

Основи кіберпростору, кібербезпеки та кіберзахисту

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.

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

ОСНОВИ КІБЕРПРОСТОРУ, КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ

Навчальний посібник

Київ
Видавництво Ліра-К
2020

УДК 004.056.5
О 60

Автори: В. М. Богущ, В. В. Богущ, 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

О 60 **Основи кіберпростору, кібербезпеки та кіберзахисту.** Навч. посіб. /
В. М. Богущ, В. В. Богущ, В. Д. Бровко, В. П. Настрадін; під. ред.
В. М. Богуща. — К.: Видавництво Ліра-К, 2020. — 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 протидії 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

© Богущ В.М., Богущ 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 гра- фічного 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 СПОСОБІВ ПРОТИ-	
БОРСТВА В ІНФОРМАЦІЙНОМУ ТА КІБЕРПРОСТОРІ	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 військовому 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 військового застосування	264
10.2.3. Інформаційна зброя загального та військового 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- стору	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	532

ВСТУП

Під впливом швидкого розвитку інформаційних технологій формуються нові — віртуальні — середовища різноманітних просторів, які набувають все більшої значущості як у міжнародних та державних відносинах, так і у зовнішніх та внутрішніх відносинах конкретних організацій. До кола таких віртуальних середовищ належить кіберпростір, що позначає особливу область соціальних взаємодій, опосередкованих сукупністю процесів, що відбуваються в інформаційно-комунікаційних мережах світу, і який перетворився на ще одне середовище буття та діяльності людини.

Крім Інтернету до кіберпростору належать багато інших мереж, наприклад, транснаціональних, через які відбувається передача даних про фінансові потоки, торги на різних біржах і операції по кредитних лініях.

Крім того, в кіберпросторі функціонують системи управління різноманітними машинами і механізмами, наприклад, панелі керування генераторами, ліфтами, насосами, транспортними та енергетичними системами тощо.

Особлива та дуже важлива частина кіберпростору належить системам та мережі управління воєнною технікою, зокрема безпілотниками (дронами), бойовими роботами, ракетами різного радіусу дії.

Цей короткий і далеко не повний перелік дозволяє дійти висновку, що кіберпростір сьогодні являє собою життєво важливу галузь інформаційної, економічної, політичної, воєнної діяльності окремих людей, корпорацій, держав та їх спільнот, наднаціональних структур і утворень.

Кіберпростір, що не обмежений державними кордонами, став найважливішим полем політичної, економічної, інформаційної та культурної конкуренції держав, суспільств та особистостей, в якому стикаються інтереси різних політичних суб'єктів, різних держав і центрів політичної сили.

Майже відразу ж після свого виникнення кіберпростір перетворився у п'яте (після суші, моря, повітря і космосу) поле битви різних політичних і воєнних сил і залишається таким [68]. Більше того, безліч протистоянь між розвідувальними організаціями різних країн, їх воєнними структурами, а також економічні та інформаційні війни, зокрема шпигунство і диверсії,

розгортаються саме у кіберпросторі. Ця обставина визначає високу значимість процесів, що відбуваються у кіберпросторі, для сучасного стану національної безпеки.

У міру розвитку кіберпростору в ньому виникали та посилювалися різні загрози, а також відповідні заходи щодо протидії цим загрозам і їх нейтралізації.

Згідно з визначенням Міжнародного союзу комунікацій, кібербезпека являє собою набір засобів, стратегій і принципів забезпечення безпеки, гарантії безпеки, підходів до управління ризиками, дії і практичного досвіду для захисту кіберсередовища, ресурсів організації і користувача [112].

Кібербезпека охоплює заходи, які можна здійснити для захисту кіберпростору як у цивільній, так і у військовій області від загроз, які пов'язані зі сформованими в ньому взаємозалежними мережами та інформаційною інфраструктурою або можуть завдати даній інфраструктурі шкоди.

Очевидно, що кібербезпека не може розглядатися ізольовано від інших аспектів і видів внутрішньої та міжнародної безпеки, а кіберзлочинність тісно пов'язана з іншими видами злочинності, такими як промислове шпигунство, діяльність розвідувальних служб, міжнародний тероризм [116].

У той же час кібербезпека має яскраво виражену специфіку, яка визначається використанням інформаційних технологій, що швидко розвиваються, її необхідно розглядати як особливу сферу національної та міжнародної безпеки з власними тенденціями розвитку та властивим їй інструментарієм.

