

**БОГУШ В.М., БОГУШ В.В.,
БРОВКО В.Д., НАСТРАДІН В.П.**

ОСНОВИ КІБЕРПРОСТОРУ, КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ



111222 0166

004(025)

0-75

004.056.5(02)

В. М. БОГУШ, В. В. БОГУШ, В. Д. БРОВКО, В. П. НАСТРАДІН

ОСНОВИ КІБЕРПРОСТОРУ, КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ

Навчальний посібник

Київ
Видавництво Ліра-К
2022

УДК 004.056.5

О 60

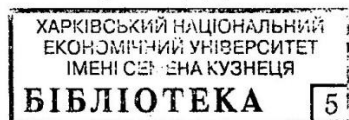
Автори: В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін

Рецензенти:

Бурячок В. В., д-р техн. наук, професор;

Кудін А. М., д-р техн. наук, старший науковий співробітник;

Козюра В. Д., к-т техн. наук, доцент



7 8 5 6 7 9

О 60 **Основи кіберпростору, кібербезпеки та кіберзахисту.** Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. — Київ : Видавництво Ліра-К, 2022. — 554 с.

ISBN 978-617-7844-54-8

У навчальному посібнику наведена систематизована сукупність відомостей про стан та перспективи розвитку широкого кола методологічних, наукових та технічних основ побудови кіберпростору, процесів протиборства у кіберпросторі, організацію забезпечення безпеки кіберпростору, методи та засоби забезпечення кіберзахисту. Навчальний посібник створений за результатами детального аналітичного вивчення сучасної міжнародної та національної нормативно-правової бази щодо сфери забезпечення кібербезпеки на міжнародному, державному рівні та на рівні організації.

Розрахований на студентів молодших курсів вищих навчальних закладів, які навчаються за всіма освітніми програмами спеціальності 125 Кібербезпека.

ISBN 978-617-7844-54-8

УДК 004.056.5

© Богуш В.М., Богуш В.В.,
Бровко В.Д., Настрадін В.П., 2020
© Видавництво Ліра-К, 2020

ЗМІСТ

ВСТУП	12
ПЕРЕЛІК АБРЕВІАТУР	15
I ОСНОВИ КІБЕРПРОСТОРУ	19
Розділ 1. ОСНОВНІ ПОЛОЖЕННЯ ТА ВИЗНАЧЕННЯ КІБЕРПРОСТОРУ	20
1.1. Загальне визначення простору та інформаційного простору	20
1.2. Основні положення інформаційного простору	20
1.2.1. Інформаційні ресурси	20
1.2.2. Засоби інформаційної взаємодії	22
1.2.3. Інформаційна інфраструктура	24
1.3. Визначення кіберпростору	25
1.4. Загальна структура кіберпростору	28
1.5. Створення та розвиток Інтернету як основної складової інфраструктури кіберпростору	29
1.5.1. Поява та створення Інтернету	29
1.5.2. Всесвітня павутина	31
1.5.3. Система доменних імен	32
1.5.4. Браузери	36
1.5.5. Способи соціальної комунікації	38
Висновки	39
Питання та практичні завдання до розділу 1	39
Розділ 2. ОСНОВНІ НАПРЯМИ РОЗВИТКУ ТЕОРІЇ КІБЕРПРОСТОРУ	41
2.1. Теоретичні основи кіберпростору	41
2.1.1. Географічні дослідження кіберпростору. Кібергеографія . .	41
2.1.2. Співвідношення кіберпростору і реального простору	42
2.1.3. Матриця М. Batty	42
2.2. Візуалізація кіберпростору	45
2.2.1. Картування кіберпростору	45
2.2.2. Атласи кіберпростору	45
2.3. Розвиток географії кіберпростору	48
2.3.1. Кібергеополітика	48

