

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

І. В. Діордіца

**КІБЕРБЕЗПЕКОВА ПОЛІТИКА УКРАЇНИ:
стан та пріоритетні напрями забезпечення**

Монографія

Запоріжжя
Видавничий дім «Гельветика»
2017

УДК 351.86:004.5(477)
Д 46

Рекомендовано до друку Вченою радою
Запорізького національного університету
(протокол № 3 від 31 жовтня 2017 р.)

Рецензенти:

О. П. Світличний – доктор юридичних наук, доцент, професор кафедри адміністративного та фінансового права Національного університету біоресурсів і природокористування України;

Я.В. Лазур – доктор юридичних наук, професор, декан юридичного факультету ДВНЗ «Ужгородський національний університет»;

І. М. Рижев – доктор юридичних наук, доцент, віце-президент Академії безпеки відкритого суспільства

Діордіца І. В.

Д 46 **Кібербезпекова політика України: стан та пріоритетні напрями забезпечення** : монографія / І. В. Діордіца. – Запоріжжя : Видавничий дім «Гельветика», 2017. – 548 с.

ISBN 978-966-916-500-8

Монографію присвячено теоретико-правовим засадам формування та розвитку кібербезпекової політики в Україні. У роботі визначено такі поняття: «кібербезпекова політика», «кібернетична функція держави», «правовий режим кібербезпекової політики», «коннотація кіберпростору», «homo cyberus», «аксіологія кіберпростору», «кіберосвіта».

Проаналізовано стан вітчизняних нормативно-правових актів, що регулюють інформаційні відносини у сфері кібербезпеки. Визначено основні ознаки кібербезпекової функції та політики. Охарактеризовано складові правовідносин, що виникають та складаються у сфері кібербезпеки. Визначено правову природу загроз у сфері кібербезпеки, напрями розбудови національної системи кібербезпеки. Окреслено особливості правового режиму кібербезпекової політики в окремих країнах, а також підготовки фахівців у сфері кібербезпеки.

Для науковців, викладачів, студентів та слухачів юридичних факультетів і закладів освіти, а також працівників безпекові сфери.

УДК 351.86:004.5(477)

ISBN 978-966-916-500-8

© І. В. Діордіца, 2017
© Запорізький національний університет, 2017

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	9
ВСТУП	10
РОЗДІЛ 1	
КОНЦЕПТУАЛЬНІ ЗАСАДИ	
КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ.....	13
1.1. Стан наукових досліджень за темою роботи	13
1.1.1. <i>Роботи, в яких предметом виступають різноманітні аспекти розвитку інформаційного суспільства, інформаційної влади та реалізації інформаційної політики</i>	<i>17</i>
1.1.2. <i>Роботи, в яких предметом виступає інформаційна безпека</i>	<i>31</i>
1.1.3. <i>Роботи, в яким предметом виступають функції держави</i>	<i>42</i>
1.1.3.1. <i>Роботи за окремими функціями держави</i>	<i>44</i>
1.1.3.1.1. <i>Соціальна функція держави.....</i>	<i>44</i>
1.1.3.1.2. <i>Правоохоронна та правозахисна функції держави.....</i>	<i>46</i>
1.1.3.1.3. <i>Економічна функція держави.....</i>	<i>46</i>
1.1.3.1.4. <i>Внутрішні та зовнішні функції.....</i>	<i>47</i>
1.1.4. <i>Роботи, в яких предметом виступають правові режими окремих видів інформації.....</i>	<i>55</i>
1.1.5. <i>Роботи, в яких предметом виступають різноманітні аспекти адміністративно-правової відповідальності</i>	<i>57</i>
1.1.6. <i>Роботи, в яких предметом виступають різноманітні аспекти права на доступ до інформації.....</i>	<i>59</i>
1.2. Мультиплікативність правових засад формування концептосфери кібербезпекової політики	66
1.2.1. <i>Юридико-лінгвістичні засади формування концептосфери кібербезпекової політики</i>	<i>67</i>