При цьому однією зі специфічних рис кібербезпеки є те, що межа між кіберзлочинністю, застосуванням кіберзброї і діями різних політичних акторів (наприклад, спецслужб різних держав) досить розмита і невизначена. Наразі виникає складність ідентифікації джерела і характеру загроз для кіберпростору, яка вже стала чинником численних внутрішньополітичних і міжнародних конфліктів, взаємних звинувачень і політичної «боротьби без правил».

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. Він складається з трьох частин і чотирнадцяти розділів.

У **першій частині** посібника здійснений аналіз основних напрямів розвитку теоретичних основ побудови та дослідження кіберпростору. Сформульовані загальні підходи щодо побудови, розвитку і використання інфраструктури кіберпростору та сервісів кіберпростору, а також методів та засобів дослідження соціологічної та психологічної сфери кіберпростору з метою виявлення загроз безпеці кіберпростору.

У **другій частині** посібника на основі системного підходу викладені методологічні та теоретичні основи забезпечення безпеки особистості, суспільства та держави у кіберпросторі, що охоплює кіберінфраструктуру, кіберсервіси, соціологічні та психологічні сфери, пов'язані з діяльністю людей. Наведені теоретичні та методологічні основи запобігання кіберзлочинності, кібертероризму, кіберконфліктам і кібервійнам на основі впровадження методів та засобів забезпечення кібербезпеки.

У **третьій частині** посібника визначені загальні завдання побудови та впровадження технологій та засобів захисту інфраструктури кіберпростору, основні напрями дослідження середовища кібербезпеки організації та розробки загальних підходів її кіберзахисту, загальної методології обґрунтування засобів, заходів та технологій кіберзахисту організації, процесу побудови системи її кіберзахисту.

Посібник містить також словник додаткових термінів і понять та покажчик ключових термінів і понять. Ключові терміни і поняття кіберпростору, кібербезпеки та кіберзахисту, які формуються 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 кіберпростору, кібербезпеки та кіберзахисту та використовувати посібник як тлумачний словник.

Автори висловлюють щирі вдячність рецензентам: доктору технічних наук, професору В. Л. Бурячку, доктору технічних наук, старшому науковому співробітнику А. М. Кудіну та кандидату технічних наук, доценту В. Д. Козюрі за змістовні зауваження та рекомендації, які безумовно сприяли покращенню книги.

ПЕРЕЛІК АБРЕВІАТУР

Україномовні

АСУ	—	автоматизована система управління
ВВС	—	взаємодія відкритих систем
ЕОМ	—	електронно-обчислювальна машина
ЕЦП	—	електронний цифровий підпис
ІКМ	—	інформаційно-комунікаційна мережа
ІКТ	—	інформаційно-комунікаційна технологія
ІнАУ	—	Інтернет асоціація України
ІПС	—	інформаційно-пошукова система
ІС	—	інформаційна система
ЗКТ	—	засоби комп'ютерної техніки
ЗМІ	—	засоби масової інформації
КВО	—	критично важливий об'єкт
КНШ	—	комітет начальників штабів
МКХ	—	міжнародний класифікатор хвороб
НСД	—	несанкціонований доступ
ОС	—	операційна система
ПК	—	персональний комп'ютер
ПЕМВ	—	побічні електромагнітні випромінювання
РЄ	—	Рада Європи
РЕЗ	—	радіоелектронний засіб
САПР	—	система автоматизованого проектування
СЗІБ	—	система забезпечення інформаційної безпеки
СЗІ	—	система захисту інформації
СІБ	—	система інформаційної безпеки
СУБД	—	система управління базою даних
СУБМ	—	система управління базою моделей
СУІБ	—	система управління інформаційною безпекою
ТД	—	точка доступу
ТЗ	—	технічний засіб
УНІАН	—	українське незалежне інформаційне агентство новин
ЦС	—	центр сертифікації

