

ГЛОБАЛЬНА ОРГАНІЗАЦІЯ СОЮЗНИЦЬКОГО ЛІДЕРСТВА  
АКАДЕМІЯ БЕЗПЕКИ ВІДКРИТОГО СУСПІЛЬСТВА  
АКАДЕМІЯ НАУК ВИЩОЇ ОСВІТИ УКРАЇНИ

В. А. ЛІПКАН, В. Ю. БАСКАКОВ

**АДМІНІСТРАТИВНО-ПРАВОВИЙ  
РЕЖИМ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ  
ДОСТУПОМ В УКРАЇНІ**

*Монографія*

*За загальною редакцією В.А.Ліпкана*

Київ  
ФОП О. С. Ліпкан  
2013

УДК 354.42/44  
ББК Х621  
Л 613

*Рецензенти:*

- Р. А. Калюжний** — доктор юридичних наук, професор, заступник директора Юридичного інституту Національного авіаційного університету;
- В. С. Цимбалюк** — кандидат юридичних наук, старший науковий співробітник, старший науковий співробітник Науково-дослідного центру правової інформатики Національної академії правових наук України
- М. Я. Швець** — доктор економічних наук, професор, член-кореспондент Національної академії правових наук України, професор кафедри інформаційних технологій Національної академії внутрішніх справ

**Ліпкан В. А.**

**Л 613** **Адміністративно-правовий режим інформації з обмеженим доступом в Україні**: [Монографія] / В. А. Ліпкан, В. Ю. Баскаков / За заг. ред. В. А. Ліпкана. — К. : ФОП О. С. Ліпкан, 2013. — 344 с.

ISBN 978-966-2439-45-8

Монографію присвячено теоретичним та адміністративно-правовим проблемам інформації з обмеженим доступом в Україні. У роботі визначено такі поняття, як інформація з обмеженим доступом, адміністративно-правовий режим інформації з обмеженим доступом, конфіденційна інформація, таємна інформація. Визначено основні ознаки інформації з обмеженим доступом в адміністративно-правовому контексті, виділено основні види такої інформації, охарактеризовано складові адміністративно-правового режиму інформації з обмеженим доступом в Україні, а також окреслено специфіку адміністративно-правових режимів державної таємниці та персональних даних (інформації про особу) як найбільш важливих видів інформації з обмеженим доступом.

З метою подальшого вдосконалення адміністративно-правового режиму інформації з обмеженим доступом було запропоновано внести відповідні зміни та доповнення до вітчизняного законодавства у цій сфері.

Монографія буде корисною аспірантам, науковим та практичним працівникам та усім, хто цікавиться питаннями розбудови ефективного інформаційного суспільства в Україні.

УДК 354.42/44  
ББК Х621

ISBN 978-966-2439-45-8

© ФОП О. С. Ліпкан, 2013.  
© В. А. Ліпкан, В. Ю. Баскаков, 2013.

GLOBAL ORGANIZATION OF ALLIED LEADERSHIP  
ACADEMY OF OPEN SOCIETY SECURITY  
ACADEMY OF SCIENCE OF HIGH EDUCATION OF UKRAINE

V. A. LIPKAN, V. J. BASKAKOV

**ADMINISTRATIVE AND LEGAL REGIME  
OF INFORMATION WITH LIMITED  
ACCESS IN UKRAINE**

*Monograph*

*Edited by V. A. Lipkan*

Kyiv  
Publisher O. S. Lipkan  
2013



**Publisher O. S. Lipkan**

***Administrative and legal regime of information with limited access in Ukraine***

*V. A. Lipkan, V. J. Baskakov*

Development Editor: Vataliy Tsybalyuk  
Assistant Editor: Rostislav Kaluzny  
Aditorial Assitant: Mykola Shwetz  
Technology Project Manager: Catrin Boyko  
Marketing Manager: Irina Mychaylenko  
Marketing Communication Manager: Olena Lipkan  
Art Director: Olexander Novikov  
Print Buyer: Dmytro Lepeshin

Permission Editor: Olga Mashkova  
Text Designer: Volodymyr Lipkan  
Photo researcher: Galina Lipkan  
Copy Editor: Olena Lipkan  
Illustrator: Olexander Novikov  
Cover Printer: Dorado Druk  
Printer: Dorado Druk  
Pro Bono Advisor: Alexander Mitroff

© 2013, O.S.Lipkan.

© V.A. Lipkan, V. J. Baskakov

ALL RIGHTS RESERVED. No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means — graphic, electronic, or mechanical, including photocopying, recording, taping, Web distribution, information storage and retrieval systems, or in any other manner — without the written permission of publisher/

For more information about our products, contact us at:

**[www.natsecurity.com.ua](http://www.natsecurity.com.ua); [www.goal-int.org](http://www.goal-int.org)**

For permission to use material from this text or product, submit a request at:

**[wlademic@gmail.com](mailto:wlademic@gmail.com)**

Any additional questions about permissions can be submitted by email to

**[goalleadership@gmail.com](mailto:goalleadership@gmail.com)**

Printed in Ukraine

ISBN 978-966-2439-45-8

**Lipkan V. A.**

**L 613 Administrative and legal regime of information with limited access in Ukraine** : [monograph] / V. A. Lipkan, V. J. Baskakov / Edited by V. A. Lipkan. — K. : O. S. Lipkan, 2013. — 344 p.

ISBN 978-966-2439-45-8

The monograph is devoted to theoretical and administrative and legal problems of protection of information with limited access in Ukraine. The paper defines the concepts of information with limited access, administrative and legal regime of such information, confidential information, secret information.

The main features of information with limited access in the administrative and legal context, highlighted the main types of such information, described the administrative and legal regime of information with limited access in Ukraine, and also outlines specific administrative and legal regimes of protection of state secrets and personal data (information about a person ) as the most important types of information with limited access.

To further improve the administrative and legal regulation and practice of national legislation on protection of information with limited access has been requested a number of measures.

Monograph will benefit graduate students, researchers and practitioners, and all those interested in gaining information society.

# ЗМІСТ

<b>BRIEF CONTENTS</b> .....	<b>10</b>
<b>CONTENTS</b> .....	<b>12</b>
<b>ПЕРЕДНЄ СЛОВО</b> .....	<b>17</b>
<b>PREFACE</b> .....	<b>20</b>
<b>ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ</b> .....	<b>23</b>
<b>ВСТУП</b> .....	<b>24</b>
<b>РОЗДІЛ I. РІВЕНЬ НАУКОВОГО РОЗРОБЛЕННЯ</b>	
<b>ПРОБЛЕМИ ТА МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ</b> .....	<b>29</b>
1.1 Бібліографія за темою дослідження .....	31
<i>Роботи з інформаційної безпеки</i> .....	32
<i>Роботи з інформаційного права</i> .....	45
<i>Роботи, присвячені безпосередньо різним аспектам</i> <i>інформації з обмеженим доступом (спеціалізовані роботи)</i> ..	58
1.2 Методологічні засади дослідження адміністративно- правового режиму інформації з обмеженим доступом .....	64
1.3 Понятійно-категорійний апарат дослідження .....	76
<i>Поняття «інформація з обмеженим доступом» у</i> <i>нормативно-правових актах</i> .....	77
<i>Поняття «інформація з обмеженим доступом» в</i> <i>доктринальних джерелах</i> .....	84
<b>РОЗДІЛ II. КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ</b>	
<b>З ОБМЕЖЕНИМ ДОСТУПОМ</b> .....	<b>89</b>
2.1 Класифікація інформації з обмеженим доступом у вітчизняному законодавстві .....	91

2.2 Класифікація інформації з обмеженим доступом в доктринальних джерелах .....	96
---	----

## **РОЗДІЛ III. ПОНЯТТЯ ТА СТРУКТУРА АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ ..... 107**

3.1 Зміст адміністративно-правового режиму інформації з обмеженим доступом в Україні. ....	109
<i>Поняття «режим»</i> .....	109
<i>Поняття «правовий режим»</i> .....	111
<i>Етапи становлення вчення про адміністративно-правовий режим</i> .....	113
<i>Поняття «адміністративно-правовий режим»</i> .....	115
<i>Ознаки адміністративно-правового режиму</i> .....	117
<i>Поняття «адміністративно-правовий режим інформації з обмеженим доступом»</i> .....	118
<i>Ознаки адміністративно-правового режиму інформації з обмеженим доступом</i> .....	118
<i>Класифікація адміністративно-правових режимів</i> .....	119
<i>Класифікація адміністративно-правового режиму інформації з обмеженим доступом</i> .....	122
3.2 Характеристика елементів адміністративно-правового режиму інформації з обмеженим доступом в Україні .....	123
<i>Підходи щодо розуміння структури адміністративного режиму</i> .....	123
<i>Мета адміністративно-правового режиму інформації з обмеженим доступом</i> .....	125
<i>Правові принципи адміністративно-правового режиму інформації з обмеженим доступом</i> .....	127
<i>Об'єкт адміністративно-правового режиму інформації з обмеженим доступом</i> .....	130
<i>Метод адміністративно-правового режиму інформації з обмеженим доступом</i> .....	132
<i>«Режимні правила» адміністративно-правового режиму інформації з обмеженим доступом</i> .....	133
<i>Спеціальні державні органи як елемент адміністративно-правового режиму інформації з обмеженим доступом</i> .....	135

Верховна Рада України як суб'єкт захисту інформації з обмеженим доступом .....	139
Президент України як суб'єкт захисту інформації з обмеженим доступом .....	144
Рада національної безпеки і оборони України (РНБО України) та Кабінет Міністрів України як суб'єкти захисту інформації з обмеженим доступом. ....	145
Органи виконавчої влади як суб'єкти захисту інформації з обмеженим доступом .....	148
Відповідальність за порушення режимних норм .....	160
Просторово-часові межі чинності адміністративно-правового режиму інформації з обмеженим доступом .....	163
<b>3.3 Удосконалення адміністративно-правового режиму інформації з обмеженим доступом .....</b>	<b>164</b>
<i>Етапи систематизації інформаційного законодавства .....</i>	<i>165</i>
<i>Напрями інкорпорації .....</i>	<i>167</i>
<i>Напрями консолідації. ....</i>	<i>169</i>
<i>Напрями кодифікації .....</i>	<i>171</i>
<i>Підходи до розроблення Інформаційного кодексу. ....</i>	<i>174</i>
<i>Проект М.Швеця та В. Брижка .....</i>	<i>175</i>
<i>Проект В. Цимбалюка .....</i>	<i>176</i>
<i>Проект Держкомтелерадіо. ....</i>	<i>179</i>
<i>Проект В. Ліпкана та В. Залізняка .....</i>	<i>181</i>

## **РОЗДІЛ IV. ОСОБЛИВОСТІ АДМІНІСТРАТИВНО-ПРАВОВИХ РЕЖИМІВ ОКРЕМИХ ВИДІВ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ. .... 185**

<b>4.1 Адміністративно-правовий режим державної таємниці .....</b>	<b>188</b>
<i>Нормативно-правове регулювання суспільних відносин у сфері державної таємниці .....</i>	<i>188</i>
<i>Поняття «державна таємниця» .....</i>	<i>191</i>
<i>Система органів, що покликані забезпечити захист державної таємниці .....</i>	<i>193</i>
<i>Етапи віднесення інформації до державної таємниці .....</i>	<i>194</i>
<i>Звід відомостей, що становлять державну таємницю .....</i>	<i>195</i>
<i>Строки, протягом яких діє рішення про віднесення інформації до державної таємниці .....</i>	<i>196</i>

Перелік інформації, що не може бути віднесена до державної таємниці . . . . .	197
Відповідальність за порушення законодавства у сфері державної таємниці . . . . .	198
Основні причини вчинення адміністративних порушень законодавства про державну таємницю . . . . .	200
Перспективи розвитку адміністративно-деліктного законодавства у сфері захисту державної таємниці. . . . .	202
4.2 Адміністративно-правовий режим персональних даних (інформація про фізичну особу) . . . . .	206
Історія ухвалення Закону України «Про захист персональних даних» . . . . .	209
Основні засади Закону України «Про захист персональних даних» . . . . .	210
Дефініція «персональних даних» . . . . .	216
Відомості, що відносяться до персональних даних. . . . .	216
Суб'єкти захисту персональних даних . . . . .	220
Процедура оформлення згоди суб'єкта персональних даних на використання його даних. . . . .	222
Юридична відповідальність за порушення законодавства у сфері захисту персональних даних. . . . .	223
4.3 Адміністративно-правовий режим службової інформації . . . . .	227
Історія становлення інституту службової інформації . . . . .	227
Сучасний стан нормативно-правового регулювання суспільних відносин у сфері службової інформації. . . . .	231
Перелік відомостей, що становить службову інформацію . . . . .	232
Поняття «службова інформація» у доктринальних джерелах. . . . .	242
Поняття «службова інформація» у нормативно-правових актах . . . . .	245
Ознаки службової інформації . . . . .	247
Співвідношення понять «службова таємниця» та «державна таємниця» . . . . .	248
Співвідношення понять «службова таємниця» і «професійна таємниця» . . . . .	250
Охорона документів, що мають гриф «Для службового користування» . . . . .	252
<b>ВИСНОВКИ . . . . .</b>	<b>254</b>



<b>CONCLUSIONS</b> .....	<b>263</b>
<b>ТЕЗАУРУС</b> .....	<b>271</b>
<b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ</b> .....	<b>288</b>
<b>КОРИСНА БІБЛІОГРАФІЯ ЗА ТЕМОЮ ДОСЛІДЖЕННЯ</b> .....	<b>302</b>
<i>Праці наукової школи Ліпкана В. А. з інформаційної тематики</i> .	302
<i>Інформація з обмеженим доступом</i> .....	309
<i>Адміністративно-правові режими</i> .....	325
<i>Кримінально-правові та криміналістичні дослідження</i> <i>інформаційної сфери</i> .....	326
<i>Праці В.А.Ліпкана щодо системи знань про безпеку</i> .....	328
<i>Угоди з інформаційних питань</i> .....	330
<i>Інформаційне право та інформаційна безпека</i> .....	331
<b>СЛОВА ДЯКИ</b> .....	<b>339</b>



