеки як функція ССУ.....	175
7.9.	Актуальність розробки єдиної методології визначення переліку індикаторів стану національної безпеки.....	178
7.10.	Система індикаторів стану національної безпеки.....	178
7.11.	Приклад системи показників (індикаторів) стану національної безпеки.....	180
7.12.	Системно-процесний підхід до визначення показників стану націо- нальної безпеки.....	183
7.13.	Приклад аналітичної обробки інформації щодо загроз.....	185
7.14.	Нормативно-методичні документи ССУ.....	186
7.15.	Структура суб'єктів ССУ.....	188
7.16.	Організаційно-технічні заходи щодо створення ССУ.....	189
7.17.	Першочергові заходи щодо створення ССУ.....	191
7.18.	Очікувані результати від впровадження ССУ.....	192
7.19.	Проблеми створення ССУ.....	195
7.20.	Засоби ССУ.....	196
7.21.	Технології програмно-методичного комплексу ССУ.....	197
7.22.	Підсистема геопросторового аналізу і картографічного моделювання.....	200
7.23.	Підсистема відеоконференцз'язку.....	200
7.24.	Підсистема зовнішнього відеоспостереження.....	201

7.25.	Комплекси візуалізації.....	201
7.26.	Висновки.....	202
8.	СИТУАЦІЙНІ ЦЕНТРИ - ІНСТРУМЕНТ РЕАГУВАННЯ НА КРИЗОВІ СИТУАЦІЇ	204
8.1.	Досвід створення ситуаційних центрів.....	206
8.2.	Утворення єдиного інформаційно-аналітичного простору.....	207
8.3.	Характеристика ситуаційних центрів галузевого рівня.....	208
8.4.	Види ситуаційних центрів.....	209
8.5.	Режими роботи СЦ.....	210
8.6.	Основні функції та завдання СЦ.....	211
8.7.	Нормативно-методичні документи ситуаційних центрів.....	212
8.7.1.	Адміністративні документи СЦ.....	213
8.7.2.	Документи СЦ верхнього рівня.....	213
8.7.3.	Документи СЦ середнього рівня.....	214
8.7.4.	Документи СЦ нижнього рівня.....	214
8.7.5.	Нормативні документи СЦ щодо захисту інформації з обме- женим доступом.....	215
8.7.6.	Рекомендації щодо оформлення нормативно-методичних доку- ментів СЦ.....	215
8.8.	Приклад аналізу об'єктів та ресурсів критичної інфраструктури.....	216
8.9.	Висновки.....	220
9.	ЕКСПЕРТНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ СИТУАЦІЙНОГО УПРАВЛІННЯ.....	222
9.1.	Технології експертно-аналітичного забезпечення.....	224
9.2.	Зміст принципів експертно-аналітичної діяльності.....	225
9.3.	Робота з інформаційними потоками.....	226
9.4.	Завдання експертно-аналітичного забезпечення.....	227
9.5.	Аналітика як наука.....	228
9.6.	Методи експертно-аналітичної діяльності.....	229
9.6.1.	Метод аналогій.....	229
9.6.2.	Спостереження.....	229
9.6.3.	Метод вартість-ефективність.....	230
9.6.4.	Методи багатокритеріальної оцінки альтернатив.....	230
9.6.5.	Метод експертних оцінок.....	231
9.6.6.	Неформальні методи.....	231
9.7.	Мистецтво аналітичної роботи.....	232
9.8.	Прогнозування - процес синтезу знань.....	233
9.9.	Методика аналізу змісту тексту.....	234
9.10.	Методологія роботи з відкритими джерелами інформації.....	236
9.10.1.	Використання власних можливостей з обробки ЗМІ.....	236
9.10.2.	Аналітична обробка.....	237
9.11.	Підготовка довідок та проектів управлінських рішень.....	238
9.12.	Методичні рекомендації написання аналітичних документів.....	239
9.12.1.	Структура й логічна побудова документа.....	239
9.12.2.	Реферування.....	239
9.12.3.	Заголовок.....	240
9.12.4.	Основна ідея документа.....	240

9.12.5.	Структура аналітичної довідки.....	241
9.12.6.	Додаткові рекомендації щодо аналізу інформації.....	243
9.13.	Висновки.....	244
10.	УНІВЕРСАЛЬНИЙ БАГАТОЦІЛЬОВИЙ ПРОГРАМНО-МЕТОДИЧНИЙ КОМП- ЛЕКС СИТУАЦІЙНОГО УПРАВЛІННЯ БЕЗПЕКОЮ.....	246
10.1.	Актуальність впровадження універсального багатocільового ПМК ССУ.....	248
10.2.	Призначення та мета створення ПМК ССУ.....	249
10.3.	Модель даних ПМК ССУ.....	250
10.4.	Функціональні модулі ССУ.....	251
10.5.	Приклади програмних модулів ПМК.....	252
10.5.1.	Модуль «Моніторинг стану безпеки».....	252
10.5.2.	Модуль «Узагальнений аналіз».....	255
10.5.3.	Модуль «Оцінка ризиків».....	256
10.5.4.	Модуль «Завдання».....	257
10.5.5.	Модуль «Графіки» (візуалізації).....	259
10.5.6.	Модуль «Карта».....	260
10.5.7.	Модуль «Довідники».....	261
10.5.8.	Модуль «Документи».....	263
10.5.9.	Модуль «Пошук інформації».....	263
10.5.10.	Модуль «Бази даних».....	264
10.5.11.	Модуль «Ситуаційні оцінки».....	266
10.5.12.	Модуль безпеки інформаційних технологій.....	268
10.6.	Користувачі ПМК ССУ.....	269
10.6.1.	Типові завдання користувачів.....	269
10.6.2.	Навчання персоналу і користувачів ПМК ССУ.....	270
10.6.3.	Підрозділ забезпечення функціонування ПМК ССУ.....	271
10.7.	Висновки.....	272
11.	БЕЗПЕКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ СИТУАЦІЙНОГО УПРАВЛІННЯ.....	274
11.1.	Безпека інформаційних технологій як складова національної безпеки.....	276
11.2.	Завдання безпеки інформаційних технологій.....	277
11.3.	Безпека інформаційних технологій об'єктів критичної інфра- структури.....	277
11.4.	Тенденції розвитку сучасних методичних підходів щодо безпеки інформаційних технологій.....	278
11.5.	Актуальність впровадження систем управління інформаційною безпекою.....	280
11.6.	Система кібернетичної безпеки України.....	282
11.6.1.	Кіберзагрози.....	283
11.6.2.	Чинники посилення кіберзагроз.....	286
11.6.3.	Загрози втручання в роботу комп'ютерних мереж.....	286
11.6.4.	Суб'єкти системи кібербезпеки.....	287
11.6.5.	Функції та завдання системи кібербезпеки.....	287
11.6.6.	Розвиток безпечного, стабільного і надійного кібер- простору.....	289

