

# ЗМІСТ

---

<b>ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ .....</b>	<b>9</b>
<b>ВСТУП .....</b>	<b>10</b>
<b>РОЗДІЛ 1</b>	
<b>КОНЦЕПТУАЛЬНІ ЗАСАДИ</b>	
<b>КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ.....</b>	<b>13</b>
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
<b>ВИСНОВКИ.....</b>	<b>470</b>
<b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ .....</b>	<b>476</b>

## ВСТУП

---

Сучасна безпекова ситуація як у державі, так і світі суттєво змінюється, що є поштовхом для розвитку якісно нових регуляторів, які у своєму арсеналі матимуть ефективні важелі впливу на нові суспільні відносини в кібернетичній сфері.

Ключовим завданням державної кібербезпекової політики дедалі виразніше виступає створення гарантованих умов реалізації національних інтересів у кіберпросторі. Даний процес уможливується завдячуючи розвитку ефективної системи правового регулювання реалізації кібербезпекової політики. Важливим завданням у даному ракурсі також виступають формування успішного, кіберграмотного та кіберосвіченого кіберсуспільства, здатного стати рушієм технологічного прориву України у сфері кібербезпеки, каталізатором розвитку держави в умовах перманентних трансформаційних змін та інформаційної глобалізації.

У правовій доктрині поняття кібербезпекової політики майже не розроблялося, а у поодиноких публікаціях, кібербезпека здебільшого інтерпретується в рамках концепту інформаційної політики, що наперед звучує як сам феномен, так і його розуміння та подальший аналіз. У науці адміністративного права проблематика кібербезпекової політики розглядалася переважно під кутом вивчення окремих компетенцій певних суб'єктів публічної адміністрації, в рамках окремих елементів адміністративно-правових режимів.

Методологія формування та розвитку державної кібербезпекової політики вже частково закладена в наукових та навчальних працях вітчизняних дослідників адміністративного та інформаційного права і політики, зокрема таких, як: В. Б. Авер'янов, О. Ф. Андрійко, І. В. Арістова, К. І. Беляков, В. М. Брижко, В. І. Гурковський, С. Ф. Джерджа, Б. А. Кормич, О. В. Кохановська, І. Ю. Крегул, Г. М. Красноступ, В. А. Ліпкан, Є. А. Макаренко, А. І. Марущак, Н. Р. Нижник, Н. Б. Новицька, А. М. Новицький, В. Д. Павловський, О. П. Світличний, І. М. Сопілко, В. Ю. Степанов, В. С. Цимбалюк, М. Я. Швець тощо.

Окремі засадничі положення державної кібербезпекової політики також розглядалися і в роботах зарубіжних дослідників: О. Б. Агапова, Ю. М. Батуріна, І. Л. Бачило, Д. Белла, А. Б. Венгерова,

О. О. Гаврилова, Б. Гейтса, М. Кастельса, В. О. Копилова, Й. Курбалія, В. Н. Лопатіна, М. М. Россолова, Ю. А. Тіхомірова, Е. Тофлера, М. А. Федотова, Х. Цинь та інших.

У дослідженні застосовані наукові та практичні підходи, що висвітлені у наукових доробках деяких фахівців, серед яких: К. О. Данилишина, В. Н. Денисов, А. В. Задорожній, І. А. Кадієвська, І. А. Кисарець, Е. Б. Кубко, Є. А. Макаренко, В. К. Мамутов, С. Є. Мартинюк, В. І. Муравйов, В. П. Нагребельний, Г. П. Несвіт, Н. М. Пархоменко, П. М. Рабінович, Н. Ф. Селивон, О. В. Скрипнюк, В. В. Цветков, Г. І. Чанишев, Р. І. Чанишев, Ю. С. Шемшученко, О. І. Ющик.

Питанням безпосередньо розвитку кіберсуспільства, формування кібербезпекової політики присвячені наукові розвідки таких дослідників, як: А. В. Баровська, В. М. Бутузов, О. О. Григор, Д. В. Дубов, О. М. Ємельяненко, О. В. Єропудова, Є. О. Калашнюк, Г. В. Камаралі, А. В. Камуз, М. Г. Карашук, В. О. Кірьян, О. П. Климентьєв, О. Г. Кривоконь, В. І. Кушерець, О. В. Литвиненко, О. В. Логінова, О. О. Маруховський, Г. П. Несвіт, О. В. Оверчук, Г. Г. Почепцов, О. О. Проскуріна, С. О. Руденко, А. Л. Свящук, А. В. Тунік, О. В. Чуприна, В. П. Шеломенцев, А. В. Яковець та ін.

Окремо виділю доробок представників наукової школи доктора юридичних наук В. А. Ліпкана, в рамках якої системно досліджуються різноманітні правові аспекти формування та реалізації державної інформаційної та кібербезпекової політики. Це роботи: Є. Є. Бамбізова, В. Ю. Баскакова, В. М. Вац, М. І. Дімчогло, О. О. Дьоміної, М. Ю. Довганя, В. А. Залізняка, Є. Ф. Збінського, В. Ю. Кобринського, О. В. Кушнір, А. М. Лободи, В. В. Майорова, О. А. Мандзюка, Ю. Є. Максименко, П. Є. Матвієнко, О. Г. Мовчуна, В. Є. Політила, Л. І. Рудник, О. В. Стоєцького, К. Г. Татарникової, О. О. Ткаченка, О. В. Топчий, К. П. Череповського, О. В. Шепети.

Однак, незважаючи на значний масив наукової літератури, питанням правового регулювання побудови системи кібербезпеки і реалізації державної кібербезпекової політики приділялось за мало уваги.

Більше того, в наукових джерелах не визначено методологічних засад дослідження кібербезпекової політики, через що недостатньою мірою акцентовано на аксіологічному потенціалі кіберпростору, не акцентовано уваги на цінності розуміння кіберпростору як окремого та самостійного простору.

Окремою новелою монографії є формування автором концепції теорії гіперболічного розвитку кіберпростору через застосування системного, міждисциплінарного та кібернетичного підходів.

Проведене дослідження виконано відповідно до основних положень Закону України „Про основні засади забезпечення кібербезпеки України” від 05.10.2017 р., набуває чинності з 09.05.2018 р., Стратегії кібербезпеки України, уведеної в дію Указом Президента України від 15 березня 2016 року № 96/2016, Положення „Про Національний координаційний центр кібербезпеки” від 07.06.2016 р.; указів Президента України „Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року „Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації” від 13 лютого 2017 року № 32/2017, „Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року „Про Доктрину інформаційної безпеки України” від 25 лютого 2017 року № 47/2017, № 398/2014 „Про інформаційно-аналітичний центр” від 12 квітня 2014 року., № 449/2014 „Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року „Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” від 1 травня 2014 року, Дорожньої карти Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО.

Головною *метою* дослідження, результати якого викладені в монографії, виступає обґрунтування і формулювання концептуальних засад щодо правової природи, методологічних засад формування засад правового регулювання державної кібербезпекової політики України.

Сформовані у роботі висновки та пропозиції визначають напрями удосконалення правового регулювання державної кібербезпекової політики України.

Зважаючи на складність роботи та її наукову новизну, автор усвідомлює, що монографія не позбавлена певних дискусійних положень щодо сутності та змісту правового регулювання державної кібербезпекової політики, зокрема й суб'єктного складу правовідносин, куди автором пропонується включити штучний інтелект. Проте хочу висловити сподівання на те, що отримані наукові здобутки сприятимуть розвитку теорії адміністративно-правового регулювання державної кібербезпекової політики.