Англомовні

API	—	Application Programming Interface (прикладний програмний інтерфейс)
AR	—	Augmented Reality (доповнена реальність)
BcN	—	Broadband convergence Network (мережа конвергенції широкосмугового зв'язку)
C4I2	—	Command, Control, Communications, Computing, Intelligence and Information Systems
C4ISR	—	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (система оперативного (бойового) управління, зв'язку, розвідки та спостереження)
C4IEW	—	Communications, Computers, Intelligence, Electronic Warfare
CDMA	—	Code Division Multiple Access (багатостанційний доступ з кодовим розділенням каналів)
CERT	—	Computer Emergency Response Team (команда реагування на комп'ютерні надзвичайні події)
CIRT	—	Cyber Incident Response Team (команда реагування на інциденти)
CSIRT	—	Computer Security Incident Response Team (команда комп'ютерної безпеки з реагування на інциденти)
CYBEX	—	Cybersecurity Information Exchange techniques (методи обміну інформацією про кібербезпеку)
DNS	—	Domain Name System (система доменних імен)
DoS	—	Denial of Service (відмова в обслуговуванні)
DDoS	—	Distributed Denial of Service (розподілена відмова в обслуговуванні)
DSM	—	Diagnostic and Statistical Manual of mental disorders (діагностичний і статистичний посібник з психічних розладів)
DTD	—	— Document Type Definition (визначення типу документа)
DWDM	—	Dense Wavelength Division Multiplexing (щільне мультиплексування з розділенням за довжиною хвилі)
EMS	—	Enterprise Management Systems (система управління підприємством)
FGN	—	Future Generation Network (мережа майбутнього покоління)
ICA	—	InfoCommunication Actor (автор (учасник) кіберінфраструктури)
ICT	—	Information and Communication Technology (інформаційно-комунікаційна технологія)
IDS	—	Intrusion Detection System (система виявлення вторгнень)
IMS	—	IP Multimedia Subsystem (мультимедійна підсистема на основі протоколу IP)
IoT	—	Internet of Things (Інтернет речей)
IP	—	Internet Protocol (міжмережний протокол)
IPO	—	Information Providing Organizations (організація, що є стороною, яка передає інформацію)

IRO	—	Information Receiving Organizations (організація, яка є стороною, що приймає інформацію)
IPTV	—	Internet Protocol Television (цифрове телебачення за протоколом IP)
IT	—	Information Technology (інформаційна технологія)
ITU	—	International Telecommunication Union (Міжнародний союз телекомунікацій)
ISMS	—	information security management system (система управління інформаційною безпекою)
ISO	—	International Organization for Standardization (Міжнародна організація стандартизації)
JCS	—	Joint Chiefs of Staff (Комітет начальників штабів)
HTML	—	Hypertext Markup Language (мова розмітки гіпертекстових документів)
HTTP	—	Hyper Text Transfer Protocol (протокол передавання гіпертекстових документів)
LAN	—	Local Area Network (локальна обчислювальна мережа)
LDAP	—	Lightweight Directory Access Protocol (полегшений протокол доступу до директорій/каталогів)
LTE	—	Long Term Evolution («довготерміновий розвиток»)
MIME	—	Multipurpose Internet Mail Extensions (багатоцільові розширення для інтернет-пошти)
NAT	—	Network Address Translation (перетворення мережних адрес)
NOC	—	Network Operations Center (мережний операційний центр)
NGN	—	Next Generation Network (мережа наступного покоління)
OAM&P	—	Operations, Administration, Maintenance, and Provisioning (операції, адміністрування та управління або операції, адміністрування та обслуговування)
OSI	—	Open Systems Interconnection model (модель взаємодії відкритих систем)
PKI	—	Public Key Infrastructure (інфраструктура відкритих ключів)
RADIUS	—	Remote Authentication in Dial-In User Service (протокол для реалізації автентифікації, авторизації та збору відомостей про використані ресурси)
SAM	—	Software Asset Management (менеджмент програмних активів)
SDP	—	Service Delivery Platform (платформа надання послуг)
SEO	—	Search Engine Optimization (пошукова оптимізація)
SMM	—	Social Media Marketing (просування в соціальних мережах)
SMO	—	Social Media Optimization (оптимізація для соціальних мереж)
SSID	—	Service Set Identifier (символьна назва безпроводної точки доступу Wi-Fi)
SQL	—	Structured Query Language (мова структурованих запитів)

VLAN	—	Virtual Local Area Network (віртуальна локальна мережа)
URL	—	Uniform Resource Locator (універсальний покажчик на ресурс)
VAR	—	Value Added Reseller (реселлер, що надає послуги)
VoIP	—	Voice over IP (передавання голосу за протоколом IP)
VPN	—	Virtual Private Network (віртуальна приватна мережа)
WLAN	—	Wireless Local Area Network (бездротова локальна мережа)
WSN	—	Wireless Sensor Networks (безпроводна сенсорна мережа)
WWW	—	World Wide Web (Всесвітня павутина)

Частина I

ОСНОВИ КІБЕРПРОСТОРУ

Розділ 1

ОСНОВНІ ПОЛОЖЕННЯ ТА ВИЗНАЧЕННЯ КІБЕРПРОСТОРУ

1.1. Загальне визначення простору та інформаційного простору

Простір [space] це одна з основних форм існування матерії (філос.), яка характеризується протяжністю і обсягом. Відповідно до спеціальної теорії відносності існує тісний зв'язок простору і часу.