2.3.2. Кібердемографія	48
2.3.3. Кіберкартографія	52
Висновки	54
Питання та практичні завдання до розділу 2	56
Розділ 3. ОСНОВИ СПІЛКУВАННЯ У КІБЕРПРОСТОРИ	57
3.1. Поняття гіпертексту	57
3.2. Елементи глобального гіпертексту: вебсторінки і сайти	58
3.2.1. Вебсторінки і сайти	58
3.2.2. Види сайтів	60
3.3. Розробка та впровадження сайтів	62
3.3.1. Процес розробки сайтів	62
3.3.2. Особливості створення гіпертексту	65
3.3.2.1. Створення гіпертексту	65
3.3.2.2. Мова Інтернету	67
3.3.2.3. Структура Інтернет-ресурсу	70
3.4. Психологія сприйняття у кіберпросторі	74
3.4.1. Види сприйняття у кіберпросторі та методи дослідження сприйняття	74
3.4.2. Вплив на сприйняття смуги прокрутки і лінії згинання	75
3.4.3. Вплив на сприйняття кольору, шрифту, зображень та графічного контенту	76
3.4.4. Вплив на сприйняття швидкості завантаження сайту	86
3.4.5. Урахування цільової аудиторії	86
3.4.6. Проблеми зі сприйняття сайту	87
3.5. Вебтехнології основних сервісів кіберпростору	89
Висновки	91
Питання та практичні завдання до розділу 3	91
Розділ 4. ЕКОНОМІЧНА ДІЯЛЬНІСТЬ У КІБЕРПРОСТОРИ	94
4.1. Особливості кіберекономіки	94
4.1.1. Загальні визначення	94
4.1.2. Бізнес у кіберпросторі	94
4.1.3. Класифікація електронної комерції за цільовою аудиторією	95
4.1.4. Переваги електронної комерції	96
4.1.5. Основні напрями електронної комерції	96
4.2. Надання мережних ресурсів	97
4.2.1. Інтернет-провайдери	97
4.2.2. Хостинг-провайдери	97
4.2.3. Продаж доменних імен	98
4.2.4. Cloud Computing	102
4.2.4.1. Визначення та основні характеристики	102
4.2.4.2. Моделі розгортання	103
4.2.4.3. Моделі обслуговування	103
4.2.4.4. Технології	104
4.2.5. Розробка сайтів	105

4.3.	Організація роботи в кіберпросторі	105
4.3.1.	Трудові ресурси	105
4.3.1.1.	Вплив кіберпростору на ринок праці	106
4.3.1.2.	Рекрутинг	106
4.3.1.3.	Особливості фрілансу	107
4.3.2.	Продаж реальних товарів у кіберпросторі	108
4.3.3.	Надання інформаційних послуг і віртуальні товари	109
4.3.3.1.	Види інформаційних послуг та віртуальних товарів	109
4.3.3.2.	Онлайн-ігри	109
4.4.	Реклама у кіберпросторі	110
4.4.1.	Банерна реклама	110
4.4.2.	Rich Media	111
4.4.3.	Текстова реклама	111
4.4.4.	Розсилка реклами	112
4.4.5.	Спам	112
4.4.5.1.	Основні характеристики спаму	112
4.4.5.2.	Шляхи боротьби із спамом	113
4.4.6.	Спрямованість реклами	114
4.4.6.1.	Медійна реклама	114
4.4.6.2.	Контекстна реклама	115
4.4.6.3.	Пошукова оптимізація	116
4.4.6.4.	Просування реклами в соціальних мережах	117
4.4.6.5.	Ринок інтернет-реклами в Україні	118
4.4.6.6.	Переваги і недоліки Інтернет-реклами	118
	Питання та практичні завдання до розділу 4	121

Розділ 5. ОСОБЛИВОСТІ ПОВУДОВИ ПОШУКОВИХ СИСТЕМ **123**

5.1.	Загальна характеристика пошукових систем	123
5.1.1.	Специфіка інформації в Інтернет	123
5.1.2.	Внутрішня структура пошукової системи	125
5.1.3.	Параметри якості пошукових систем	126
5.2.	Популярні пошукові системи	129
5.2.1.	Порівняння пошукових систем	129
5.2.2.	Приклади популярних пошукових систем	130
5.2.3.	Інші популярні пошукові системи	132
5.3.	Пошук у Google	133
5.4.	Електронні бібліотеки і каталоги	134
	Висновки	135
	Питання та практичні завдання до розділу 5	135

Розділ 6. ОСОБЛИВОСТІ ПОВУДОВИ ТА ФУНКЦІОНУВАННЯ СОЦІАЛЬНИХ МЕРЕЖ **136**

6.1.	Поняття соціальної мережі	136
6.1.1.	Визначення соціальної мережі	136
6.1.2.	Уточнення понять — комп'ютерні, соціальні, віртуальні	137