11.6.7.	<i>Кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури</i>	290
11.6.8.	<i>Кіберзахист критичної інфраструктури</i>	291
11.6.9.	<i>Розвиток потенціалу сектора безпеки і оборони у сфері забезпечення кібербезпеки</i>	292
11.6.10.	<i>Боротьба з кіберзлочинністю</i>	294
11.7.	Процеси забезпечення живучості ССУ.....	295
11.8.	Система технічного захисту інформації ССУ.....	296
11.8.1.	<i>Загальні положення</i>	296
11.8.2.	<i>Визначення й аналіз загроз</i>	298
11.8.3.	<i>Розроблення плану захисту інформації</i>	299
11.8.4.	<i>Реалізація плану захисту інформації</i>	300
11.9.	Підрозділ технічного захисту інформації СЦ.....	300
11.9.1.	<i>Мета створення підрозділу захисту інформації</i>	300
11.9.2.	<i>Завдання підрозділу захисту інформації</i>	301
11.9.3.	<i>Функції ПЗІ під час створення комплексної системи захисту інформації</i>	302
11.9.4.	<i>Функції ПЗІ під час експлуатації комплексної системи захисту інформації</i>	303
11.9.5.	<i>Повноваження та відповідальність підрозділу захисту інформації</i>	305
11.9.6.	<i>Відповідальність ПЗІ</i>	306
11.9.7.	<i>Взаємодія підрозділу захисту інформації з іншими підрозділами ситуаційного центру та зовнішніми організаціями</i>	307
11.9.8.	<i>Штатний розклад та структура підрозділу захисту інформації</i>	308
11.10.	Організація проведення обстеження об'єктів ситуаційного центру.....	309
11.11.	Організація розроблення системи захисту інформації.....	310
11.12.	Реалізація організаційних заходів захисту.....	311
11.13.	Атестація системи технічного захисту інформації.....	311
11.14.	Контроль функціонування та керування системою захисту інформації.....	313
11.15.	Категоріювання об'єктів інформаційної діяльності ситуаційного центру.....	315
11.16.	Порядок проведення робіт з категоріювання об'єктів.....	316
11.17.	Технічний захист інформації в інформаційно-комунікаційній системі ситуаційного центру.....	317
11.17.1.	<i>Визначення несанкціонованого доступу</i>	317
11.17.2.	<i>Політика безпеки інформації</i>	318
11.18.	Створення комплексної системи захисту інформації СЦ.....	318
11.19.	Формування загальних вимог до КСЗІ СЦ.....	319
11.19.1.	<i>Обґрунтування необхідності створення КСЗІ СЦ</i>	319
11.19.2.	<i>Обстеження середовищ функціонування ПМК СЦ</i>	320
11.19.3.	<i>Формування завдання на створення КСЗІ СЦ</i>	320
11.20.	Розробка політики безпеки інформації.....	321
11.20.1.	<i>Вивчення об'єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт</i>	321
11.20.2.	<i>Вибір варіанту КСЗІ</i>	321
11.20.3.	<i>Оформлення політики безпеки</i>	321
11.20.4.	<i>Розробка технічного завдання на створення КСЗІ</i>	321

11.21.	Розробка проекту КСЗІ СЦ.....	322
	11.21.1. <i>Ескізний проект КСЗІ СЦ.....</i>	322
	11.21.2. <i>Технічний проект КСЗІ СЦ.....</i>	322
	11.21.3. <i>Розробка документації на КСЗІ СЦ.....</i>	323
	11.21.4. <i>Робочий проект КСЗІ СЦ.....</i>	323
11.22.	Введення КСЗІ в дію та оцінка захищеності інформації у СЦ.....	323
	11.22.1. <i>Підготовка КСЗІ до введення в дію.....</i>	323
	11.22.2. <i>Навчання користувачів.....</i>	324
	11.22.3. <i>Комплектування КСЗІ СЦ.....</i>	324
	11.22.4. <i>Будівельно-монтажні роботи.....</i>	324
	11.22.5. <i>Пусконаладжувальні роботи.....</i>	324
	11.22.6. <i>Попередні випробування.....</i>	325
	11.22.7. <i>Дослідна експлуатація.....</i>	325
	11.22.8. <i>Державна експертиза КСЗІ СЦ.....</i>	325
	11.22.9. <i>Супроводження КСЗІ СЦ.....</i>	326
11.23.	Висновки.....	326
	СЛОВНИК ТЕРМІНІВ ТА ВИЗНАЧЕНЬ.....	328
	ЛІТЕРАТУРА.....	346