На рівні практичного сприйняття під простором розуміють місце, у якому можливий рух, різноманітні положення і розташування об'єктів, відношення близькості-дальності, поняття спрямованості, місце, де відбуваються події і дії, що містить всі місця, об'єкти і структури.

Інформаційний простір [information space] — одне з первинних понять, що не може бути точно визначене. Найчастіше термін розуміють як логічне зіставлення об'єктному (предметному, фізичному, матеріальному) світу. З практичної точки зору вважається, що інформаційний простір — це теж саме, що семантичний простір [21].

Для практичного застосування краще використати визначення інформаційного простору як будь-якого середовища, де інформація створюється, через яке передається, приймається, в якому зберігається, обробляється і знищується [86].

Основними компонентами інформаційного простору є:

- інформаційні ресурси;
- засоби інформаційної взаємодії;
- інформаційна інфраструктура.

1.2. Основні положення інформаційного простору

1.2.1. Інформаційні ресурси

У загальному випадку під інформаційними ресурсами розуміють результат об'єктивного цілеспрямованого відображення закономірностей і фактів реалізації будь-яких процесів, що відбуваються у суспільстві та в навколишньому середовищі (природі). Вони являють собою сукупність наукових знань, зафіксованих на паперових чи інших носіях, що зберігають-

ся у довідково-інформаційних фондах інформаційних органів та бібліотек [11].

До інформаційних ресурсів також відносять окремі документи і окремі масиви документів, документи і масиви документів у інформаційних системах (бібліотеках, архівах, фондах, банках, банках даних і т. ін.), що містять інформацію з усіх напрямків життєдіяльності суспільства, а також сукупність даних, які є цінними для установи (організації) і виступають як матеріальні ресурси, зокрема, це основні та допоміжні дані, що зберігаються в зовнішній пам'яті комп'ютерних систем, та вхідні документи.

Класифікація інформаційних ресурсів:

за видом інформації — інформаційні ресурси, що можуть містити інформацію наступних видів:

- правову;
- науково-технічну;
- політичну;
- економічну (фінансово-економічну);
- статистичну;
- інформацію про стандарти і регламенти, метрологічну;
- соціальну;
- інформацію про охорону здоров'я;
- інформацію про надзвичайні ситуації;
- особисту інформацію (персональні дані);
- кадастри (земельний, містобудівний, лісовий, майновий і т. ін.);
- інформацію іншого виду;

за режимом доступу — інформаційні ресурси, що містять відкриту інформацію (без обмежень) або інформацію обмеженого доступу (державну таємницю, конфіденційну інформацію, комерційну таємницю, професійну таємницю, службову таємницю, особисту (персональну) таємницю);

за видом носія — інформаційні ресурси, інформація в яких може бути записана на папері, на машиночитаних носіях, у вигляді зображення на папері, на екрані ЕОМ, в пам'яті ЕОМ, у каналах зв'язку, на інших видах носіїв;

за способом формування і розповсюдження — інформаційні ресурси, що знаходяться у стаціонарному або рухомому (мобільному) стані;

за способом організації зберігання і використання — інформаційні ресурси, для зберігання і використання інформації, в яких можуть використовуватися традиційні форми (масиви документів, фонди документів, архіви) або автоматизовані форми (банки даних, інформаційні системи, бази знань);

за формою власності — інформаційні ресурси, що можуть складати:

- загальнодержавне національне надбання;
- державну власність;
- муніципальну власність;
- приватну власність;
- колективну власність.

1.2.2. Засоби інформаційної взаємодії

Умови інформаційної взаємодії

Термін «інформація» походить від лат. *informatio*, що означає «роз'яснення» і передбачає наявність будь-якої форми діалогу між відправниками і одержувачами інформації.

Усі якісні і кількісні визначення інформації також передбачають наявність відправників і одержувачів інформації, тобто мова йде про деякий вид взаємодії об'єктів.

Взаємодію об'єктів, яка призводить до зміни знань хоч би одного з них, можна назвати **інформаційною взаємодією**, а сукупність засобів, що забезпечують взаємодію об'єктів — засобами інформаційної взаємодії [48].

Умови інформаційної взаємодії на прикладі передачі знань за допомогою усного мовлення можна сформулювати наступним чином.

Для того, щоб процес передачі знань від одного об'єкта до іншого був успішним, слід дотримуватися низки умов. **Процес інформаційної взаємодії** на прикладі передачі знань за допомогою усного мовлення можна уявити п'ятикомпонентною (п'ятивимірною векторною) величиною, що складається з компонентів:

1. фізичної;
2. сигнальної;
3. лінгвістичної;
4. семантичної;
5. прагматичної.