6.1.3.	Віртуальна соціальна мережа	137
6.2.	Види та підвиди соціальних мереж	138
6.2.1.	Класи і структура соціальних мереж	138
6.2.2.	Загальне в соціальних мережах і ресурсах	139
6.3.	Особливості використання соціальної мережі	140
	Висновки	142
	Питання та практичні завдання до розділу 6	142
Розділ 7. СОЦІАЛЬНЕ, ПСИХОЛОГІЧНЕ ТА КУЛЬТУРНЕ СЕРЕДОВИЩЕ КІБЕРПРОСТОРУ		144
7.1.	Соціально-культурологічні аспекти кіберпростору	144
7.1.1.	Трансформація традиційної системи цінностей	144
7.1.2.	Поява нових соціальних інститутів	146
7.1.3.	Інтернет — новий соціальний інститут	147
7.1.4.	Особливості Інтернет-культури	148
7.2.	Основні соціально-психологічні риси кіберпростору	149
7.3.	Мотивації користувачів у кіберпросторі	155
7.3.1.	Основи мотивації	155
7.3.2.	Особливості мотивації користувачів Інтернету	157
7.3.3.	Основні види мотивів	159
7.3.4.	Віртуальні образи створювані людьми при спілкуванні в Інтернеті	163
7.3.4.1.	Особливі соціальні ролі — аватари, нові імена (ніки)	163
7.3.4.2.	Основні підходи до вибору ніка	164
7.3.4.3.	Психологія вибору ніка	164
7.3.4.4.	Самопрезентація в Інтернеті	166
7.4.	Образи особистостей у кіберпросторі	168
7.4.1.	Соціальна нерівність серед користувачів Інтернету	168
7.4.1.1.	Соціальна нерівність серед користувачів Інтернету: нові підстави для стратифікаційного поділу	168
7.4.1.2.	Соціальна нерівність серед користувачів Інтернету	170
7.4.2.	Хакери як нова соціальна група	172
7.4.2.1.	Хакери як соціальна група, їх типологія і мотивація діяльності	172
7.4.2.2.	Мотиви діяльності кракерів	176
7.4.3.	Залежність від Інтернету	178
	Висновки	181
	Питання та практичні завдання до розділу 7	182

II ОСНОВИ КІБЕРБЕЗПЕКИ **185**

Розділ 8. ОСНОВНІ ПОЛОЖЕННЯ КІБЕРБЕЗПЕКИ		186
8.1.	Основи національної безпеки держави	186
8.1.1.	Історичні аспекти формування категорії національна безпека	186
8.1.2.	Основні поняття національної безпеки	189

8.1.3.	Основні категорії теорії національної безпеки та їх відображення у правовому забезпеченні національної безпеки	191
8.2.	Роль і місце кібербезпеки у системі національної безпеки держави	195
8.2.1.	Основні загрози та пріоритетні напрями забезпечення національної безпеки в інформаційній сфері та кіберпросторі	195
8.2.2.	Основні положення Доктрини інформаційної безпеки України	197
8.2.3.	Стратегія кібербезпеки України	206
8.2.4.	Національна система кібербезпеки	208
8.2.5.	Пріоритети та напрями забезпечення кібербезпеки України	209
8.3.	Основні положення кібербезпеки відповідно до Закону України Про основні засади забезпечення кібербезпеки України	215
8.3.1.	Загальні положення та правові основи забезпечення кібербезпеки України	215
8.3.2.	Організаційне забезпечення кібербезпеки України	215
8.3.3.	Принципи забезпечення кібербезпеки	218
8.3.4.	Національна система кібербезпеки та основи її функціонування	219
8.3.5.	Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA	224
8.3.6.	Взаємодія у сфері кібербезпеки	225
	Висновки	226
	Питання та практичні завдання до розділу 8	227

Розділ 9. ОСНОВНІ ВИДИ ПРОТИБОРСТВА У КІБЕРПРОСТО-	РІ	229
9.1.	Визначення поняття протиборства в інформаційній сфері та кіберпросторі	229
9.1.1.	Протиборство в інформаційній сфері	229
9.1.2.	Протиборство в кіберпросторі як складова інформаційного протиборства	232
9.1.3.	Сфера протиборства у кіберпросторі	233
9.2.	Основні складові протиборства в інформаційному та кіберпросторі	234
9.2.1.	Інформаційна злочинність та кіберзлочинність	234
9.2.2.	Інформаційний тероризм та кібертероризм	239
	9.2.2.1. Загальні положення про інформаційний тероризм та кібертероризм	239
	9.2.2.2. Складові частини кібертероризму як правопорушення	241
	9.2.3. Інформаційна війна та кібервійна	249
	9.2.4. Інформаційна безпека та кібербезпека	252
	Висновки	253
	Питання та практичні завдання до розділу 9	254

