

Ю. І. Когут

КІБЕРВІЙНА ТА БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ПРАКТИЧНИЙ ПОСІБНИК

*За редакцією доктора технічних наук, професора, заслуженого діяча
науки і техніки України, лауреата Державної премії України
в галузі науки і техніки Довгополого А. С.*

Київ

Консалтингова компанія «СІДКОН»



2021

Купити книгу на сайті kniga.biz.ua >>>

*Рекомендовано до друку науково-технічною радою
Центрального науково-дослідного інституту озброєння
та військової техніки Збройних Сил України
«19» серпня 2021 року, протокол № «7»*

Рецензенти:

Гордієнко Сергій Георгійович, Завідувач кафедри національної безпеки навчально-наукового інституту права ім. князя Володимира Великого МАУП, доктор юридичних наук, доцент, полковник запасу.

Лапицький Сергій Володимирович, Головний науковий співробітник Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, працівник Збройних Сил України.

Луханін Михайло Іванович, Головний науковий співробітник Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, працівник Збройних Сил України.

Сунгуровський Микола Вікторович, Директор воєнних програм Українського центру економічних та політичних досліджень ім. О. Разумкова, кандидат технічних наук, полковник запасу.

Ярухін Юрій Михайлович, Віце-президент Незалежного аналітичного центру геополітичних досліджень «Борисфен Інтел», кандидат військових наук, полковник запасу.

Когут Ю. І.

К57 Кібервійна та безпека об'єктів критичної інфраструктури: практичний посібник / Ю. І. Когут; за ред. док-ра тех. наук, проф. А. С. Довгополого. – Київ : Консалтингова компанія «СІДКОН» ; ВД Дакор, 2021. – 332 с.

ISBN 978-617-95100-3-8

ISBN 978-617-8066-00-0

В книзі розкриті та проаналізовані питання створення національної системи безпеки та стійкості критичної інфраструктури для протидії гібридним загрозам в умовах стрімкого зростання кіберризиків для функціонування критичної інфраструктури.

Надано дієві рекомендації для розбудови державних можливостей гарантувати безпеку суспільства в умовах реалізації багаточисельних гібридних загроз у світі.

Посібник адресований фахівцям з безпеки, у тому числі для практичного використання у процесі діяльності критично важливих об'єктів з метою зниження та нейтралізації загроз безпеці їх функціонування, а також прийняття ефективних управлінських рішень. Цей посібник також буде цікавий студентам економічних спеціальностей ВНЗ, зокрема, які готують фахівців з національної безпеки.

УДК 351.746.1+004.946.5.056

*Всі права на матеріал належать ТОВ «Консалтингова компанія «СІДКОН».
Копіювання або використання фрагментів матеріалу можливе тільки
з письмового дозволу ТОВ «Консалтингова компанія «СІДКОН».*

ISBN 978-617-95100-3-8

ISBN 978-617-8066-00-0

© Когут Ю. І., 2021

© ТОВ «Консалтингова компанія
«СІДКОН», 2021**ЗМІСТ**

ВІДОМОСТІ ПРО АВТОРІВ	10
ПЕРЕДМОВА	12
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	20
ВСТУП	21
РОЗДІЛ 1. КІБЕРВІЙНА В АСПЕКТІ ГЛОБАЛІЗАЦІЇ ТА ЦИФРОВІЗАЦІЇ: АКТУАЛЬНІ ПРОБЛЕМИ НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ КІБЕРБЕЗПЕКИ	24
1.1. Кібервійна: поняття, історія, прояви, характерні ознаки, об'єкти посягань, суб'єкти протистояння, сучасні тенденції	24
1.2. Кібервійна як різновид інформаційних війн. Кібератаки та гібридні форми кібервійн як інструменти впливу на геополітичному рівні	33
1.2.1. Різновиди інформаційних війн	34
1.2.2. Види інформаційно-психологічної та інформаційно- технічної війн	35
1.2.3. Гібридні форми та елементи кібервійни	39
1.2.4. Засади теорії мережевоцентричних (мережевих) війн	45
1.3. Найвідоміші кібератаки на критично важливі об'єкти у світі: історія, типи кібератак	48
1.3.1. Хронологія основних цільових кібератак, реалізованих в Україні за останні декілька років. Кібератака вірус- вимагача Retya.A, а також атака на компанію «Прикарпаттяобленерго»	50
1.3.2. Найбільш відомі та значні за негативними наслідками кібератаки у зарубіжних країнах	57
1.3.2.1. Атака мережевого «хробака» Хелкерна	57