Перша компонента — фізична, тобто необхідна наявність фізичного джерела звуку (голосових зв'язок), фізичного середовища поширення звуку (повітря) і фізичного приймача (вуха).

Друга компонента — сигнальна: амплітудно і частотно модульовані коливання.

Третя компонента — лінгвістична: необхідно, щоб обидва співрозмовники знали хоча б одну спільну мову.

Четверта компонента — семантична, тобто в переданому повідомленні повинен бути присутнім змістовний опис об'єкта або впливу, щоб при отриманні повідомлення могли змінитися знання у того, хто приймає ці повідомлення

П'ята компонента — прагматична: необхідна наявність бажання (мотивації) передавати і приймати повідомлення.

Інформаційна взаємодія відкритих систем

Як приклад класифікації інформаційних взаємодій можна навести протокольні рівні в міжнародних стандартах взаємодії відкритих мереж [93]. При взаємодії двох користувачів в комунікаційній мережі реалізується сукупність протоколів семи рівнів:

1. фізичного;
2. канального;
3. мережного;
4. транспортного;
5. сеансового;
6. представницького;
7. прикладного.

Перші три протокольні рівні визначають такі особливості роботи мережі зв'язку при обслуговуванні користувачів, як стандарт електричних сигналів в мережі, виявлення та виправлення помилок, маршрутизація в транспортній мережі і т. ін.

Наступні чотири рівні визначають такі стандарти взаємодії самих користувачів, як контроль за цілісністю повідомлення, відновлення без втрат сеансу взаємодії в разі переривання, представлення даних на дисплеях і друкуючих пристроях тощо.

Класи взаємодії відкритих систем

Спектр інформаційних взаємодій надзвичайно широкий. Можна умовно розділити досліджувані інформаційні взаємодії по об'єктах на три класи:

- 1-й клас — взаємодія штучних (технічних) систем;
- 2-й клас — взаємодія змішаних систем;
- 3-й клас — взаємодія природних (живих) систем.

До першого класу відносяться інформаційні взаємодії в технічних системах — від найпростіших регуляторів до глобальних комп'ютерних мереж.

До другого класу — інформаційні взаємодії типу «живий організм — штучний орган», «людина — машина», «живий дослідник — неживий об'єкт досліджень» і т. ін.

До третього класу належать інформаційні взаємодії, що діють в межах від молекулярно-генетичного рівня до рівня соціальних спільнот.

При такому різноманітті взаємодіючих об'єктів завдання опису законів інформаційної взаємодії надзвичайно складне, оскільки треба описати як обмін однією інформацією типу «включено — виключено» в технічних системах, так і формування моралі в людських співтовариствах.

При описі кожного з цих рівнів доводиться спиратися на специфічну для відповідного рівня концепцію перетворювача інформації, свої мови опису, закономірності, що розробляються в рамках відповідних дисциплін (наук), які, тим самим, вивчають інформаційну взаємодію на даному рівні.

1.2.3. Інформаційна інфраструктура

Інформаційна інфраструктура [information infrastructure] — система організаційних структур і підсистем, що забезпечують функціонування засобів інформаційної взаємодії в інформаційному просторі.

Вона включає в себе: сукупність інформаційних центрів, підсистем, банків даних і знань, систем комунікацій, центрів управління, апаратно-програмних засобів і технологій, що забезпечують збирання, зберігання, оброблення і передавання інформації, а також доступ споживачів до інформаційних ресурсів [11].

Глобальна інформаційна інфраструктура — інформаційна інфраструктура світового (міждержавного) масштабу. Може створюватися на основі трансформації національних інформаційних інфраструктур при створенні глобального інформаційного суспільства з дотриманням наступних принципів:

- забезпечення справедливої конкуренції;
- заохочення приватних інвестицій;
- визначення й адаптація регулюючих механізмів;
- забезпечення відкритого доступу до мереж;
- створення умов для забезпечення універсального доступу до інформаційних послуг;
- забезпечення рівних можливостей для громадян;
- забезпечення різноманітності змісту, включаючи культурний і мовний.

Ці принципи застосовуються до глобальної інформаційної інфраструктури за допомогою:

Книги, які можуть вас зацікавити



Організаційно-правові
основи забезпечення
кібербезпеки



Кібербезпека та ризики
цифрової
трансформації
компаній



Кібервійни,
кібертероризм,
кіберзлочинність
(концепції, стратегії,
технології)



Кібернологія: цифрова
віртуальність та воєнна
реальність



Кібербезпека в Україні:
нормативна база,
коментарі та
роз'яснення, актуальна
судова практика



Захист вітчизни:
історія, сучасність,
перспектива

Перейти до галузі права
Інформаційне право



Перейти на сайт →