# BRIEF CONTENTS

<b>PART 1. THE LEVEL OF SCIENCE RESEARCH AND ITS CORE METHODOLOGY</b> .....	<b>29</b>
Chapter 1. Bibliography of research .....	31
Chapter 2. Methodological basis of research .....	64
Chapter 3. Key definitions of research .....	76
<b>PART 2. CLASSIFICATION OF INFORMATION WITH LIMITED ACCESS</b> .....	<b>89</b>
Chapter 1. Classification of information with limited access in Ukrainian legislation .....	91
Chapter 2. Classification of information with limited access in doctrinal sources .....	96
<b>PART 3. THE DEFINITION AND STRUCTURE OF ADMINISTRATIVE AND LEGAL REGIME OF INFORMATION WITH LIMITED ACCESS IN UKRAINE</b> .....	<b>107</b>
Chapter 1. The essence of administrative and legal regime of information with limited access in Ukraine .....	109
Chapter 2. Characteristics of the elements of administrative and legal regime of information with limited access in Ukraine .....	123
Chapter 3. Improvement of administrative and legal regime of information with limited access in Ukraine .....	164
<b>PART 4. FEATURES OF ADMINISTRATIVE AND LEGAL REGIMES OF CERTAIN TYPES OF INFORMATION WITH LIMITED ACCESS</b> .....	<b>185</b>
Chapter 1. Administrative and legal regime of state secrets .....	188
Chapter 2. Administrative and legal regime of personal data (information about a person) .....	206
Chapter 3. administrative and legal regime of service information .....	227

<b>CONCLUSION</b> .....	<b>263</b>
<b>TEZAURUS</b> .....	<b>271</b>
<b>USED LITERATURE</b> .....	<b>288</b>
<b>USEFUL BIBLIOGRAPHY</b> .....	<b>302</b>
<b>GRATITUDE</b> .....	<b>339</b>

# CONTENTS

<b>BRIEF CONTENTS</b> .....	<b>10</b>
<b>CONTENTS</b> .....	<b>12</b>
<b>PREFACE</b> .....	<b>20</b>
<b>THE LIST OF ABBREVIATIONS</b> .....	<b>23</b>
<b>INTRODUCTION</b> .....	<b>24</b>
<b>PART 1. THE LEVEL OF SCIENCE RESEARCH AND ITS CORE</b>	
<b>METHODOLOGY</b> .....	<b>29</b>
Chapter 1. Bibliography of research .....	31
<i>Researches on information security</i> .....	32
<i>Researches on information law</i> .....	45
<i>Researches, directly devoted to various aspects of information with limited access (specialized scientific papers)</i> .....	58
Chapter 2. Methodological basis of research .....	64
Chapter 3. Key definitions of research .....	76
<i>Classification of information with limited access in doctrinal sources</i> ..	77
<i>Classification of information with limited access in regulatory legal acts</i> .....	84
<b>PART 2. CLASSIFICATION OF INFORMATION WITH LIMITED ACCESS</b> .....	<b>89</b>
Chapter 1. Classification of information with limited access in Ukrainian legislation .....	91
Chapter 2. Classification of information with limited access in doctrinal sources .....	96

**PART 3. THE DEFINITION AND STRUCTURE OF  
ADMINISTRATIVE AND LEGAL REGIME OF  
INFORMATION WITH LIMITED ACCESS IN UKRAINE ..... 107**

Chapter 1. The essence of administrative and legal regime of information with limited access in Ukraine ..... 109

*The concept of “regime”* .....109

*The concept of “legal regime”* .....111

*The stages of teachings about administrative and legal regime forming* .....113

*The concept of “administrative and legal regime”*.....115

*Features of administrative and legal regime* .....117

*The concept of “administrative and legal regime of information with limited access “* .....118

*Features of administrative and legal regime of information with limited access.* .....118

*Classification of administrative and legal regimes* .....119

*Classification of administrative and legal regime of information with limited access* .....122

Chapter 2. Characteristics of the elements of administrative and legal regime of information with limited access in Ukraine ..... 123

*Approaches to the structure of the administrative regime understanding.* .....123

*Purpose of administrative and legal regime of information with limited access.* .....125

*Legal principles of administrative and legal regime of information with limited access* .....127

*The object of administrative and legal regime of information with limited access.* .....130

*The method of administrative and legal regime of information with limited access.* .....132

*“Regime rules” of administrative and legal regime of information with limited access* .....133

*Special public authorities as an element of administrative and legal regime of information with limited access* .....135

*Verkhovna Rada of Ukraine as entity of protection of information with limited access* .....139

*President of Ukraine as entity of protection of information with limited access.* .....144

<i>National Security and Defense Council of Ukraine (NSDC of Ukraine) and the Cabinet of Ministers of Ukraine as entities of protection of information with limited access</i> . . . . .	145
<i>The executive bodies as entities of protection of information with limited access.</i> . . . . .	148
<i>Responsibility for violation of regime norms.</i> . . . . .	160
<i>Spatially-temporal boundaries into force of administrative and legal regime of information with limited access.</i> . . . . .	163
Chapter 3. Improvement of administrative and legal regime of information with limited access in Ukraine . . . . .	164
<i>The stages of systematization of information legislation</i> . . . . .	165
<i>Directions of incorporation.</i> . . . . .	167
<i>Directions of consolidation</i> . . . . .	169
<i>Directions of codification</i> . . . . .	171
<i>Approaches to Information Code forming.</i> . . . . .	174
<i>M. Shwetz's Project</i> . . . . .	175
<i>V.Tsybalyuk's Project.</i> . . . . .	176
<i>Project of the State Committee on Television and Radio Broadcasting</i> . . . . .	179
<i>V.Lipkan's and V.Zaluzniak's Project</i> . . . . .	181

**PART 4. FEATURES OF ADMINISTRATIVE AND LEGAL REGIMES OF CERTAIN TYPES OF INFORMATION WITH LIMITED ACCESS . . . . . 185**

Chapter 1. Administrative and legal regime of state secrets . . . . .	188
<i>Normative and legal regulation of social relations in the state secrets field.</i> . . . . .	188
<i>The concept of "state secrets"</i> . . . . .	191
<i>The system of of state authorities, that are designed to protect state secrets</i> . . . . .	193
<i>Stages of classification information as state secrets</i> . . . . .	194
<i>The list of data, that constitutes state secrets.</i> . . . . .	195
<i>The term within the decision on referring of information to state secret is valid.</i> . . . . .	196
<i>The list of information, that can not be classified as state secrets</i> . . . . .	197
<i>Responsibility for violation of legislation on state secrets.</i> . . . . .	198
<i>The main causes of committing administrative violations of legislation on state secrets</i> . . . . .	200

<i>Prospects for the development of administrative and delictual legislation in the state secrets protection</i> . . . . .	202
Chapter 2. Administrative and legal regime of personal data (information about a person) . . . . .	206
<i>The history of the adoption of the Law of Ukraine “On Personal Data Protection”</i> . . . . .	209
<i>Basic Principles of the Law of Ukraine “On Personal Data Protection”</i> . . . . .	210
<i>The definition of “personal data”</i> . . . . .	216
<i>The information belonging to personal data</i> . . . . .	216
<i>Entities of personal data protection</i> . . . . .	220
<i>The procedure for processing subject’s consent to use his personal data</i> . . . . .	222
<i>Legal liability for violations of legislation in the sphere of personal data protection</i> . . . . .	223
Chapter 3. Administrative and legal regime of service information . . . . .	227
<i>History of the Institute of service information foundation</i> . . . . .	227
<i>The current state of normative and legal regulation of public relations in the service information field</i> . . . . .	231
<i>The list of information, which is service information</i> . . . . .	232
<i>The concept of “service information” in doctrinal sources</i> . . . . .	242
<i>The concept of “service information” in regulatory legal acts</i> . . . . .	245
<i>Features of service information</i> . . . . .	247
<i>Correlation of concepts “service secret” and “state secrets”</i> . . . . .	248
<i>Correlation of concepts “service secret” and “professional secret”</i> . . . . .	250
<i>Protection of documents “For Official Use Only” have marked</i> . . . . .	252
<b>CONCLUSIONS</b> . . . . .	<b>263</b>
<b>TEZAURUS</b> . . . . .	<b>271</b>
<b>USED LITERATURE</b> . . . . .	<b>288</b>
<b>USEFUL BIBLIOGRAPHY</b> . . . . .	<b>302</b>
<i>Lipkans` science school researches</i> . . . . .	302
<i>Information with limited access</i> . . . . .	309
<i>Administrative and legal regimes</i> . . . . .	325

<i>Criminal Law and Criminalistics researches about information sphere</i> .....	326
<i>Lipkans` Reasearhes on Security Studies.</i> .....	328
<i>Information treaties</i> .....	330
<i>Information law and information security</i> .....	331
<b>GRATITUDE</b> .....	<b>339</b>



## ПЕРЕДНЄ СЛОВО

Чому я вирішив започаткувати серію **«ODRDO ORDINANS»**?

Передусім мене спонукало внутрішнє переконання у необхідності подолати той штучний бар'єр, за якого нинішнє покоління і прийдешня генерація втрачають свій іманентний докорінний зв'язок. Сучасні проблеми розвитку науки в Україні набули системного характеру, але до болю прикро, що нині бракує спорідненості між науковими поколіннями.

Здебільшого ті, хто вже здобув науковий ступінь, дуже прискіпливо і почасти суб'єктивно ставляться до здібного молодого покоління, а ще й намагаються нав'язати небезталанній молоді своєрідну панщину — безмежне удосконалення власних теоретичних досліджень.

Такий інтелектуальний сепаратизм почасти перетворюється на наукову «дідівщину», коли певні групи докторів наук унеможливають захист дисертацій, прикриваючись сумнівними гаслами про «необхідність удосконалення і глибокого вивчення предмета дослідження».

Отже, нині в науці справжнісінька монополія на певні теми, напрями досліджень, що не лише негативно впливає на саму науку, а й призводить до сумнівів у світло науки, змушує молодь замислитись про здатність до самостійної роботи. Причому нині в Україні поняття наукової школи чомусь опинилось майже поза законом, особливо це стосується правових наук. Роль держави — це окрема тема, на жаль, в Україні наука ледь животіє на маргінесі.

Ще хотів би привернути увагу до системи підготовки наукових кадрів, яка потребує докорінної зміни. Переконаний, що варто вивчати досвід інших країн, особливо США, де мені пощастило навчатися. Зокрема, в університетах США підготовка наукових кадрів здійснюється за тими напрямками, за якими вже працюють провідні науковці, таким чином наявність наукової школи там — це основний рушій подальшого розвою науки. Саме тому, наприклад, у професора Інституту національної безпеки Університету Делаве-

ру (США) М.Дж.Мілера, який присвятив свій науковий пошук проблемам міграції, немає учнів, які досліджували б проблеми реформування юстиції в США або питання відшкодування шкоди учасникам кримінального судочинства через неправомірні дії органів державної влади.

Більш того, порядок унормування і формування аспірантського корпусу визначається не адміністрацією закладу, а самими професорами, які власноруч одбирають собі аспірантів. Кожен професор відповідає за наукове розроблення певної тематики, кожен рік на це затверджується бюджет, в рамках якого і здійснюється набір найбільш кмітливих і творчих аспірантів. Тому бажання недолугих спудеїв пересидіти в аспірантурі кілька років — там нездійсненне. Тож ніколи не розв'яже проблем жорсткий адміністративний контроль, яким хизуються українські ВНЗ, адже річ не в тім, аби ті, хто поступив — захистили дисертації. Питання у збереженні наукових традицій, розвитку наукових шкіл і наукового руху до нових горизонтів пізнання.

Неправильне розуміння цього призвело до легітимації положення, закріпленого в настановах ВАК, про те, що тема докторської дисертації не може повторювати кандидатської. Утім, пробачте, про яку тоді наступність у науці може йтися, коли чиновники забороняють автору обрати напрям дослідження на все життя, щоб поступово, відповідно до вимог оформлення робіт кандидатського і дисертаційного рівня досліджувати обрану проблему?

Кандидатська дисертація є початком наукового шляху, а докторська має слугувати його органічним продовженням. За таких умов можна буде говорити і про цілісність, і насамкінець про системність дослідження, і про безперервність наукового зростання особистості.

Переконаний, що визначальна роль у підготовці фахового та компетентного науковця має належати науковому керівникові. Від його компетенції, педагогічної майстерності, особистих якостей, вміння мотивувати та сприяти у подоланні фрустрацій на тернистому науковому шляху залежить якість кінцевого продукту — ступінь вартості наукового фахівця. Науковий керівник, наче батько, який, узявши за руку, веде крізь терни до зірок, буремним світом науки, де чимало клипнів, а головне — так важко повірити у власні сили, і так легко зневіритись у можливість наукових перемог. Тому керівник, на мою думку, за даного випадку є своєрідним **ordo ordinans** — упорядковуючим початком. Не вдаючись у філософський зміст даного поняття, яке запропонував І.Г.Фіхте, я хотів би на-

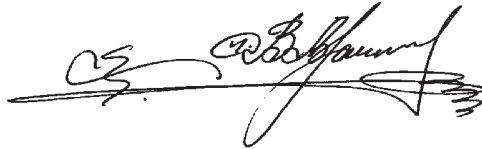
голосити на директивному значенні керівника, на необхідності підвищення його відповідальності за формування наукових шкіл.

Саме тому я і вирішив започаткувати випуск серії книг, в яких знаходили б своє відлуння результати, квінтесенція спільної роботи наукового керівника і його учня. Причому одразу ж зауважу, що як на мене, то уособлює обумовлений порядок єдине упорядковуюче начало для молодого науковця — його керівник. Тому братиму до уваги не тільки ті роботи, де я фактично виступав офіційно закріпленим науковим керівником, а й ті, де безпосередньо був тим упорядковуючим началом для аспіранта і сприяв його становленню як майбутнього науковця.