1.2.2. Кібернетичний простір vs інформаційний в контексті правничої герменевтики	74
1.2.3. Репрезентація термінології кібербезпекової політики у текстах нормативно-правових актів України	83
1.3. Засади формування кібернетичної функції держави	90
1.3.1. Основні поняття та ідеї кібернетики як засади кібернетичної функції держави	90
1.3.2. Чинники формування кібернетичної функції	96
1.3.2.1. Позитивні	96
безпековий блок:	96
світоглядний блок:	98
кібернетичний блок:	98
інфраструктурний блок:	100
блок стратегічних комунікацій:	100
правовий блок:	101
фінансово-економічний блок:	103
1.3.2.2. Негативні	104
світоглядний блок:	104
безпековий блок:	105
інфраструктурний блок:	106
організаційний блок:	108
інформаційний блок:	109
кримінальний блок:	111
правовий блок:	111
фінансово-економічний блок:	113
1.3.3. Ознаки функцій держави	114
1.3.4. Ознаки кібернетичної функції держави	116
1.3.5. Тенденції розвитку кібернетичної функції держави	119
1.3.6. Очікувані результати від реалізації кібернетичної функції	122
1.3.7. Детермінованість кібербезпекової політики кібернетичною функцією	123
1.3.9. Мета кібернетичної функції держави	128
1.3.10. Принципи кібербезпеки	130
Висновки до першого розділу	131

РОЗДІЛ 2

МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ..... 140

2.1. Методологічні підходи до дослідження кібербезпекової політики.....	144
2.1.1. Тектологічний підхід.....	144
2.1.2. Кібернетика і кібернетичний підхід.....	154
2.1.3. Системний підхід.....	161
2.1.4. Матричний підхід.....	163
2.1.5. Аксиологічний потенціал кіберпростору.....	164
2.1.6. Гіперболічна теорія розвитку кіберпростору.....	166
2.2. Засади кібернетичної деонтології.....	171
2.2.1. Зміст кібернетичної деонтології через співвідношення категорій: <i>суцє та належне</i>	172
2.2.3. <i>Поняття, мета, завдання, об'єкти та предмет, завдання кібернетичної деонтології</i>	183
2.2.4. <i>Принципи кібернетичної деонтології</i>	186
2.2.5. <i>Функції кібернетичної деонтології</i>	188
2.2.6. <i>Висновки щодо кібернетичної деонтології</i>	194
Висновки до другого розділу.....	196

РОЗДІЛ 3

ПРАВОВА ПРИРОДА ЗАГРОЗ КІБЕРБЕЗПЕЦІ УКРАЇНИ

НА СУЧАСНОМУ ЕТАПІ ДЕРЖАВОТВОРЕННЯ..... 200

3.1. Поняття та зміст кіберзагроз на сучасному етапі.....	200
3.1.1. <i>Нормативно-правові підходи до визначення поняття „кіберзагроз”</i>	203
3.1.2. <i>Доктринальні визначення поняття кіберзагроз та теоретичні проблеми їх легітимації у нормативно-правових актах</i>	206
3.1.3. <i>Життєво важливі інтереси в інформаційній сфері</i>	210
3.1.4. <i>Смислові війни</i>	213
3.1.5. <i>Критичні об'єкти національної інформаційної інфраструктури</i>	214

3.1.6. Міжнародна статистика кіберінцидентів	218
3.2. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України.....	221
3.2.1. Джерела кібернетичних загроз.....	224
3.2.2. Об'єкти, на які спрямовано дію кіберзагроз.....	225
3.2.3. Перелік кіберзагроз для України	226
3.2.4. Чинники, що актуалізують загрози кібербезпеці.....	228
3.2.5. Мережеві загрози також поділяються на три види	229
3.3. Кіберзлочинність як загроза кібербезпеці України.....	231
3.3.1. Поняття кіберзлочинності	234
3.3.2. Поняття кіберзлочину.....	237
3.4. Кібершпигунство як загроза кібербезпеці України	242
3.5. Кібертероризм як загроза кібербезпеці України.....	261
3.6. Інформаційні інтервенції як загроза кібербезпеці України ...	276
Висновки до третього розділу	288