1.3.2.2. Атака мережесих «хробаків» <i>Duqu, Flame та Stuxnet, Gauss і Sputnik. Міждержавна кампанія з кібершпиунства Red October</i>	58
1.3.2.3. Кібератака «хробака»-вимагача <i>WannaCry</i> як найбільшого вірусу-шантажиста в комп'ютерній історії	60
1.3.2.4. Кібератака 2019 р., що викликала блекаут у Венесуелі	62
1.3.2.5. Кібератаки 2008 р. та 2019 р. в Грузії	62
1.3.2.6. Кібератака <i>Sunburst</i> 2020 р. в США	63
1.3.2.7. Систематизація найбільш масштабних кібератак в історії людства проти критичної інфраструктури різних країн світу	65
1.4. Структурна модель поняття «кіберзброя», що застосовується у ході кібервійн. Формування захисту від застосування кіберзброї у міжнародних конфронтаціях	71
1.4.1. Поняття та характеристики кіберзброї. Концептуальна модель використання кіберзброї	73
1.4.2. Фази життєвого циклу кіберзброї	76
1.4.3. Структура кіберзброї	78
1.4.4. Класифікація кіберзброї	79
1.4.5. Види кіберзброї	80
1.4.6. Місце кіберзброї у системі озброєнь. Ознаки кіберзброї. Необхідність поширення дії міжнародного права на використання кіберзброї	81
1.5. Кібервійська провідних держав світу: розроблення заходів стримування, протидії та розгортання кібервійн	86
США	87
КНР	90
Німеччина	91
Російська Федерація	91
Білорусь	92
Ізраїль	92
Північна Корея	93
Естонія	94
Литва	94

<i>Латвія</i>	95
<i>Нідерланди</i>	95
<i>Японія</i>	97
<i>Іспанія</i>	97
1.6. Міжнародні та національні структури, які забезпечують кібербезпеку на державному та глобальному рівнях	98
1.6.1. Особливості діяльності Агентства ЄС з кібербезпеки ENISA (до червня 2019 р. – Європейське агентство з мережевої та інформаційної безпеки)	98
1.6.2. Особливості протидії кіберзагрозам та здійснення кібероборони у країнах – членах НАТО. Органи управління НАТО у сфері кібероборони	101
1.6.3. «Талліннський посібник 2.0 з міжнародного права щодо методів ведення кібернетичних операцій»	103
1.6.4. Суб'єкти національної системи кібербезпеки України	105
1.6.5. Національні структури, які забезпечують кібербезпеку на державному рівні, у зарубіжних країнах	115
<i>США</i>	115
<i>Німеччина</i>	116
<i>Ізраїль</i>	117
<i>Російська Федерація</i>	118
<i>Естонія</i>	119
<i>Литва</i>	120
<i>Нідерланди</i>	123
<i>Великобританія</i>	125
<i>Франція</i>	127
<i>Польща</i>	127
<i>Канада</i>	128
<i>Австрія</i>	129
<i>Іспанія</i>	129
<i>Австралія</i>	130
РОЗДІЛ 2. ЗАГРОЗИ КРИТИЧНІЙ ІНФРАСТРУКТУРИ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ПІДХОДІВ ДО РЕГУЛЮВАННЯ БЕЗПЕКИ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ	132

2.1. Поняття та ознаки критичної інфраструктури в різних країнах. Секторальне охоплення та категоріювання об'єктів критичної інфраструктури	132
2.1.1. Поняття та ознаки критичної інфраструктури в зарубіжних країнах	134
2.1.2. Секторальне охоплення об'єктів критичної інфраструктури в різних країнах	137
2.1.3. Особливості об'єктного та суб'єктно-діяльнісного підходів до регулювання безпеки критичної інформаційної інфраструктури в різних зарубіжних країнах. Категоріювання об'єктів критичної інформаційної інфраструктури	139
2.2. Загрози об'єктам критичної інфраструктури. Використання безпілотних літальних апаратів (БПЛА) проти критично важливих об'єктів	144
2.2.1. Найбільш поширені загрози об'єктам критичної інфраструктури	145
2.2.2. Безпілотні літальні апарати (дрони) як загрози безпеці критичної інфраструктури	147
2.3. Національні суб'єкти забезпечення безпеки об'єктів критичної інфраструктури в зарубіжних країнах	151
<i>США</i>	153
<i>Російська Федерація</i>	156
<i>Казахстан</i>	158
<i>Грузія</i>	160
<i>Євросоюз</i>	161
Порівняльно-правовий аналіз правового статусу невідних суб'єктів забезпечення безпеки критичної інформаційної інфраструктури в зарубіжних країнах	163
2.4. Зарубіжний досвід захисту критичної інфраструктури на прикладі окремих провідних країн світу та на наднаціональному рівні	165