Разом із керівником і його учнем безпосередню участь в реалізації проголошеної мною концепції бере спеціалізована Вчена Рада, члени якої своїми порадами сприяють подальшому нахненню в удосконаленні роботи.

Відтак, серія **«ORDO ORDINANS»** — це моя наукова позиція і конкретний внесок у **пропаганду системної науки в Україні**, в якій наукове співтовариство, що складається з вчених, молодих дослідників і майбутніх науковців як найбільш фаховий, інтелектуальний та обізнаний шар української історичної нації — являє собою єдиний, цілісний інтелектуальний континуум, епістемологічну спільноту — еліту, яка має формувати дороговкази майбуття та прогресивного розвитку нашої держави.

**З непохитною вірою  
в переможну ходу науки**



**В. А. Ліпкан**

## PREFACE

Why have I decided to start this series «**ORDO ORDINANS**»?

First of all, I have led an inner conviction of the need to overcome that artificial barrier, in which the current generation and future generation lose their inherent connection. Modern development of science in Ukraine becomes systematic, but painfully sad that now lacks affinity between scientific generations.

In most cases, those who earned a scientific degree, treat the talented younger generation very meticulously and partly subjective. They also try to impose on them unlimited improvement of their own theoretical studies.

Such intellectual separatism is partly converted into scientific «bullying» when certain groups of doctors of sciences make it impossible to defend dissertations, hiding behind dubious slogans **such as** «necessity of improvement and deeper studying of the subject of research».

Science in Ukraine is now faced with a real monopoly in certain topics. Those research areas not only affect the science itself, but also lead to the doubt in the light of science, which forces young people to doubt the ability to work independently. Moreover, the concept of scientific school in Ukraine has somehow ended up almost outlawed, especially in the legal sciences. The role of the state is a separate issue, and unfortunately, science in Ukraine hardly exists at such margin.

I would also like to draw attention to the system of training of scientific personnel that needs radical change. I am convinced, it is necessary to study the experience of other countries, especially the U.S., where I was fortunate to study myself. In particular, training of scientific personnel at U.S. universities is carried out in the areas where the leading scientists are already working, thus the presence of scientific school there is a key driver of further development of science. This is why, for example, Professor of National Security University of Delaware (USA) M. J. Miller, who has devoted his scientific research to problems of migration, does not have any students who would

study the problem of reforming the justice system in the United States or recovering of damages to participants of criminal proceedings through illegal actions of state authorities.

Moreover, the procedure of normalization and formation of postgraduate corps is determined not by the administration of the institution, but by the professors who personally select postgraduates themselves. Each professor is responsible for the scientific development of a certain topic, and each year the budget is approved for that, within which the admission of the most clever and creative graduate students is carried out. Therefore, the desire of mediocre students to overstay in graduate school a few years — is impossible. (So the hard administrative control, which boast Ukrainian universities, never resolve the problems because that is not the question that those who entered — defend their dissertations.) So the strict administrative control, which is flaunted by the Ukrainian universities, never resolves the problems, because the point is not whether those who entered defended their dissertations. The point is in preserving scientific traditions, the development of scientific schools and scientific movement to the new horizons of knowledge.

Incorrect comprehension of this has led to legitimization of provision fixed in the guidelines of HAC, that the theme of the doctoral thesis cannot repeat the Ph.D. thesis. However, I'm sorry, about what kind of continuity in science can we talk about when officials prohibit the author to choose the direction of his research for a lifetime, in order to research gradually selected problem, according to the requests to the works of candidate and dissertation-level?

Ph.D. thesis is the beginning of a scientific way, and doctoral thesis should serve the organic extension of the Ph.D. thesis. Under such circumstances it will be possible to talk about integrity, and finally about the systematic research, and about the continuity of scientific and personal growth.

I am convinced that the determining role in the preparation of a professional and competent scientist must belong to a scientific leader. From his/her competence, pedagogical skills, personal qualities, ability to motivate and assist in overcoming frustrations on thorny scientific way, depends the quality of the final product — the value of the degree of scientific expert. Scientific leader, like a father figure, who takes by the hand and leads through the thorns to the stars, through the stormy world of science, where there are many difficulties, and most importantly, so hard to believe in your own strength, and so easy to lose faith in the possibility of scientific victories. Therefore, the

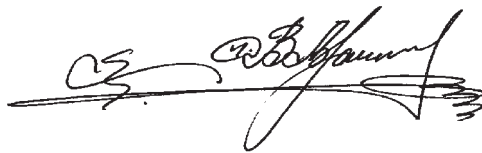
scientific leader, in my opinion, in this case is unique **ordo ordinans** — **the directive order**. Without going into the philosophical meaning of this concept, which is proposed by I. H. Fihte, I would like to emphasize the directive sense of the scientific leader, the need to increase his/her responsibility for the formation of scientific schools.

This is why I decided to start the production of a series of books, in which the result, quintessential of teamwork of scientific leader and his disciple, would find its echo. At once I note that in my opinion, it represents due order, arranging beginning for the young scientist — his leader. Therefore, I will take into account not only those works, where I was actually officially assigned as a scientific leader, but also those where I was directly arranging the beginning for graduate students and contributed to their establishment as a future scientist.

Together with the head and his/**her** student, the Specialized Scientific Council, whose members contribute through their advice to further inspiration in the improvement of the work, directly participate in the implementation of the proclaimed concept.

Therefore, a series of **«ORDO ORDINANS»** — is my scientific position and concrete contribution to the **promotion of systemic science in Ukraine**, in which the scientific community, which consists of scientists, young researchers and future researchers as the most professional, intelligent and knowledgeable layer of Ukrainian historical nation — represents a single, holistic intellectual continuum, epistemological community — an elite, that has to establish ways to the future and progressive development of our country.

*With steadfast faith in  
the victorious course  
of science*



V.A. Lipkan

## ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

- ВРУ** — Верховна Рада України;
- ДСЗПД України** — Державна служба України з питань захисту персональних даних;
- ЄС** — Європейський Союз;
- КУпАП** — Кодекс України про адміністративні правопорушення;
- ККУ** — Кримінальний кодекс України;
- НПА** — нормативно-правовий акт;
- ОВВ** — органи виконавчої влади;
- РСО** — режимно-секретні органи;
- СБУ** — Служба безпеки України;
- ТЗІ** — технічний захист інформації;
- ЦКУ** — Цивільний кодекс України.

## ВСТУП

У ХХІ сторіччі інформація виступає головним чинником соціалізації людини, об'єднуювальною ланкою між людиною, суспільством і державою. Своєчасне та правдиве інформування громадян з боку держави та надання необхідної для функціонування держави інформації з боку громадян, отримання учасниками суспільних відносин достовірної й повної інформації про перебіг подій у країні, в навколишньому середовищі, використання інформації задля задоволення власних потреб є основою та запорукою побудови і формування демократичної, правової держави.

Утім, кожна держава володіє такою інформацією, розголошення чи оприлюднення якої може завдати шкоди національним інтересам. Отже, виникає дилема пошуку балансу між реалізацією прав і свобод людини й громадянина в інформаційній сфері та забезпеченням інформаційної безпеки. Результатом розв'язання такої проблеми стала поява інституту інформації з обмеженим доступом.

Якщо державні органи унеможливають доступ громадськості до публічної інформації, то це призводить до порушень права громадян на інформацію. Стосовно інформації з обмеженим доступом, то обов'язок державних органів полягає у забезпеченні захисту такої інформації легальними шляхами.

Лібералізація та гуманізація вітчизняного законодавства обумовили необхідність перегляду сутності та значення правового режиму інформації з обмеженим доступом, зокрема критеріїв формування переліку відомостей, що її становлять, порядку та умов надання таким відомостям статусу інформації з обмеженим доступом, адекватності заходів захисту й охорони тощо.

Тривалий час захист інформації з обмеженим доступом забезпечувався винятково кримінально-правовими нормами. Нині до Кодексу України про адміністративні правопорушення внесені відповідні змі-



ни та доповнення, згідно з якими окремі види інформації з обмеженим доступом стали охоронятись адміністративно-правовими нормами.

Дана тенденція обумовлена тим, що останнім часом спостерігається збільшення кількості зловживань із боку органів державної влади щодо віднесення тих чи інших відомостей до інформації з обмеженим доступом. Це призводить до порушення права громадян на доступ до публічної інформації або навпаки — до збільшення кількості правопорушень особами, які мають доступ до інформації з обмеженим доступом, внаслідок чого відбувається її незаконний витік і оприлюднення. Таким чином, відсутність законодавчого визначення поняття інформації з обмеженим доступом, її видів, наявність значної кількості суперечностей між окремими нормативно-правовими актами щодо процедури, строків та переліку відомостей, які не можна відносити до інформації з обмеженим доступом та тих, які дозволено, недосконалість деліктного законодавства та нечітке визначення відповідальних державних інституцій у цій сфері негативно впливають на рівень захисту й охорони інформації з обмеженим доступом, зокрема на адміністративно-правовий режим такої інформації. У зв'язку з чим дослідження адміністративно-правового режиму інформації з обмеженим доступом наразі доволі актуальні для сучасної юридичної науки, що й обумовило вибір означеної тематики для монографії.

При написанні роботи автори широко використовували праці вітчизняних і зарубіжних вчених у галузях інформаційного права, адміністративного права, теорії держави та права, конституційного права, цивільного права, зокрема: В. Б. Авер'янова, І. В. Арістової, В. Ю. Баскакова, М. І. Дімчогло, П. Б. Євграфової, В. А. Залізняка, Р. А. Калюжного, В. В. Копейчикова, О. О. Кулініча, Б. М. Лазарева, О. В. Логінова, Ю. Є. Максименко, А. І. Марущака, П. Є. Матвієнко, В. Я. Мацюка, Н. М. Онищенко, В. Ф. Опришка, О. П. Полінця, В. П. Портнова, П. М. Рабіновича, В. І. Ремньова, А. О. Селіванова, З. К. Симорота, А. І. Сироти, С. Г. Стеценка, Р. Й. Халфіної, В. В. Цветкова, В. С. Цимбалюка, К. П. Череповського, В. Є. Чиркіна, М. Я. Швеця, О. В. Шепети та інших.

Утім, незважаючи на наявність численних наукових розвідок, присвячених дослідженню різних аспектів правового регулювання інформації з обмеженим доступом, поза науковим обігом залишилося комплексне, системне дослідження адміністративно-правового режиму інформації з обмеженим доступом.

Саме тому й виникла **актуальна наукова проблема** — відсутність адекватного розуміння та наукового опрацювання питань правового режиму інформації з обмеженим доступом.

**Мета роботи:** на основі досягнень юридичної науки, узагальнення правозастосовної діяльності, аналізу вітчизняного й зарубіжного законодавства розробити та надати науково обґрунтовані пропозиції щодо удосконалення вітчизняного законодавства у сфері інформації з обмеженим доступом задля підвищення його ефективності.

Для досягнення мети необхідно вирішити наступні **завдання:**

- окреслити історіографію дослідження інформації з обмеженим доступом у вітчизняній адміністративній та інформаційно-правовій доктрині;
- надати авторське визначення поняття «інформація з обмеженим доступом» та виділити її конститутивні ознаки в адміністративно-правовому контексті;
- визначити поняття «адміністративно-правовий режим інформації з обмеженим доступом» та виокремити основні його ознаки;
- здійснити класифікацію інформації з обмеженим доступом;
- надати характеристику елементам адміністративно-правового режиму інформації з обмеженим доступом;
- визначити недоліки та надати пропозиції щодо удосконалення адміністративно-правового режиму державної таємниці;
- розкрити стан та перспективи розвитку адміністративно-правового режиму персональних даних;
- охарактеризувати адміністративно-правовий режим службової інформації.

*Об'єкт дослідження* — суспільні відносини, що виникають у зв'язку із захистом і охороною інформації з обмеженим доступом.

*Предмет дослідження* — адміністративно-правовий режим інформації з обмеженим доступом в Україні.

Методологічна основа дослідження складається із сукупності загальних, галузевих та спеціальних наукових методів, які, застосовуючись комплексно, дають змогу виконати поставлені завдання та досягнути мети дослідження. Базовою методологічною основою став загальнонауковий *системний підхід*, який обґрунтовує взаємозв'язок і взаємообумовленість соціальних процесів і суспільних явищ як еле-

ментів системи та за допомогою якого інформація з обмеженим доступом розглядається як системне утворення.