Розділ 10. ВІЙНА ЯК ОДИН З ОСНОВНИХ СПОСОВІВ ПРОТИ-	
БОРСТВА В ІНФОРМАЦІЙНОМУ ТА КІБЕРПРОСТОРИ	255
10.1. Основні поняття інформаційної війни	255
10.1.1. Визначення інформаційної війни	255
10.1.2. Концепція інформаційної війни	256
10.1.3. Органи інформаційної війни	256
10.1.4. Основні форми інформаційної війни	257
10.1.5. Основні форми інформаційної війни на державному рівні	257
10.1.6. Основні форми інформаційної війни на воєнному рівні	259
10.1.7. Необхідні умови для досягнення інформаційної переваги	261
10.2. Інформаційна зброя та кіберзброя в інформаційній війні та кібервійні	263
10.2.1. Застосування інформаційної зброї та кіберзброї	263
10.2.2. Інформаційна зброя воєнного застосування	264
10.2.3. Інформаційна зброя загального та воєнного застосування	265
10.2.4. Особливості, що характеризують основні риси застосування інформаційної зброї	277
10.3. Особливості бойових дій в кіберпросторі	277
10.3.1. Кібертака	278
10.3.2. Кіберконтратака	278
10.3.3. Оборонні засоби протидії в кіберпросторі	278
Висновки	280
Питання та практичні завдання до розділу 10	281
Розділ 11. ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ	282
11.1. Основні положення безпеки кіберпростору	282
11.1.1. Основні положення безпеки кіберпростору організації	282
11.1.2. Загальна модель технології забезпечення кібербезпеки	285
11.1.3. Загальний підхід до реалізації технології забезпечення кі- бербезпеки	288
11.2. Стейкхолдери та активи кіберпростору	289
11.2.1. Класифікація стейкхолдерів	289
11.2.2. Загальна характеристика активів кіберпростору	290
11.3. Загрози безпеці кіберпростору	292
11.3.1. Загальна характеристика основних загроз безпеці кіберпро- сторю	293
11.3.2. Загальна характеристика уразливостей кіберпростору	295
11.3.3. Механізми основних атак у кіберпросторі	296
11.4. Ролі стейкхолдерів у забезпеченні кібербезпеки	299
11.4.1. Ролі споживачів	299
11.4.2. Ролі провайдерів (постачальників) послуг	302
11.5. Настанови стейкхолдерам щодо забезпечення кібербезпеки	302
11.5.1. Загальні питання щодо поводження з ризиками	303
11.5.2. Настанови споживачам	305
11.5.3. Настанови провайдерам	307
11.5.3.1. Загальні відомості	307
11.5.3.2. Загальні рекомендації щодо поводження з ризиками	308

11.5.3.3. Вимоги безпеки для провайдерів вебхостингу і/або інших мережних сервісів	315
11.5.4. Рекомендації щодо захисту споживачів	317
Висновки	318
Питання та практичні завдання до розділу 11	321

III ОСНОВИ КІБЕРЗАХИСТУ **322**

Розділ 12. АРХІТЕКТУРА БЕЗПЕКИ ІНФРАСТРУКТУРИ КІБЕРПРОСТОРУ **323**

12.1. Характеристика галузі безпеки мереж та систем кіберінфраструктури	323
12.1.1. Історичні аспекти розвитку інфраструктури кіберпростору	324
12.1.2. Базові поняття щодо безпеки інформації	328
12.1.2.1. Основні властивості інформації як предмета захисту	328
12.1.2.2. Основні характеристики інформаційної системи як об'єкта захисту	334
12.1.2.3. Основні проблеми захисту інформаційних технологій	336
12.1.2.4. Класифікація загроз безпеці інформації та інформаційних ресурсів	340
12.1.2.5. Класифікація джерел загроз інформації	344
12.1.2.6. Класифікація уразливостей безпеці	351
12.1.2.7. Класифікація актуальних загроз	354
12.1.2.8. Основні напрями захисту інформації та інформаційних ресурсів	354
12.1.3. Система безпеки кіберінфраструктури	357
12.2. Основні моделі та архітектурні рішення забезпечення безпеки (захисту) інфраструктури кіберпростору	363
12.2.1. Характеристика галузі безпеки мереж та систем кіберінфраструктури	363
12.2.2. Моделі безпеки мереж та систем кіберінфраструктури	365
12.2.2.1. Архітектура безпеки для моделі взаємодії відкритих систем	366
12.2.2.2. Моделі безпеки нижніх і верхніх рівнів	370
12.2.3. Структури безпеки	370
12.2.4. Архітектура безпеки для систем, що забезпечують зв'язок між кінцевими пристроями	374
12.3. Основні підходи до реалізації загальних завдань забезпечення безпеки (захисту) інформаційно-комунікаційних систем	378
12.3.1. Загрози й ризики безпеки інформаційно-комунікаційних систем	378
12.3.2. Вимоги та послуги безпеки	381
12.3.2.1. Взаємовідносини функціональних вимог, загроз і завдань безпеки	381