РОЗДІЛ 4

ПРАВОВИЙ ВИМІР ЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ 295

4.1. Правовий зміст національної системи кібербезпеки України.....	295
4.2. Національна система кібербезпеки як складова системи забезпечення національної безпеки України	303
4.2.1. Поняття національної системи кібербезпеки	306
4.2.2. Міжнародний досвід формування національних систем кібербезпеки.....	310
4.3. Правовий зміст системи забезпечення кібербезпеки.....	316
4.3.1. Чинники, що зумовлюють необхідність формування системи забезпечення кібербезпеки	318
4.3.2. Поняття системи забезпечення кібербезпеки.....	321
4.3.3. Зміст та призначення системи забезпечення кібербезпеки.....	324
4.3.3.1. Завдання СЗКБ.....	325

4.3.3.2. <i>Нормативно-правове регулювання діяльності суб'єктів забезпечення кібербезпеки</i>	326
4.3.4. <i>Об'єкти правовідносин у сфері кібербезпеки</i>	336
4.3.5. <i>Зміст правовідносин у сфері кібербезпеки</i>	337
4.3.6. <i>Проблеми управління СЗКБ</i>	345
4.4. <i>Правове регулювання діяльності суб'єктів національної системи кібербезпеки</i>	347
4.4.1. <i>Поняття суб'єктів забезпечення кібербезпеки</i>	348
4.4.2. <i>Загальні та спеціальні суб'єкти забезпечення кібербезпеки</i>	350
4.4.3. <i>CERT-UA як спеціальний суб'єкт забезпечення кібербезпеки України</i>	353
4.4.4. <i>Повноваження спеціальних суб'єктів забезпечення кібербезпеки України</i>	358
4.4.5. <i>Функціональна модель системи забезпечення кібербезпеки</i>	367
4.4.6. <i>Рефлексія „кібербезпеки” у Щорічних посланнях Президента України</i>	371
Висновки до четвертого розділу	376

РОЗДІЛ 5

МАГІСТРАЛЬНІ НАПРЯМИ УДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ УКРАЇНИ

384

5.1. <i>Напрями оптимізації правового регулювання державної кібербезпекової політики</i>	384
5.1.1. <i>Сучасний правовий зміст державної кібербезпекової політики</i>	385
5.1.1.1. <i>Напрями ДПГБ відповідно до ЗУ „Про основні засади забезпечення кібербезпеки України”</i>	388
5.1.1.2. <i>Напрями ДПГБ відповідно до ЗУ „Про основи національної безпеки України”</i>	390
5.1.1.3. <i>Напрями ДПГБ відповідно до Доктрини інформаційної безпеки України</i>	393
5.1.1.4. <i>Напрями ДПГБ стосовно Національного координаційного центру кібербезпеки при РНБОУ</i>	395

5.1.1.5. Стосовно посилення інформаційної безпеки.....	395
5.1.1.6. Напрями ДКБП досвід Великої Британії.....	396
5.2. Засади правового регулювання діяльності агентів впливу при реалізації кібербезпекової політики.....	397
5.2.1. Поняття агентів впливу.....	398
5.2.2. Поняття лобювання.....	399
5.2.2.1. Риси лобізму.....	401
5.2.2.2. Функції лобізму.....	403
5.2.2.3. Лобізм в Україні.....	404
5.2.2.4. Форми лобізму.....	407
5.2.2.5. Поняття „лобіст”.....	407
5.2.2.6. Методи та форми лобістської діяльності.....	410
5.3. Правове регулювання формування кіберосвіти в Україні як напрям підвищення ефективності державної кібербезпекової політики.....	412
5.3.1. Правові та організаційні засади формування фахівців із кібербезпеки.....	412
5.3.2. Стан підготовки фахівців у сфері кібербезпеки.....	419
5.3.3. Напрями підготовки та підвищення кваліфікації фахівців із кібербезпеки.....	428
5.3.4. Освітні стандарти підготовки фахівців із кібербезпеки.....	436
5.3.5. Кваліфікаційні вимоги до компетенцій фахівців із кібербезпеки.....	444
5.3.6. Оцінка фахівців з кібербезпеки як один із засобів їх формування та підвищення ефективності професійної діяльності.....	451
5.3.7. Удосконалення нормативно-правового регулювання професійної діяльності суб'єктів кібербезпекової політики.....	458
Висновки до п'ятого розділу.....	465
ВИСНОВКИ.....	470
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	476