За допомогою *діалектичного та історичного методів* досліджено генезис наукових розвідок, присвячених окремим аспектам порушеної проблематики, стан та розвиток адміністративно-правового режиму окремих видів інформації з обмеженим доступом, особливості адміністративно-правового режиму інформації з обмеженим доступом. *Формально-логічний та соціологічний методи* допомогли визначити роль та місце адміністративно-правового режиму інформації з обмеженим доступом у правовій системі України, його значущість для суспільства та особливості, а також стали в пригоді при дослідженні понятійно-категорійного апарату. *Статистичний та порівняльно-правовий методи* використовувалися для окреслення правового регулювання суспільних відносин у сфері інформації з обмеженим доступом та шляхів удосконалення вітчизняного інформаційного законодавства в контексті порушеної проблематики. За допомогою *логіко-семантичного методу та методу сходження* від абстрактного до конкретного поглиблено понятійний апарат, визначено поняття, загальні та особливі риси інформації з обмеженим доступом. *Метод порівняльно-правового аналізу* було покладено в основу аналізу та зіставлення національного і зарубіжного законодавства у сфері інформації з обмеженим доступом. За допомогою *формально-юридичного методу* досліджувалися норми вітчизняних і зарубіжних нормативно-правових актів, що регулюють інформаційні відносини у сфері інформації з обмеженим доступом, з'ясовувалися зміст і значення використаних у них термінів, обґрунтовувалися висновки й пропозиції щодо їх зміни та доповнення. *Структурно-функціональний метод* сприяв аналізу елементів адміністративно-правового режиму інформації з обмеженим доступом, накресленню напрямів його удосконалення. За допомогою *герменевтичного методу* встановлювалася текстуальна сутність нормативних приписів вітчизняних і зарубіжних законодавчих актів, що регулюють інформаційні відносини у сфері інформації з обмеженим доступом. Завдяки *аксіоматичному методу* були визначені вихідні параметри дослідження; *індуктивний та дедуктивний методи* застосовувалися при узагальненні та аналізі емпіричної інформації. Історичні аспекти становлення адміністративно-правового режиму інформації з обмеженим доступом в Україні та за кордоном досліджувалися за допомогою *порівняльно-ре-*

*троспективного, історико-генетичного методів, а також методів екстраполяції і факторного аналізу. Прогностичний аналіз, що передбачав виявлення тенденцій розвитку інформаційного законодавства у сфері інформації з обмеженим доступом, здійснювався на підставі використання методів прогнозування, а саме: методу експертних оцінок, екстраполяції, методу аналогії. Інформаційна та теоретична бази дослідження складаються з національного та зарубіжного законодавства, підзаконних нормативно-правових актів, міжнародних документів, що стосуються предмета дослідження.*

# **РІВЕНЬ НАУКОВОГО РОЗРОБЛЕННЯ ПРОБЛЕМИ ТА МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ**

---

---

- 1.1 БІБЛІОГРАФІЯ ЗА ТЕМОЮ ДОСЛІДЖЕННЯ
- 1.2 МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ  
АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЇ  
З ОБМЕЖЕНИМ ДОСТУПОМ
- 1.3 ПОНЯТІЙНО-КАТЕГОРІЙНИЙ АПАРАТ ДОСЛІДЖЕННЯ





## 1.1 БІБЛІОГРАФІЯ ЗА ТЕМОЮ ДОСЛІДЖЕННЯ

Сучасне розуміння забезпечення інформації з обмеженим доступом обумовлене складним та тривалим періодом його формування, становлення і розвитку. Вільне отримання, володіння, користування інформацією завжди визнавалось ознакою демократичності країни, оскільки за допомогою інформації кожна людина в змозі контролювати і наскільки діяльність компетентних органів ефективна, чи припустимі їх повноваження, межі втручання в особисте життя людини.

Для кожної історичної доби та конкретної країни правовий режим інформації з обмеженим доступом, види таємниць, процедури надання статусу інформації з обмеженим доступом, строки, протягом яких інформація є інформацією з обмеженим доступом, відповідальність тощо мали різний зміст.

Інститут інформації з обмеженим доступом у вітчизняній адміністративній доктрині доволі новий та нерозроблений. Оскільки ця монографія є однією з перших наукових робіт, що досліджує правовий режим інформації з обмеженим доступом під адміністративно-правовим кутом, то значного масиву джерел з цієї тематики, на жаль, сучасною наукою адміністративного права не напрацьовано.

**Алгоритм дослідження бібліографії** за темою дослідження побудовано з урахуванням критеріїв історичності по кожній групі, а саме:

- 1) роботи з інформаційної безпеки;
- 2) роботи з інформаційного права;
- 3) роботи, присвячені безпосередньо різним аспектам інформації з обережним доступом (спеціалізовані роботи).

## *Роботи з інформаційної безпеки*

Здебільшого окремі аспекти цієї проблематики порушувались у контексті розгляду питань забезпечення інформаційної безпеки. Це, насамперед, пов'язано з тим фактом, що захист інформації з обмеженим доступом визначається як найдавніший і найважливіший напрям інформаційної безпеки держави.

Слід зауважити, що інформаційна безпека в силу своєї багатогранності розглядається у загальнотеоретичному, історичному, управлінському, філософському, економічному, політологічному, геополітичному, юридичному та інших ракурсах. Кожна з наук, що її досліджує, окреслює різні аспекти цього феномена, що відповідає специфіці науки та використаному інструментарію.

У одних із перших наукових розвідках, присвячених інформаційній безпеці, відсутній розгляд захисту інформації з обмеженим доступом, оскільки інформаційна безпека зводиться до протидії комп'ютерній злочинності, інформаційному тероризму та спеціальним психологічним операціям. Зокрема, в такому ракурсі на рівні дисертаційного дослідження інформаційна безпека як складова національної безпеки в Україні вперше розглядалась О. В. Литвиненком у політологічній роботі «Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії)» [1, с. 14].

Таке саме розуміння інформаційної безпеки надається науково-педагогічним колективом Національної академії Служби безпеки України в підручнику «Інформаційна безпека (соціально-правові аспекти)», де розкриваються сутність, технології та засоби маніпулювання свідомістю, проведення інформаційних війн і спеціальних інформаційних операцій, історія і сучасний стан інформаційно-психологічного протиборства, особливості інформаційного впливу в терористичній діяльності та економічному протиборстві [2].

Лише згодом дослідники інформаційної безпеки почали розмежовувати безпеку інформації як складову інформаційної безпеки та інформаційну безпеку як більш широку категорію, що охоплює інші складові.

Так, у дисертаційній роботі загальнотеоретичного спрямування «Теоретико-правові засади забезпечення інформаційної безпеки України» Ю. Є. Максименко складові інформаційної безпеки були виокрем-



лені шляхом аналізу загроз національній безпеці в інформаційній сфері відповідно до Закону України «Про основи національної безпеки». На думку дослідниці, інформаційна безпека становить систему, що складається з таких структурних елементів як інформаційна безпека у сфері прав і свобод людини та громадянина, інформаційно-технічна й інформаційно-психологічна безпека [3, с. 55–56].

Авторка зауважує, що захист інформації з обмеженим доступом являє собою зміст інформаційної безпеки у сфері прав і свобод людини та громадянина, оскільки в основі цього структурного елемента інформаційної безпеки лежать на сучасному етапі такі головні реальні та потенційні загрози національній безпеці України, стабільності в суспільстві, в інформаційній сфері (згідно із Законом України «Про основи національної безпеки України»), як прояви обмеження свободи слова та доступу громадян до інформації, а також розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства та держави.

Такий погляд на інформаційну безпеку як систему, що охоплює три структурні елементи (інформаційну безпеку у сфері прав і свобод людини та громадянина, інформаційно-технічну й інформаційно-психологічну), та критерій їх виділення вважаємо не зовсім коректним, оскільки законодавець зазначив лише головні реальні та потенційні загрози національній безпеці України, стабільності в суспільстві в інформаційній сфері у Законі України «Про основи національної безпеки України». Саме тому захист інформації з обмеженим доступом може бути складовою не лише інформаційної безпеки у сфері прав і свобод людини та громадянина, а й інформаційно-технічної безпеки, оскільки розголошення такої інформації завдає шкоди як особистим інтересам, так і державним.

В іншому дисертаційному дослідженні загальнотеоретичного спрямування «Забезпечення інформаційної безпеки як функція держави» О. О. Тихомирова<sup>1</sup>, а також у деяких інших роботах цього автора теж не знайшло відображення питання дослідження інформації з обмеженим доступом. Як слушно зауважує О. О. Тихомиров: «...досвід України та інших країн свідчить, що загрози, які існують в інформаційному

<sup>1</sup> Тихомиров О. О. Забезпечення інформаційної безпеки як функція держави : дис. ... канд. юрид. наук : 12.00.01 / Олександр Олександрович Тихомиров. — К., 2011. — 210 с.

просторі, мають здебільшого глобальну природу, високу динаміку і латентність, спонтанність виникнення і розвитку, внаслідок чого суттєво ускладнюють і певною мірою обмежують державний і правовий вплив на їх попередження, подолання, усунення чи мінімізацію суспільно небезпечних наслідків»<sup>2</sup>.

Також привертають увагу доволі ґрунтовні дослідження цього автора таких питань, як система забезпечення інформаційної безпеки, функції державного забезпечення інформаційної безпеки: структурні та класифікаційні аспекти, зміст державної діяльності по забезпеченню інформаційної безпеки, особливості правового регулювання забезпечення інформаційної безпеки, міжнародні, європейські та національні правові стандарти забезпечення інформаційної безпеки, нормативно-правове регулювання інформаційної безпеки в Україні тощо.

Слід зауважити, що актуальність теоретико-правових досліджень в умовах становлення інформаційного суспільства не викликає заперечень. Хоча їх інтенсивність, порівняно з іншими напрямками правових досліджень, незначна. Серед них доцільно виокремити роботи В. В. Балдіцина «Охоронні відносини у сфері забезпечення інформаційної безпеки Росії (Теоретико-правовий аспект)», В. М. Боєра «Інформаційно-правова політика і безпека Росії: теоретико-правовий аспект», В. М. Лопатіна «Інформаційна безпека Росії», О. В. Надигіної «Теоретико-правовий аналіз впливу інформаційних технологій на правосвідомість», Т. А. Полякової «Теоретико-правовий аналіз законодавства в області забезпечення інформаційної безпеки Російської Федерації», Н. В. Римарьової «Концептуальні питання формування системи правового регулювання інформаційної безпеки Російської Федерації», А. О. Стрельцова «Теоретичні та методологічні основи правового забезпечення інформаційної безпеки Росії», а також О. А. Тамодліна «Державно-правовий механізм забезпечення інформаційної безпеки особистості»<sup>3</sup>.

<sup>2</sup> Тихомиров О. О. Забезпечення інформаційної безпеки як функція держави : дис. ... канд. юрид. наук : 12.00.01 / Олександр Олександрович Тихомиров. — К., 2011. — 210 с.

<sup>3</sup> Балдицын В. В. Охранительные правоотношения в сфере обеспечения информационной безопасности современной России (теоретико-правовой аспект) : дисс. ... канд. юрид. наук : 12.00.01 / Балдицын Василий Вячеславович. — СПб., 2000. — 178 с.

Боер В. М. Информационно-правовая политика и безопасность России : теоретико-правовой аспект : автореф. дисс. на соискание ученой степени доктора юрид. наук. : спец. 12.00.01 «Теория и история государства и права ; история правовых учений» / В. М. Боер ; Санкт-Петербург.

У роботі В. Я. Василюка та С. О. Климчука «Інформаційна безпека держави» не знайшло системного дослідження основи захисту інформації з обмеженим доступом чи розкриття змісту такої інформації. Автори зосереджують увагу на розгляді правових засад лише державної, комерційної таємниць та захисту персональних даних у деяких країнах світу. Погоджуємось з думкою дослідників, що «...історія і практика діяльності людства свідчить про те, що втрата цієї категорії інформації наносить інтересам держави, суспільства і особистості найбільш значну шкоду» [4, с. 54].

У навчальному посібнику українських авторів О. К. Юдіна та В. М. Богуна «Інформаційна безпека держави» наведено систематизовану сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення, визначено місце інформаційної безпеки в загальній системі національної безпеки, вплив дестабілізуючих факторів та інформаційних загроз на безпеку особистості, суспільства і держави, основи протиборства та інформаційної боротьби, зміст і форми психологічних операцій та інформаційно-психологічної безпеки, а також загальні підходи до забезпечення безпеки інформаційних технологій [5]. Проблема захисту інформації з обмеженим доступом не стала окремим напрямом дослідження в цій роботі. Разом із тим праця містить словник додаткових термінів і понять, які не мають нормативного закріплення у вітчизняному законодавстві, однак допомагають розкри-

---

академия МВД России. — СПб., 1998. — 15 с.; Лопатин В. Н. Информационная безопасность России : дисс. ... доктора юрид. наук : 12.00.01 / Владимир Николаевич Лопатин. — СПб., 2000. — 433 с.; Надыгина Е. В. Теоретико-правовой анализ влияния информационных технологий на правосознание : дисс. ... канд. юрид. наук : 12.00.01 / Елена Владимировна Надыгина. — Нижний Новгород, 2007. — 211 с.; Полякова Т. А. Теоретико-правовой анализ законодательства в области обеспечения информационной безопасности Российской Федерации : автореф. дисс. на соискание ученой степени канд. юрид. наук. : спец. 12.00.01 «Теория и история государства и права; история правовых учений»/ Т. А. Полякова; Министерство юстиции Российской Федерации. Российская правовая академия. — М., 2002. — 24 с.; Рымарева Н. В. Концептуальные вопросы формирования системы правового регулирования информационной безопасности в Российской Федерации : дисс. ... канд. юрид. наук : 05.13.19 / Наталья Валерьевна Рымарева. — Воронеж, 2005. — 182 с.; Стрельцов А. А. Теоретические и методологические основы правового обеспечения информационной безопасности России : дисс. ... доктора юрид. наук : 05.13.19 / Анатолий Александрович Стрельцов. — М., 2004. — 371 с.; Тамодлин А. А. Государственно-правовой механизм обеспечения информационной безопасности личности : дисс. ... канд. юрид. наук : 12.00.01 / Александр Анатольевич Тамодлин. — Саратов, 2006. — 175 с.

ти сутність інформації з обмеженим доступом. Зокрема визначено такі поняття, як «відомості в галузі економіки, науки і техніки, які можуть становити державну таємницю», «відомості в галузі зовнішньої політики і економіки, які можуть становити державну таємницю», «відомості в галузі розвідувальної, контррозвідувальної і оперативно-розшукової діяльності, які можуть становити державну таємницю», «відомості у воєнній галузі, які можуть становити державну таємницю», «відомості, що становлять державну таємницю», «відомості, які не підлягають засекречуванню», «допуск до державної таємниці», «доступ до інформації», «орган захисту державної таємниці», «орган технічного захисту інформації», «таємниця», «державна таємниця» тощо. Щодо інших видів таємниць та інформації з обмеженим доступом загалом, то відсутні будь-які відомості.