12.3.2.2.	Характеристика основних вимог безпеки та їхнього взаємозв'язку з послугами безпеки	383
12.3.2.3.	Послуги безпеки та рівні взаємодії відкритих систем	390
12.3.3.	Спеціальні механізми безпеки та їх взаємозв'язок з послугами безпеки	393
12.3.4.	Криптографічні методи забезпечення безпеки систем та мереж кіберінфраструктури	398
12.3.4.1.	Основні поняття та визначення	398
12.3.4.2.	Поняття симетричної криптосистеми шифрування	401
12.3.4.3.	Поняття асиметричної криптосистеми шифрування	402
12.3.5.	Механізми цифрового підпису	404
12.3.5.1.	Процес електронного цифрового підпису	404
12.3.5.2.	Застосування функції гешування	408
12.3.5.3.	Проблема довіри до відкритих ключів	411
Висновки		412
Питання та практичні завдання до розділу 12		415
Розділ 13. ОСНОВНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЇ		417
13.1.	Заходи кібербезпеки на рівні захисту додатків	417
13.2.	Заходи кібербезпеки на рівні захисту серверів	420
13.3.	Заходи кібербезпеки на рівні захисту кінцевих користувачів	421
13.4.	Заходи кібербезпеки щодо атак соціальної інженерії	424
13.4.1.	Загальні відомості	425
13.4.2.	Організаційно-розпорядчі аспекти	425
13.4.3.	Функціонально-когнітивні аспекти	426
13.5.	Готовність до проявів подій кібербезпеки та інші заходи кібербезпеки	429
13.5.1.	Даркнет-моніторинг	430
13.5.2.	Технологія сінкхолінг	432
13.5.3.	Методи зворотного трасування	433
13.6.	Основи обміну інформацією та координації	435
13.6.1.	Політики інформаційної взаємодії	436
13.6.2.	Правила і процедури інформаційної взаємодії	438
13.7.	Персонал, техніка і технології інформаційної взаємодії	441
13.7.1.	Рекомендації персоналу	441
13.7.2.	Підвищення обізнаності та готовності	442
13.7.3.	Рекомендації щодо застосування техніки та технології	443
13.7.4.	Впровадження рекомендацій	445
Висновки		446
Питання та практичні завдання до розділу 13		448
Розділ 14. РЕАЛІЗАЦІЯ ОСНОВНИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЇ		450
14.1.	Визначення середовища кібербезпеки організації	451
14.1.1.	Середовище кібербезпеки організації	451
14.1.2.	Визначення загроз кібербезпеці організації	453

14.1.3. Загальний підхід до вибору механізмів захисту	454
14.2. Методи, засоби та технології кіберзахисту організації	457
14.2.1. Загальні підходи до реалізації заходів та засобів кіберзахисту організації	457
14.2.2. Забезпечення безпеки управління	463
14.2.3. Багаторівнева безпека програм, мережі та управління мережею	467
14.2.4. Живучість мережі навіть у момент злому	468
14.3. Основні методи дій зловмисників у кіберпросторі організації	470
14.3.1. Способи, методи, засоби і методики злому кіберпростору організації	471
14.3.2. Загрози кібербезпеці організації	475
14.4. Вибір технологічних механізмів забезпечення кібербезпеки організації	480
14.4.1. Криптографія	480
14.4.2. Технологія контролю доступу	482
14.4.3. Антивірус і цілісність системи	489
14.4.4. Аудит і моніторинг	490
14.4.5. Управління	491
14.5. Типова система кібербезпеки організації	495
14.5.1. Захист віддаленого доступу	496
14.5.2. Організація захисту IP-телефонії	499
14.5.3. Організація захисту віддаленого офісу	505
14.6. Організація захисту WLAN	507
14.6.1. Загальні питання безпеки WLAN	508
14.6.2. Механізми та вимоги до безпеки всередині і перед бездротовою точкою доступу	509
14.6.3. Покращення безпеки для технічних умов IEEE 802.11	510
14.6.4. Багаторівневий підхід до організації захисту бездротових мереж LAN	511
Висновки	517
Питання та практичні завдання до розділу 14	520
СЛОВНИК ДОДАТКОВИХ ТЕРМІНІВ І ПОНЯТЬ	522
ПРЕДМЕТНИЙ ПОКАЖЧИК	532
ЛІТЕРАТУРА	545