Порівняльно-правовий аналіз підходів до регулювання критичної інформаційної інфраструктури в зарубіжних країнах ..	163
<i>Німеччина</i>	170
<i>США</i>	172
<i>Великобританія</i>	193
<i>Франція</i>	194
<i>Японія</i>	195
<i>Китай</i>	197
<i>Фінляндія</i>	199
<i>Нідерланди</i>	200
<i>Польща</i>	201
<i>Угорщина</i>	202
<i>Словаччина</i>	203
<i>Чехія</i>	205
<i>Румунія</i>	206
<i>ЄС: наднаціональне регулювання у сфері безпеки критичної інфраструктури, зокрема інформаційної</i>	207
<i>Російська Федерація</i>	210
<i>Сінгапур</i>	212
<i>Казахстан</i>	214
2.5. Міжнародні, наднаціональні нормативні правові акти, стандарти та керівництва в галузі регулювання критичної інфраструктури та протидії гібридним загрозам. Стандарти та ініціативи НАТО з протидії гібридним загрозам та захисту критично важливих об'єктів	217
2.5.1. Екскурс в історію розроблення національних нормативних правових актів у галузі регулювання критичної інфраструктури	217
2.5.2. Нормативно-правова база ЄС з питань захисту кіберпростору, безпеки в галузі регулювання критичної інфраструктури та протидії гібридним загрозам. Нова стратегія Євросоюзу з кібернетичної безпеки 2020 р., Директива NIS	220
2.5.3. Ініціативи НАТО щодо протидії гібридним загрозам	231

2.5.4. Стандарти та ініціативи НАТО щодо захисту критичної інфраструктури та протидії кіберзагрозам	235
2.5.5. Інструментарій НАТО зі стримування гібридних загроз	247
2.6. Правові засади кіберзахисту критично важливих об'єктів України	252
2.6.1. Системоутворюючі (базові) нормативно-правові акти України у сфері кібербезпеки критичної інфраструктури	252
2.6.2. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури України	257
РОЗДІЛ 3. КРИТИЧНА ІНФРАСТРУКТУРА: УПРАВЛІННЯ РИЗИКАМИ ТА НАПРЯМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ	259
3.1. Управління ризиками критичної інфраструктури: превентивні заходи, розроблення стратегії та впровадження кризового менеджменту на її об'єктах	259
3.1.1. Розкриття змісту процесу управління ризиками критичної інфраструктури	259
3.1.2. Розроблення стратегії управління ризиками та кризами щодо критичної інфраструктури. Превентивні заходи та кризовий менеджмент щодо забезпечення безпеки критичної інфраструктури	262
3.1.3. Ризик-орієнтовані підходи щодо критичної інфраструктури, використовувані у провідних країнах світу	267
3.2. Місія, цілі та завдання із забезпечення безпеки та стійкості критичної інфраструктури як важливої складової національної безпеки держави. Використання безпілотних літальних апаратів (дронів, БПЛА) для забезпечення захисту критичної інфраструктури	270
3.2.1. Місія, цілі та завдання із забезпечення безпеки та стійкості критичної інфраструктури	270
3.2.2. Використання БПЛА для захисту критичної інфраструктури	272

3.3. Вимоги до кадрів та підрозділів, які забезпечують безпеку об'єктів критичної інфраструктури, специфічні умови їх підготовки та атестації	275
3.4. Аудит критичної інформаційної інфраструктури: цілі, завдання, особливості, етапи, схема проведення	282
3.4.1. Особливості проведення аудиту критичної інформаційної інфраструктури	283
3.4.2. Цілі та завдання аудиту критичної інформаційної інфраструктури	284
3.4.3. Етапи та формальна процедура проведення аудиту об'єкта критичної інформаційної інфраструктури	285
3.5. Створення комплексної системи захисту критичної інфраструктури та протидії кібервійнам у державі	292
ВИСНОВКИ	307
ДОДАТОК	310
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	317