Компаративний аналіз особливостей забезпечення інформаційної безпеки в країнах-членах Європейського Союзу, стандарти ЄС у цій сфері та відповідність вітчизняного інформаційного законодавства вищезазначеним стандартам розглянуто в роботі В. А. Ліпкана, Ю. Є. Максименко, В. М. Желіховського «Інформаційна безпека України в умовах євроінтеграції» [6]. Аналіз вищезазначеними науковцями Хартії основних прав Європейського Союзу від 7 грудня 2000 року надали можливість виокремити ряд прав і свобод людини в інформаційній сфері, що безпосередньо стосуються проблеми захисту інформації з обмеженим доступом. Зокрема даний НПА закріплює таємницю кореспонденції (ст. 7), право людини на доступ до матеріалів, що мають до неї безпосереднє відношення, при забезпеченні законних інтересів конфіденційності, а також професійної і комерційної таємниці (ст. 41), право доступу до документів Європейського парламенту, Ради та Європейської комісії (ст. 42) тощо. Таким чином, термінологія у сфері інформації з обмеженим доступом та види такої інформації мають різне смислове навантаження у вітчизняному та міжнародному законодавстві.

Розгляд проблем забезпечення інформаційної безпеки в країнах ЄС та іншої впливової безпекової міжнародної організації — НАТО визначено у навчальному посібнику В. С. Сідака і В. Ю. Артемова, призначеному для навчальних курсів за спеціальностями «Національна безпека», «Інформаційна безпека», «Організація захисту інформації з обмеженим доступом» тощо. У цій роботі дослідники розкрили такі

важливі питання, як сутність і зміст організаційно-правових основ захисту інформації з обмеженим доступом у країнах НАТО та ЄС, місце і роль правових основ захисту інформації з обмеженим доступом у країнах НАТО та ЄС, основні шляхи приведення внутрішньодержавного законодавства у відповідність до вимог ЄС та НАТО щодо організаційно-правових норм захисту інформації.

Як слушно зауважують автори: «...використання позитивного досвіду країн-членів ЄС та НАТО при вдосконаленні нормативно-правової бази діяльності державних органів України у цій сфері здатне певною мірою забезпечити гармонійне входження України до правового поля європейського співтовариства» [7, с. 5]. Доречна думка дослідників і щодо необхідності за аналогією з НАТО створити в Україні Національний орган безпеки, який формував би перелік відомостей, віднесених до державної таємниці, за необхідності проводив міжвідомчу експертизу правомірності віднесення відомостей до державної таємниці, погоджував розподіл між міністерствами, відомствами та іншими органами державної влади повноважень та від імені держави готував перелік відомостей, віднесених до державної таємниці, для затвердження президентом й оприлюднення [7, с. 126].

Корисними для розкриття предмета нашого дослідження можна назвати роботи таких українських дослідників-адміністративістів, як І. В. Арістова, В. І. Гурковський, Б. А. Кормич, В. А. Ліпкан, О. В. Логінов, Л. С. Харченко [8–13].

Так, Б. А. Кормич у своєму навчальному посібнику «Інформаційна безпека: організаційно-правові основи» виокремлює розділ під назвою «Організаційно-правові основи захисту та обмеження обігу інформації в цілях інформаційної безпеки», де окреслюються такі питання: правове регулювання обігу інформації в суспільстві, режими доступу до інформації, державна таємниця, таємниця приватного життя, обмеження доступу до інформації в інтересах слідства та судочинства, службова, комерційна, професійна таємниці, а також обмеження щодо виробництва та ввезення в Україну інформаційної продукції.

Привертає увагу думка дослідника, що застосування обмежень щодо доступу обумовлюється великою суспільною цінністю інформації і можливими суспільно небезпечними наслідками несанкціонованих дій з такою інформацією, а також необхідності класифікації інформації на відкриту та обмеженого доступу на основі методів правово-

го регулювання, що застосовуються до регулювання суспільного обігу того чи іншого виду інформації. Як зауважує Б. А. Кормич: «...два правові методи регулювання створюють три можливі види правового обігу інформації: відкритий, що регулюється виключно цивільно-правовими нормами, закритий, що регулюється адміністративно-правовими нормами, і нарешті обмежений, до якого застосовуються обидва види правового регулювання. До них також долучається вільний обіг інформації, який правом не врегульований взагалі» [9, с. 276].

У своїй монографії «Організаційно-правові засади політики інформаційної безпеки України» Б. А. Кормич також звертає увагу на розгляд організаційно-правових основ захисту та обмеження обігу інформації в цілях інформаційної безпеки. У главі IV «Правові гарантії інформаційної безпеки держави» автор розкриває співвідношення інформаційної безпеки та захисту інформації з обмеженим доступом: «... об'єктом захисту в цілях інформаційної безпеки є лише та інформація, яка згідно з законом знаходиться в закритому або обмеженому обігу, тобто інформація, до якої знову ж таки законом встановлені обмеження імперативного характеру» [10, с. 337].

Один із підрозділів дисертаційного дослідження Б. А. Кормича також розкриває особливості захисту інформації з обмеженим доступом. Дослідник знову ж таки виділяє на основі двох правових методів регулювання відкритий, закритий та обмежений види правового обігу інформації та зауважує, що «інформація змінюючи свою суспільну цінність, може переходити з одного виду обігу до іншого (зняття грифів «таємно», або «для службового користування», закінчення строку дії авторських прав тощо)» [12, с. 263].

Окремі аспекти забезпечення інформаційної безпеки в Україні були досліджені автором в інших його роботах<sup>4</sup>.

<sup>4</sup> Кормич Б. А. Національна безпека як правова категорія аналізу митної діяльності держави / Б. А. Кормич // Актуальні проблеми політики : зб. наук. праць. — Одеса, 2001. — Вип. 10. — С. 56–61.; Кормич Б. А. Засади правового захисту національної безпеки в сфері зовнішньоекономічних відносин / Б. А. Кормич // Актуальні проблеми політики : зб. наук. праць. — Одеса, 2001. — Вип. 11. — С. 732–738.; Кормич Б. А. Співвідношення національної безпеки та національних інтересів / Б. А. Кормич // Вісник університету внутрішніх справ. — Х., 2001. — Вип. 13. — С. 71–76.; Кормич Б. А. Національна безпека як категорія аналізу законодавчого забезпечення державної політики / Б. А. Кормич // Парламентаризм в Україні: теорія і практика : матеріали міжнар. наук.-практ. конф., присвяченої 10-й річниці з дня проголошення незалежності України та 5-й річниці з дня прийняття Конституції України, (26 черв. 2001 р.). —



Організаційно-правові засади забезпечення інформаційної безпеки також розглянуто в дисертаційному дослідженні В. І. Гурковського «Організаційно-правові питання взаємодії органів державної влади у сфері інформаційної безпеки», де автор, крім того, що окреслив важливі проблеми організаційного та правового характеру в процесі забезпечення взаємодії органів державної влади щодо формування, охорони і захисту суспільних інформаційних відносин, запропонував шляхи вдосконалення механізму державного управління у сфері національної інформаційної безпеки, висловив, на нашу думку, дискусійні міркування, що «серед позитивних тенденцій розвитку правового регулювання суспільних інформаційних відносин можна виділити те, що в останні роки суттєво вдосконалено, а за деякими напрямками заново створено, відповідну нормативно-правову базу системи захисту інформації в державі» та «найважливішим здобутком сучасної правотворчості системи національної інформаційної безпеки є створення юридичного підґрунтя для захисту інформації в мережах передачі даних» [12, с. 156].

Дискусійність вищезазначених думок полягає в тому, що, незважаючи на динамічне та інтенсивне зростання кількості різноманітних нормативно-правових актів, що урегульовують суспільні відносини у сфері захисту інформації, їх якість потребує значного удосконалення. А тому не завжди кількість законодавчих актів корелюється з ефективністю правового регулювання відповідних суспільних відносин.

Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України стало предметом дослідження Д. О. Красікова, який зауважив, що, незважаючи на прийняті нормативно-правові акти, а також ратифіковані міжнародні стандарти забезпечення інформаційної безпеки, статистичні дані засвідчують, що кількість інформаційних правопорушень постійно зростає.

Вважаємо, що динаміка вчинення правопорушень вказує не так на неефективність правового регулювання інформаційних відносин, як на інтенсивне впровадження інформаційно-телекомунікаційних технологій в усі сфери життєдіяльності суспільства, та, як наслідок, динаміку інформаційних правопорушень.

К., 2001. — С. 228–232.; Кормич Б. А. Авторське право та інтелектуальна власність / Б. А. Кормич // Соціальне партнерство — механізм реалізації прав людини, розбудови правової держави, громадянського суспільства. — К., 2001. — Т. 24. — С. 272–275.

Підтримуємо пропозицію автора щодо необхідності створення в системі МВС України єдиного підрозділу (шляхом інтеграції відповідних функцій Департаменту інформаційно-аналітичного забезпечення, Режимно-секретного управління та Відділу спеціального зв'язку), який забезпечував би інформаційну безпеку в ОВС<sup>5</sup>.

У подібному ракурсі питання інформаційної безпеки розглядалось у дисертації О. В. Логінова «Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади», а також в інших роботах цього автора<sup>6</sup>. Дослідник обґрунтував положення щодо необхідності виділити Державний департамент з питань зв'язку та інформатизації зі складу Міністерства транспорту та зв'язку, створивши на його базі Міністерство інформації України.

Не менш цінними є пропозиції О. В. Логінова щодо необхідності створення підсистеми органів виконавчої влади управління національною інформаційною сферою та ліквідації різновиду центральних органів виконавчої влади — центральні органи виконавчої влади зі спеціальним статусом (для підтвердження приналежності до виконавчої гілки влади пропонується змінити їх назву на «спеціальні органи виконавчої влади»), прийняття доктрини інформаційної безпеки України, яка повинна стати основним системоутворювальним фактором у процесах становлення системи інформаційної безпеки органів виконавчої влади тощо.

Окремі аспекти захисту інформації з обмеженим доступом стали предметом розгляду І. В. Арістової. Так, у своїй дисертації дослідни-

<sup>5</sup> Красіков Д. О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / Д. О. Красіков. — К., 2012. — 20 с.

<sup>6</sup> Логінов О. В. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління / О. В. Логінов // Науковий вісник Юридичної академії МВС України. — Дніпропетровськ, 2003. — № 3. — С. 199–205.; Логінов О. В. Гносеологічний аспект управління інформаційною безпекою України / О. В. Логінов // Науковий вісник Юридичної академії МВС України. — Дніпропетровськ, 2004. — № 2. — С. 153–161.; Логінов О. В. Деякі аспекти інформаційного забезпечення діяльності Уряду України / О. В. Логінов // Сучасні проблеми управління : зб. матеріалів II Міжнар. наук.-практ. конференції / [уклад.: Б. В. Новиков, І. І. Федорова та ін.]. — К., 2003. — Ч. 1. — С. 127–130.; Логінов О. В. Інформаційна безпека: потребнісний та гносеологічний підходи / О. В. Логінов // Забезпечення прав людини та громадянина в умовах реформування політичної та правової системи України : тези доп. наук.-практ. конференції. — К., 2004. — С. 253–256.



ця зауважує: «Ключовою проблемою є створення відкритого інформаційного простору (національної інформаційної сфери), що сприяє забезпеченню інформаційної прозорості державної влади, необхідної для формування громадянського суспільства, інформаційної держави і досягнення ефективної взаємодії між суспільством та владою на принципах довіри, порозуміння і ділового партнерства» шляхом «механізму практичної реалізації конституційного права громадян на свободу одержання інформації», в основі якого «повинні стати законодавчо закріплені чіткі правила, умови та порядок одержання громадянами та інституціональними структурами суспільства інформації в органах державної влади і місцевого самоврядування, від інших державних і недержавних юридичних осіб, а також прямиий доступ до державних і недержавних інформаційних ресурсів» [13, с. 181].

Ми підтримуємо думку автора, що «...при цьому тільки в рамках законодавства доступ до деяких видів інформації повинен бути обмеженим з метою захисту особистих прав і свобод громадян, інтересів економічних та інших структур суспільства, держави і національної безпеки. Особливо збалансований підхід потрібний під час роботи з персональними даними і шифруванням інформації, тому що саме в цих сферах найбільш можливе виникнення загроз недоторканності особистого життя й обмеження прав на особисту, сімейну і комерційну таємницю як при надмірному втручанні держави, так і у разі несанкціонованої діяльності недержавних структур» [13, с. 182].

Проте проблема захисту інформації з обмеженим доступом не стала безпосереднім предметом розгляду вищевказаної дослідниці, а визначається нею як потенційний перспективний напрям наукової діяльності.

Серед більш сучасних робіт з інформаційної безпеки слід зазначити дисертаційні дослідження таких авторів, як І. Р. Березовська «Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні», О. В. Стоєцький «Адміністративна відповідальність за правопорушення у сфері інформаційної безпеки України» тощо.

Так, І. Р. Березовська у своєму дослідженні<sup>7</sup> визначила історичні віхи становлення і розвитку адміністративно-правових засобів забез-

<sup>7</sup> Березовська І. Р. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / І. Р. Березовська. — К., 2012. — 18 с.

печення інформаційної безпеки України, виокремила їх ознаки, особливості, а також надала їх класифікацію. Конструктивною є пропозиція дослідниці щодо доцільності включити в Указ Президента України «Про Доктрину інформаційної безпеки України» спеціальний розділ «Стан інформаційної безпеки», в якому слід чітко визначити актуальні проблеми державної політики забезпечення інформаційної безпеки та зосередити увагу на необхідності їх розв'язання. Доволі актуальний і розроблений нею проект Положення про єдину систему міжвідомчої електронної взаємодії. Інші аспекти цієї проблематики конкретизовано в наукових статтях та тезах<sup>8</sup>.

Якщо І. Р. Березовська лише поверхово окреслила особливості адміністративної відповідальності у сфері забезпечення інформаційної безпеки, то О. В. Стоєцький у своїх роботах детально розглянув особливості адміністративної відповідальності за правопорушення у сфері інформаційної безпеки України<sup>9</sup>.

Аналіз праць О. В. Стоєцького надав можливість виокремити такі основні конструктивні ідеї, що підтримуються нами: внесення змін до КУпАП шляхом виокремлення глави, яка охоплювала б адміністративні правопорушення у сфері інформаційної безпеки, поділивши їх залежно від того, яке право порушується, а саме адміністративні правопорушення, що посягають на суспільні відносини у сфері збирання інформації; зберігання інформації; використання інформації; поширення інформації; доповнення КУпАП статтею такого змісту: «*Кіберхуліганство*, тобто вчинення в соціальних мережах діяння, направлено-го на нанесення шкоди честі, гідності, здоров'ю людини шляхом використання інформаційно-комунікаційних технологій, — тягне за собою

<sup>8</sup> Березовська І. Р. Адміністративно-правове регулювання інформаційної взаємодії органів виконавчої влади з громадянами: постановка проблеми / І. Р. Березовська // Наукові записки ЛУБП. — 2010. — Вип. № 5. — С. 206–208.; Березовська І. Р. Поняття та зміст адміністративно-правових засобів забезпечення системи інформаційної безпеки держави / І. Р. Березовська // Підприємництво, господарство і право. — 2011. — № 5. — С. 117–119.; Березовська І. Р. Суспільно небезпечні прояви у виборчому процесі в Україні / І. Р. Березовська // Наукові записки ЛУБП. — 2011. — Вип. № 7. — С. 321–324.

<sup>9</sup> Стоєцький О. В. Реалізація адміністративно-правових норм у сфері забезпечення інформаційної безпеки / О. В. Стоєцький // Адвокат. — 2008. — № 12. — С. 36–39; Стоєцький О. В. Суб'єкти забезпечення інформаційної безпеки України: адміністративно-правові засади / О. В. Стоєцький // Підприємництво, господарство і право. — 2009. — № 11. — С. 161–164.; Стоєцький О. В. Характеристика інформаційної безпеки як складової інформаційної сфери / О. В. Стоєцький // Підприємництво, господарство і право. — 2009. — № 12. — С. 72–75.

накладення штрафу від десяти до двадцяти неоподаткованих мінімумів доходів громадян. Повторне протягом року вчинення порушення, передбаченого частиною першою цієї статі, за яке особу вже було піддано адміністративному стягненню, — тягне за собою накладання штрафу на громадян від двадцяти п'яти до п'ятдесяти неоподаткованих мінімумів доходів громадян»; пропозиція з огляду на протиріччя між ст. 212<sup>2</sup> КУпАП та ст. 28 Закону України «Про державну таємницю» щодо суб'єктів, які мають нести відповідальність за збереження державної таємниці, встановити відповідальність іноземців та осіб без громадянства за порушення законодавства про державну таємницю, доступ до державної таємниці яким надано у виняткових випадках на підставі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

У цілому аналіз праць, присвячених інформаційній безпеці України, дав змогу дійти висновку, що найпоширеніші — це галузеві розвідки, які, своєю чергою, можна поділити на три напрями.

Перший і наймасштабніший — це адміністративно-правові дослідження. Їх предметна сфера складається з проблем формування організаційно-правового забезпечення політики інформаційної безпеки в умовах глобалізації, інтеграції, становлення інформаційного суспільства, зокрема захисту персональних даних, захисту інформаційних ресурсів, забезпечення інформатизації, регулювання суспільних відносин щодо комп'ютерних програм, права громадян на інформацію у сфері державного управління, інформаційного забезпечення діяльності різних державних органів, а також проблем інформаційної культури в управлінській діяльності та теоретико-методологічних засад інформаційного права<sup>10</sup>.

Другий напрям галузево-правових досліджень — цивільно-правові. Основним їх предметом є цивільно-правові аспекти забезпечення інформаційної безпеки, до яких в основному належать проблеми цивільно-правової охорони, захисту та реалізації авторського права в умовах

<sup>10</sup> Новицька Н. Б. Організаційно-правові аспекти інформаційної культури в управлінській діяльності : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / Н. Б. Новицька ; Нац. акад. держ. подат. служби України. — Ірпінь, 2007. — 19 с.; Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / О. В. Олійник ; Інститут законодавства Верховної Ради України. — К., 2006. — 20 с.;

розвитку інформаційно-комунікаційних технологій, авторського права у сфері новітніх комп'ютерних технологій (комп'ютерних програм, комп'ютерних мереж, зокрема Інтернету), а також загальні цивільно-правові проблеми інформаційних відносин<sup>11</sup>.

Третій напрям — це кримінально-правові, кримінологічні та криміналістичні дослідження, актуальність яких зумовлена, передусім, посиленням такої загрози в інформаційній сфері як кіберзлочинність, проявами якої є комп'ютерне піратство, шахрайство, хакерство, а також потенційна загроза — кібертероризм. У зв'язку з цим, предметом кримінально-правових та кримінологічних досліджень виступають особливості кримінальної відповідальності за злочини у сфері комп'ютерної інформації, шляхи кримінально-правової охорони інформації в комп'ютерних системах і телекомунікаційних мережах, незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом, концептуальні питання забезпечення інформаційної безпеки кримінально-правовими засобами тощо.

Предметну сферу криміналістичних досліджень складають: питання методики та особливостей розслідування злочинів у сфері інформаційних комп'ютерних технологій; особливості предмета доказування у справах про комп'ютерні злочини; криміналістичний аналіз об'єктів комп'ютерних злочинів; використання комп'ютерних технологій для фіксації криміналістично значимої інформації у процесі розслідування; використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій, а також особливості розслідування різних злочинів, вчинених із використанням комп'ютерних технологій.

<sup>11</sup> Янина Е. В. Гражданско-правовое регулирование информационной безопасности : дисс. ... канд. юрид. наук : 12.00.03, 12.00.14 / Елена Владимировна Янина. — М., 2004. — 166 с.; Селіванов М. В. Захист права на комп'ютерну програму (авторсько-правовий аспект) : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес ; сімейне право ; міжнародне приватне право»/ М. В. Селіванов ; Нац. ун-т внутр. справ. — Х., 2002. — 20 с.; Кохановська О. В. Цивільно-правові проблеми інформаційних відносин в Україні : автореф. дис. на здобуття наук. ступеня доктора юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес ; сімейне право ; міжнародне приватне право»/ О. В. Кохановська ; Київ. нац. ун-т ім. Тараса Шевченка. — К., 2006. — 34 с.

## *Роботи з інформаційного права*

Безперечно, що аналіз бібліографії за темою дослідження не був би вичерпним, якщо ми не звернулися б до робіт з інформаціології та інформаційного права. Адже багатогранність і специфіка інформації сприяла появі значного масиву наукових досліджень, присвячених окремим її аспектам. Серед робіт вищезазначеного спрямування можна виокремити як присвячені інформаційному праві загалом, так і окремим її інститутам.

Хочемо наголосити:

**в Україні набагато раніше за всі колишні республіки СРСР було розроблено концепцію інформаційного права як окремої галузі права та проект Інформаційного кодексу України (Кодексу України про інформацію).**

Ми маємо пишатися, що саме українські науковці є гордістю інформаційної науки. Питання в іншому: як наші владці і парламентарі, а також чиновники від науки, які вирішують кому і коли можна захищатися, це використали, як змогли пристосувати інноваційні знання до химерних кліше ВАКівських спеціальностей і вимог МОН. Бо такі прізвища, як: **М. Я. Швець, Р. А. Калюжний, В. С. Цимбалюк** — мають бути вписані в аннали української інформаційної науки.

Саме ці вчені заклали підвалини і досі активно пропагують вже не тільки інформаційне право, а й правову кібернетику, активно підтримують на цьому шляху представників наукової школи В.А.Ліпкана, які протягом декількох років захистили понад 10 дисертаційних робіт за даної тематики.

Узагальненим авторським лейтмотивом бачення проблем у сфері інформаційного права можна визнати концептуальні положення робіт **В. С. Цимбалюка**, зокрема стосовно розмежування таких термінів, як «правова інформатика» та «інформаційне право». На прикладі дослідження джерел суспільних відносин стосовно розвитку інформатики, формування під її масовим впливом такого соціально-технічного та соціально-технологічного явища, як інформатизація, автор аргументовано пояснює природу структуризації інститутів інформаційного права. Воно розглядається ним як комплексна галузь права, що поступово інтегрує (через комплексне застосування методів інших галузей права)

на засадах теорії гіперсистем через предмет суспільних відносин — інформацію — три провідні його умовні складові — підсистеми, що поступово набувають ознак спеціальних підгалузей цього права:

- *мас-медіа права* (гуманітарна, семантична складова);
- *інформатизаційного права* (інфраструктурна, інженерно-технічна складова);
- *права інформаційної безпеки* (забезпечувальна складова).

Між цими трьома провідними складовими інформаційного права поступово формуються й інші спеціальні комплексні інститути права за напрямками (чи видами) інформаційної діяльності: освітнє право; архівне право; бібліотечне право тощо.

Ключовим *критерієм формування* таких інституцій права у загальній системі інформаційного права виступає філософський закон діалектики: перехід кількісних чинників (створення критичної маси інформації) на якісні — інституціоналізація суспільних відносин щодо інформації через прояв її як ознаки (предмета) діяльності певних суб'єктів суспільних відносин. При цьому інформація (критична її маса, кількість) набуває ознак суспільного ресурсу, без чого не може забезпечуватися подальший прогрес людства в умовах поступового вичерпування із природи її ресурсів (корисних копалин, води, чистого повітря і т.п.).

Важливо, що ці ідеї знаходять свій подальший вияв і в працях інших вчених інформаціологів: І. Арістової, К. Белякова, І. Березовської, В. Брижка, В. Гавловського, В. Гурковського, М. Гуцалюка, М. Дімчогло, О. Золотаря, Л. Капінус, В. Кір'ян, О. Климентьєва, Б. Кормича, О. Кохановської, Г. Красноступа, О. Логінова, Г. Линника, Є. Макаренко, Ю. Максименко, А. Марущака, П. Матвієнко, Д. Перова, І. Сопілки, В. Стоєцького, К. Татарнікової, А. Туніка, К. Череповського, О. Чуприни тощо.

Нині в рамках інформаційного права існують різні самостійні міжгалузеві наукові теорії. Так, **уперше в українській правовій літературі** дослідником К. І. Беляковим у монографії «Управление и право в период информатизации» запропоновано основні положення правової інформатики як самостійної міжгалузевої наукової теорії юридичного спрямування. Як зазначає автор, у рамках правової інформатики розробляються загальні методологічні основи інформатизації щодо всіх юридичних наук, управлінської та юридичної діяльності в цілому,



правова інформатика набуває рис загальної теорії вирішення правових завдань із використанням методів інформатики<sup>12</sup>.

У згаданій праці досліджуються проблеми сутності, завдань, цілей, умов і наслідків інформатизації в Україні, особливості правового регулювання сфери інформаційних відносин як інструмента державного управління процесами інформатизації.

Однією із перших вітчизняних робіт з інформаційного права була праця А. А. Письменицького, який до сфери інформаційного права України зарахував загальне інформаційне законодавство, Закон України «Про інформацію»; законодавче регулювання у сфері засобів масової інформації (законодавство України про друковані засоби масової інформації (пресу), про телебачення і радіомовлення, про інформаційні агентства); правове регулювання режиму інформації (законодавство України про державну таємницю), про захист інформації в автоматизованих системах; законодавство України у сфері науково-технічної інформації, автоматизованих систем інформації, бібліотечної справи [14].

Серед вітчизняних робіт з інформаційного права, де була приділена увага окремим аспектам захисту інформації з обмеженим доступом, особливе місце займає навчальний посібник з курсу «Інформаційне право», підготовлений колективом дослідників Науково-дослідного центру правової інформатики Академії правових наук України та Академії державної податкової служби України [15]. У межах розділу «Міжнародні аспекти інформаційного права» цієї розвідки автори розглядають питання міжнародної діяльності України в галузі захисту інформації шляхом окреслення основних положень щодо міжнародної діяльності України в галузі захисту інформації в автоматизованих системах, міжнародного захисту технологій, міжнародного захисту комерційної таємниці. Робота містить також розділ «Стан правового регулювання охорони та захисту інформації».

Аналіз думок та позицій дослідників надає можливість дійти висновку про відсутність системного бачення інституту захисту інформації та місця в ньому інформації з обмеженим доступом. Вже в другому виданні, переробленому та доповненому, автори, крім міжнародного захисту комерційної таємниці, виділяють окремий розділ, присвячений охороні та захисту персональних даних, розкриваючи, зокрема,

<sup>12</sup> Беляков К. И. Управление и право в период информатизации : [монография] / К. И. Беляков. — К. : КВІЦ, 2001. — 301 с.

такі питання, як становлення правової охорони і захисту персональних даних, історія гармонізації захисту персональних даних у європейських країнах, ідентифікаційний номер як об'єкт охорони і захисту персональних даних, національні підходи у регулюванні відносин щодо ідентифікаційних номерів, міжнародні підходи у регулюванні відносин щодо ідентифікаційних номерів, переваги та недоліки використання ідентифікаційних номерів, становлення охорони та захисту персональних даних в Україні [16].

Не менш важливим для розкриття теми дослідження є навчальний посібник А. І. Марущака «Інформаційне право: доступ до інформації», де автор системно розглядає сутність, зміст і структуру саме інституту доступу до інформації в контексті інформаційного права [17]. В іншому навчальному посібнику з інформаційного права, підготовленому А. І. Марущаком, вже відсутній розділ, присвячений захисту інформації з обмеженим доступом. Лише в межах розділу «Правове регулювання державної статистики в Україні» автор виділяє підрозділ «Доступ до статистичної інформації». Як зауважує А. І. Марущак, «...первинні дані, отримані органами державної статистики від респондентів під час проведення статистичних спостережень, а також адміністративні дані щодо респондентів, отримані органами державної статистики від органів, що займаються діяльністю, пов'язаною із збиранням та використанням адміністративних даних, є конфіденційною інформацією, яка охороняється Законом і використовується виключно для статистичних цілей у зведеному знеособленому вигляді» [18, с. 242].

Слід зауважити, що виданню вищезазначених навчальних посібників з інформаційного права передувало опублікування науково-практичного посібника А. І. Марущака «Правомірні засоби доступу громадян до інформації» у 2006 році. У цій науковій праці розкриваються теоретичні основи та практичні засади реалізації права громадян на доступ до інформації, досліджуються національно-правові та міжнародно-правові гарантії реалізації права громадян на доступ до інформації, визначаються особливості правової регламентації різноманітних засобів і процедур отримання громадянами інформації, зокрема доступу до інформації про діяльність органів державної влади, приватної інформації про фізичну особу, інформації про суб'єктів господарювання та їх діяльність, розкриваються правові основи отримання відкритої інформації через ЗМІ, доступу громадян до інформації через Інтернет,



доступу до інформації в архівах, окреслюються види юридичної відповідальності за порушення права на доступ до інформації тощо.

Аналіз вищезазначеної праці також вказує на відсутність єдиного уніфікованого понятійно-категоріального апарату у сфері доступу до інформації. Зокрема дослідник використовує поняття «відкрита інформація», «приватна інформація про фізичну особу» та інші.

Ми погоджуємось з думкою автора, що «...для простих громадян право на інформацію і, зокрема, його складова — доступ до інформації — є важливим чинником реалізації особистих майнових і немайнових прав, участі у громадському житті, в управлінні державними справами тощо. Для державних службовців розуміння особливостей права на доступ до інформації — це, по-перше, можливість реалізувати передбачені законом владні повноваження, а, по-друге, запорука ефективної реалізації громадянами їх права «знати...». Однак нерідко дана сфера суспільних відносин характеризується проблемними випадками і конфліктністю інтересів відповідних учасників. Зокрема, громадяни не знають механізмів доступу до інформації, меж реалізації власних прав на ту чи іншу інформацію. Це спричиняє негативні наслідки для них, як мінімум, у вигляді витраченого часу на безрезультатні інформаційні пошуки, і, як максимум, у вигляді юридичної відповідальності» [19, с. 6].

Серед інших вітчизняних навчальних посібників цього автора, присвячених інформаційному праву, варто згадати «Інформаційне право: регулювання інформаційної діяльності»<sup>13</sup>, де розкриваються поняття та види інформаційної діяльності в Україні; особливості нормативно-правового регулювання процесу розвитку інформаційного суспільства в Україні, поняття та основні напрями інформатизації в Україні. Крім того, визначено правовий статус суб'єктів інформаційної діяльності: друкованих засобів масової інформації (преси) в Україні, інформаційних агентств і бібліотек, архівних установ, телерадіоорганізацій, а також суб'єктів кінематографії, видавничої справи, державної статистики й рекламної діяльності.

У цілому аналіз вітчизняних і російських робіт з інформаційного права дає змогу дійти висновку про неоднозначне розуміння не тільки предмета та об'єкта інформаційного права, а і його системи. Так, у

<sup>13</sup> Марущак А. І. Інформаційне право : регулювання інформаційної діяльності : [навч. посіб.] / А. І. Марущак. — К. : Скіф ; КНТ, 2008. — 344 с.

російських наукових розвідках система інформаційного права структурно поділяється на дві частини — загальну та особливу. Щодо українських наукових праць, то певна градація на частини відсутня, а вибір тем залежить від авторського усвідомлення змістовного наповнення інформаційного права. Причому почасти авторське бачення не містить наукової аргументації, не ґрунтується на виявленні онтогенетичних зв'язків між суспільними явищами та правовою системою того чи іншого суспільства.

Здебільшого окреслення конкретних тем у роботах із інформаційного права неаргументоване та дискусійне. Зокрема, на нашу думку, викликає наукові заперечення відсутність у цитованій роботі А. І. Марущака розділу, присвяченого питанням інформаційної безпеки. Незважаючи на достатню кількість публікацій із даної теми, А. І. Марущак, який є одним із послідовників формування інформаційного права в Україні<sup>14</sup>, не розглядає інформаційну безпеку як інститут інформаційного права. Проте інформаційне суспільство наразі не може існувати поза контекстом інформаційної безпеки.

На загал, контекст безпеки стає онтологічним будь-яким питанням, які розглядаються в суспільстві. Саме тому В. А. Ліпкан і працює в напрямі формування загальної системи знань про безпеку<sup>15</sup>. Більш того, спроби наближення до теоретичних напрацювань В. А. Ліпкана робляться і в інших країнах, зокрема в США, де один із авторів даної монографії (В.А.Ліпкан) навчався за тематикою «Національна безпека США». Але, на жаль, попри значний потенціал безпекової наукової школи, в нашій державі такі знання поки непотрібні, а в РНБОУ і досі ухвалюють рішення, керуючись не знаннями про безпеку, а необхідністю задоволення олігархічних інтересів правлячої верхівки.

<sup>14</sup> Марущак А. І. Інформаційне право : доступ до інформації : [навч. посіб.] / А. І. Марущак. — К. : КНТ, 2007. — 532 с.; Марущак А. І. Інформаційне право : регулювання інформаційної діяльності : [навч. посіб.] / А. І. Марущак. — К. : Скіф ; КНТ, 2008. — 344 с.

<sup>15</sup> Ліпкан В. А. Теорія національної безпеки : [підруч.] / В. А. Ліпкан. — К. : КНТ, 2009. — 631 с.; Ліпкан В. А. Національна безпека України : [навч. посіб.] / В. А. Ліпкан. — [2-е вид.]. — К. : КНТ, 2009. — 576 с.; Ліпкан В. А. Національна і міжнародна безпека у визначеннях та поняттях / В. А. Ліпкан, О. С. Ліпкан. — [2-вид. доповн. і переробл.]. — К. : Текст, 2008. — 400 с.; Ліпкан В. А. Непарадигма національної безпеки / В. А. Ліпкан // Право України. — 2002. — № 11. — С. 19—23. Липкан В. А. Основы права национальной безопасности / В. А. Липкан // Публичное и частное право. — 2009. — № 2. — С. 34—46.

Повертаючись до аналізу праці *А. І. Марущака*, варто зауважити, що інформаційне право, виступаючи регулятором даних суспільних відносин, у тому числі відносин у сфері безпеки, є взаємопов'язаним із усіма елементами інформаційного суспільства. Тому можна підтримати думку *В. А. Ліпкана* і *Ю. Є. Максименко*, що інформаційна безпека є важливим і невід'ємним інститутом інформаційного права<sup>16</sup>.

Динамічність інформаційних процесів сприяла виокремленню комплексної галузі права, міжгалузевої юридичної науки. Інформаційне право як система норм, що регулює інформаційні відносини, ставить за мету дослідження інформаційної сфери правового регулювання суспільних відносин, виявлення об'єктів і суб'єктів інформаційних правовідносин, підготовку проектів нормативних правових актів у галузі дії інформаційного права, оцінювання ефективності проектів цих актів з використанням інформаційних технологій<sup>17</sup>.

В іншій вітчизняній праці з інформаційного права, підготовленої *В. С. Цимбалюком* [20], також порушуються важливі аспекти становлення нової галузі права — інформаційної, зокрема історичні джерела інформаційного права, формування методології і структури інформаційного права, законодавче забезпечення формування та розвитку єдиного інформаційного простору України, міжнародне інформаційне право, проблеми міжнародного співробітництва в правовому регулюванні та розвитку глобального інформаційного простору, удосконалення правової основи інформаційного простору й інформаційних ресурсів України. Водночас автор не зосереджує уваги на характеристиці основних підгалузей та інститутів інформаційного права, а саме інституту захисту інформації з обмеженим доступом. Хоча в межах розділу «Удосконалення правової основи інформаційного простору й інформаційних ресурсів України» дослідник пропонує проведення кодифікації вітчизняних нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері, як шлях та створення Кодексу України про інформацію. В окремі глави цього Кодексу *В. С. Цимбалюк* виділив такі, як «Захист інформації та персональних даних», «Комерційна таємниця», що ще раз доводить відсутність системного розуміння

<sup>16</sup> Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : [навч. посіб.] / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. — К. : КНТ, 2006. — 280 с.

<sup>17</sup> Копылов В. А. Информационное право : [учеб.] / В. А. Копылов. — [2-е изд., перераб. и доп.]. — М., 2003. — 512 с.

інституту захисту інформації з обмеженим доступом, чіткого значення основних видів таємниць.

На відміну від українських наукових джерел, у російських працях з інформаційного права [21] дослідники чітко класифікують галузі інституту інформаційного права, де в межах інституту захисту інформації з обмеженим доступом особливу увагу приділяють таким видам інформації, як «державна таємниця», «комерційна таємниця», «персональні дані».

Таким чином, на відміну від зарубіжних джерел з інформаційного права, де чітко спостерігається виділення загальної та особливої частин інформаційного права, а в рамках останньої виокремлюються конкретні види таємниць, у вітчизняних роботах відсутня градація інформаційного права на частини та розуміння критеріїв розмежування інформації з обмеженим доступом.

Крім робіт, де розглядаються різні аспекти інформаційної безпеки як важливого інституту інформаційного права, окремого розгляду в межах інформаційного права потребують роботи з системного удосконалення нормативно-правового регулювання інформаційних відносин, зокрема ті, що присвячені систематизаційній діяльності інформаційного законодавства в Україні.

У цьому контексті слід відмітити дисертаційні дослідження таких дослідників як В. А. Залізняк «Систематизація інформаційного законодавства в Україні», М. І. Дімчогло «Консолідація інформаційного законодавства України», К. П. Череповський «Інкорпорація інформаційного законодавства України», К. Г. Татарникова «Кодифікація законодавства України про інформацію».

Нині можемо констатувати, що в Україні вже склалася нова наукова школа доктора юридичних наук В. А. Ліпкана, представники якої вже захистили дисертації з різноманітних тем інформаційного права, а головне призначення і спрямування діяльності цієї школи націлено на формування системного ефективного правового регулювання розвинутого інформаційного суспільства в Україні в умовах динамічної і почасти інформаційно деструктивної глобалізації.

Так, В. А. Залізником у своїх працях<sup>18</sup> вперше запропоновано визначення поняття **«систематизація інформаційного законодавства»**

<sup>18</sup> Залізняк В. А. Систематизація інформаційного законодавства України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінан-

як цілеспрямованої діяльності компетентних органів чи окремих осіб з упорядкування нормативно-правових актів, що регулюють інформаційні відносини з метою підвищення ефективності правореалізації; проведено розмежування термінів «систематизація інформаційного законодавства», «удосконалення інформаційного законодавства», «розвиток інформаційного законодавства», «ефективність інформаційного законодавства».

Зокрема «удосконалення інформаційного законодавства» є більш широким поняттям, ніж «систематизація інформаційного законодавства» тому, що остання лише одна із численних форм удосконалення. Щодо поняття «розвиток інформаційного законодавства», то воно є більш широким ніж поняття «удосконалення інформаційного законодавства», оскільки охоплює не тільки зміну якісних характеристик законодавства, а й кількісних.

«Ефективність інформаційного законодавства» є ширшим щодо «удосконалення інформаційного законодавства», оскільки удосконалення лише один із факторів, що впливають на його ефективність. Крім удосконалення законодавства, ефективність законодавства обумовлена і механізмом правореалізації, рівнем правової культури населення, соціально-культурним, економічним та політичним потенціалом конкретної країни тощо. Саме тому поняття «ефективність інформаційного законодавства» є ширшим щодо поняття «удосконалення інформаційного законодавства». Отже, дані поняття від загального до конкретного слід розташувати за такою схемою: ефективність інформаційного законодавства — розвиток інформаційного законодавства — удосконалення інформаційного законодавства — систематизація інформаційного законодавства.

Автор зауважує, що «незважаючи на значну кількість праць, присвячених окремим аспектам систематизації законодавства України загалом, та інформаційного зокрема, комплексного і системного дослідження систематизації інформаційного законодавства України на монографічному рівні не здійснювалось. Наукові розвідки у цій сфері присвячені насамперед кодифікації як формі систематизації. Особливості розвитку інформаційного законодавства України розглядаються дослідниками через висвітлення окремих інститутів інформаційного

---

сове право ; інформаційне право» / В. А. Залізняк ; Нац. ун-т біоресурсів і природокористування України. — К., 2011. — 18 с.

права, найбільш популярним з яких є інститут інформаційної безпеки. У більшості наукових праць з цієї проблематики закріплено необхідність удосконалення інформаційного законодавства України шляхом систематизації, але без конкретних рекомендацій щодо форми чи напрямів її проведення».

Роботи<sup>19</sup> М. І. Дімчогло присвячені консолідації інформаційного законодавства, що передує кодифікації. У своїх працях дослідниця визначила особливості консолідації як виду систематизації, з'ясувала природу та ознаки консолідації, визначила співвідношення з інкорпорацією та кодифікацією, розробила засоби удосконалення інформаційного законодавства України при його кодифікації через консолідацію з іншими галузями вітчизняного права; здійснила консолідацію конституційних положень щодо інформаційних правовідносин у законодавстві, надала авторське бачення особливостям застосування консолідації при кодифікації інформаційного законодавства України тощо.

На основі досягнень юридичної науки, узагальнення правозастосування, аналізу вітчизняного та зарубіжного інформаційного законодавства розробив та надав науково обґрунтовані пропозиції щодо інкорпорації як важливого етапу систематизації інформаційного законодавства України задля підвищення його ефективності через наступну його кодифікацію К. П. Череповський у дисертаційному дослідженні «Інкорпорація інформаційного законодавства України».

У своїх численних працях<sup>20</sup> автор охарактеризував теоретичні засади інкорпорації інформаційного законодавства через аналіз наукової розробленості даної проблематики, сформував загальні методологічні положення інкорпорації як складового елемента систематизації інформаційного законодавства України, визначив концептуальні підходи проведення інкорпорації інформаційного законодавства України

<sup>19</sup> Дімчогло М. І. Основи теорії консолідації інформаційного законодавства / М. І. Дімчогло // Підприємництво, господарство і право. — 2012. — № 5. — С. 41–46.; Дімчогло М. І. Консолідація як вид систематизації інформаційного законодавства / М. І. Дімчогло // Правова інформатика. — 2012. — № 1 (33). — С. 15–24.; Дімчогло М. І. Консолідація конституційних положень щодо інформаційних правовідносин у законодавстві / М. І. Дімчогло // Підприємництво, господарство і право. — 2012. — № 6. — С. 39–42.

<sup>20</sup> Череповський К. П. Окремі питання інкорпорації міжнародного інформаційного права / К. П. Череповський // Правова інформатика. — 2012. — № 1 (33). — С. 68–76; Череповський К. П. Інкорпорація як етап до кодифікації інформаційного законодавства / К. П. Череповський // Підприємництво, господарство і право. — 2012. — № 5. — С. 47–49.



та складові елементи структури правового регулювання інформаційних відносин в Україні, обґрунтував необхідність проведення інкорпорації міжнародного інформаційного права як передумови гармонізації з ним інформаційного законодавства України, охарактеризував процеси здійснення інкорпорації інформаційного законодавства в окремих країнах, надав пропозиції щодо удосконалення правового регулювання інформаційних відносин в Україні, обґрунтував необхідність інкорпорації як етапу, що передуює кодифікації інформаційного законодавства України, та структуру проекту Кодексу України про інформацію на основі досліджень інкорпорації інформаційного законодавства.

Слід акцентувати увагу на монографії за редакцією В. А. Ліпкана та В. А. Залізняка «Систематизація інформаційного законодавства України», що стала першою роботою серії «**ORDO ORDINANS**» як наукової позиції і конкретного внеску дослідників у **пропаганду системної науки в Україні**, в якій наукове співтовариство вчених, молодих дослідників і майбутніх науковців, тобто найбільш фаховий, інтелігентний та обізнаний шар української історичної нації являє собою єдиний інтелектуальний континуум, епістемологічну спільноту — еліту, яка має формувати дороговкази майбуття та прогресивного розвитку нашої держави<sup>21</sup>.

У цій роботі автори з'ясували зміст понять «інформація», «правове регулювання інформаційних відносин в Україні», «інформаційне законодавство», «систематизація інформаційного законодавства», «ефективність законодавства», «уніфікація законодавства», «розвиток законодавства» та відмежували поняття «систематизація інформаційного законодавства» від інших споріднених понять, визначили правові передумови систематизації інформаційного законодавства та виокремили основні недоліки національного інформаційного законодавства, охарактеризували міжнародно-правові стандарти регулювання інформаційних відносин, виділили основні етапи систематизації вітчизняного інформаційного законодавства та концептуальні засади створення Інформаційного кодексу України, визначили основні форми систематизації інформаційного законодавства та надали їм характеристику,

<sup>21</sup> Ліпкан В. А. Систематизація інформаційного законодавства України : [монографія] / В. А. Ліпкан, В. А. Залізняка ; за заг. ред. В. А. Ліпкана. — К. : О. С. Ліпкан, 2012. — 304 с.; Ліпкан В. А. Правові та організаційні засади взаємодії суб'єктів протидії торгівлі людьми [монографія] / В. А. Ліпкан, О. В. Кушнір ; за заг. ред. В. А. Ліпкана. — К. : О. С. Ліпкан, 2013. — 376 с.

внесли пропозиції до проекту Інформаційного кодексу України та обґрунтували роль доктрини інформаційної безпеки як дороговказу до систематизації інформаційного законодавства України.

Ґрунтовність розгляду різних наукових підходів щодо порушеної проблематики, конструктивність та інноваційність поглядів і пропозицій авторів надає можливість констатувати, що це перше новаторське видання, де чітко простежується початок формування наукової школи В. А. Ліпкана.

У рамках цієї серії підготовлено та опубліковано також ще одну монографію представниці даної наукової школи — О. В. Шепети «Адміністративно-правові засади технічного захисту інформації», де розглядаються теоретичні та адміністративно-правові проблеми технічного захисту інформації в Україні<sup>22</sup>. Зокрема розкрито зміст становлення та розвитку технічного захисту інформації, організація цього захисту в Україні, а також його нормативно-правове регулювання.

Особливо корисними для розкриття нашого предмета дослідження є окреслені авторкою такі питання, як:

- технічний захист інформації як об'єкт адміністративно-правового регулювання;
- органи державної влади та система технічного захисту інформації України;
- взаємодія суб'єктів системи технічного захисту інформації;
- удосконалення державної політики технічного захисту інформації;
- актуальні напрями удосконалення інформаційного законодавства України;
- підвищення ефективності правового регулювання технічного захисту інформації;
- поліпшення системи підготовки фахівців з технічного захисту інформації (ТЗІ).

Вважаємо конструктивними запропоновані О. В. Шепетою основні напрями удосконалення державної політики у сфері ТЗІ, а саме:

- удосконалення чинних та створення нових нормативно-правових актів щодо захисту інформації, яка становить державну та

<sup>22</sup> Адміністративно-правові засади технічного захисту інформації : [монографія] / О. В. Шепета. — К. : О. С. Ліпкан, 2012. — 296 с.



- іншу, передбачену законом, таємницю, конфіденційної інформації, що належить державі;
- розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави;
  - удосконалення правових механізмів організаційного забезпечення ТЗІ;
  - удосконалення нормативно-правових актів щодо умов і правил провадження діяльності у сфері ТЗІ;
  - удосконалення нормативно-правових актів щодо здійснення контролю за імпортом з метою впровадження в Україні іноземних інформаційних технологій з захистом інформації та засобів забезпечення ТЗІ;
  - розроблення нормативних документів з питань формування та розвитку моделі загроз для інформації;
  - розроблення нормативних документів з питань сертифікації засобів забезпечення ТЗІ та атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;
  - удосконалення чинних і розроблення нових нормативних документів із питань ТЗІ;
  - удосконалення організаційного забезпечення, що охоплює забезпечення створення підрозділів ТЗІ в органах державної влади та органах місцевого самоврядування, академіях наук, Збройних силах, інших військових формуваннях, органах внутрішніх справ, на підприємствах, в установах і організаціях усіх форм власності, діяльність яких пов'язана з інформацією, що підлягає технічному захисту; підготовка кадрів для роботи у сфері ТЗІ; залучення до розв'язання проблем ТЗІ вітчизняних науковців і висококваліфікованих спеціалістів; розвиток міжнародного співробітництва у сфері ТЗІ;
  - удосконалення науково-технічної та виробничої діяльності<sup>23</sup>.

<sup>23</sup> Адміністративно-правові засади технічного захисту інформації : [монографія] / О. В. Шепета. — К. : О. С. Ліпкан, 2012. — 296 с.

## *Роботи, присвячені безпосередньо різним аспектам інформації з обмеженим доступом (спеціалізовані роботи)*

Сплеск досліджень, присвячених безпосередньо захисту інформації з обмеженим доступом, припав на 2006–2007 роки. Одними із перших робіт в окресленому контексті були праці таких дослідників як О. В. Ботвінкін, В. П. Ворожко, А. К. Гринь, А. М. Гуз, В. В. Макаренко, А. І. Марущак, С. М. Сидоренко, А. Б. Стоцький, С. В. Суслін [22–23].

Так, О. В. Ботвінкін та В. П. Ворожко підготували аналітичний огляд для викладачів, науковців, слухачів і студентів Інституту захисту інформації Національної академії Служби безпеки України, співробітників режимно-секретних органів усіх відомств, присвячений інституту інформації з обмеженим доступом в законодавстві України, де розглянули питання класифікації інформації з обмеженим доступом, режими доступу до неї, особливості її поширення та встановлення відповідальності за правопорушення у цій сфері. Автори на основі аналізу нормативної бази досліджують наскільки врегульована сфера охорони кожного з передбачених українським законодавством видів інформації з обмеженим доступом, що не є державною таємницею [23, с. 5]. Дослідниками було виокремлено ряд таємниць (конфіденційна інформація про особу, адвокатська, банківська, військова, комерційна, лікарська, професійна, службова таємниці, а також таємниця голосування, кореспонденції, листування, наради суддів, нотаріальних дій, страхування, телефонних розмов, усиновлення, вкладів (рахунків), заповіту, слідства, інформації у поштовому зв'язку, про стан здоров'я, псевдоніма). Незважаючи на актуальність вищезазначеного дослідження, виникає питання про критерій виділення того чи того виду таємниць, оскільки автори його не визначають, окреслюючи конкретну таємницю залежно від власного бачення проблематики. Водночас незрозуміла, наприклад, різниця та співвідношення професійної, службової, військової, лікарської таємниць. Вкрай важливі висновки О. В. Ботвінкіна та В. П. Ворожко щодо основних проблем захисту інформації з обмеженим доступом в Україні:

- недосконалість правових норм, що регулюють встановлення режимів обмеження доступу до інформації, обов'язки суб'єктів правовідносин щодо захисту інформації з обмеженим доступом, відповідальності за порушення;

- недостатній розвиток правового регулювання відносин, які пов'язані з поширенням певних видів інформації у відкритих інформаційно-комунікаційних мережах;
- недостатня ефективність правових механізмів встановлення відповідальності за правопорушення встановлених режимів обмеження доступу до інформації.

Одним із перших, хто розробив курс лекцій для студентів, що навчаються за спеціальностями «Організація захисту інформації з обмеженим доступом», «Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом», «Правоохоронна діяльність», був А. І. Марущак. У своїй науковій праці «Правові основи захисту інформації з обмеженим доступом» він розкриває такі складні аспекти проблематики, як правовий статус інформації, поняття та зміст інформації з обмеженим доступом, охорона державної таємниці в Україні, правові основи захисту комерційної таємниці, поняття та зміст банківської таємниці, правовий статус і зміст інформації з обмеженим доступом про особу, захист конфіденційної інформації, що є власністю держави, правова регламентація технічного захисту інформації в Україні, правові основи захисту інформації в інформаційно-телекомунікаційних системах, національна система конфіденційного зв'язку, юридична відповідальність за правопорушення у сфері обігу інформації з обмеженим доступом, міжнародно-правові основи захисту інформації з обмеженим доступом.

Дослідження вищезазначеної роботи надає можливість дійти висновку, що автор зосереджує увагу лише на окремих видах інформації з обмеженим доступом: державній, комерційній, банківській таємниці, а також інформації з обмеженим доступом про особу. Хоча дослідник зауважує, що інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну, до видів останньої відповідно до чинного законодавства належить державна, комерційна, службова, професійна, військова, банківська, адвокатська, лікарська, а також таємниця страхування, усиновлення, голосування, нотаріальних дій, листування, телефонних розмов, телеграфної та іншої кореспонденції [24, с. 23–25]. Слід зазначити, що через відсутність законодавчого уніфікованого понятійно-категоріального апарату в цій сфері помітна розбіжність понять і в цій розвідці. Зокрема, поряд з «інформацією з обмеженим доступом про особу» використовується поняття «персональна інформація» тощо.

Зроблений нами аналіз вітчизняних джерел з порушеної проблематики обумовлює висновок про відсутність, крім зазначених вище, ще будь-яких робіт, предметом дослідження яких є системний розгляд захисту інформації з обмеженим доступом. Значне коло наукових робіт присвячено окремим видам інформації з обмеженим доступом: конфіденційній інформації, комерційній, державній, банківській, адвокатській тощо таємницям, а також персональним даним [25–31].

Організаційно-правові основи охорони конфіденційної інформації, що є власністю держави, розкрито у навчальному підручнику, підготовленому науково-педагогічним колективом Національної академії Служби безпеки України. У підручнику окреслено питання становлення і формування поняття та змісту службової таємниці у законодавстві СРСР, основи правового регулювання захисту конфіденційної інформації, що є власністю держави, порядок обігу, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, охорона конфіденційної інформації, що є власністю держави, під час прийому іноземних делегацій, груп та окремих іноземців, порядок здійснення СБ України контролю за обігом документів, які містять конфіденційну інформацію, що є власністю держави, порядок оформлення матеріалів про адміністративні правопорушення у сфері охорони конфіденційної інформації, що є власністю держави, законодавство іноземних країн про захист службової таємниці тощо [32].

Як слушно зауважують автори підручника: «...аналіз чинного законодавства та окремих аспектів оперативно-службової діяльності СБ України свідчить, що передумовами до витоку ІзОД створюються внаслідок безпечності, халатності, безвідповідальності осіб, обізнаних з нею, послаблення контролю та спрощеного підходу деяких керівників органів державної влади до організації її захисту. Безперечно цьому сприяє й недостатність правового регулювання деяких аспектів обігу конфіденційної інформації, що є власністю держави» [32, с. 5].

Інформація з обмеженим доступом, як ми вже зазначали, лежить у площині предмета дослідження інформаційної безпеки як адміністративного й інформаційного права, так і кримінального, цивільного, міжнародного, конституційного тощо.

Наголошуємо, що найбільш широкими за багатоманітністю розкритих аспектів інформації з обмеженим доступом є російські праці, де вчені розкривають цивільно-правовий, конституційний, кри-

мінально-правовий, міжнародний аспекти цієї проблематики на рівні дисертаційних досліджень. Насамперед варто відзначити таких, як: А. О. Антопольський, І. О. Вельдер, А. В. Дворецький, А. С. Маркевич, І. Ю. Мирських, Н. І. Петрікіна, І. І. Салихов, О. В. Семашко, І. В. Строганова, І. О. Юрченко.

Однією із перших вітчизняних наукових робіт, що досліджує під кримінально-правовим кутом захист інформації з обмеженим доступом є дисертаційне дослідження М. В. Рудика «Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом». Цінність цієї праці в тому, що її автором: «...досліджено законодавче регулювання різних видів таємниць, закріплених у вітчизняному та зарубіжному кримінальному законодавстві, проаналізовано окремі види таємниць і визначено їх класифікацію, здійснено системний та порівняльний аналіз складів злочинів, які передбачають відповідальність за посягання на таємницю: приватного життя, комерційну, банківську, державну, розглянуто дискусійні питання кваліфікації злочинів, пов'язаних з незаконним збутом, розповсюдженням комп'ютерної інформації з обмеженим доступом, а також розроблено пропозиції щодо вдосконалення чинного законодавства у сфері кримінально-правової охорони комп'ютерної інформації з обмеженим доступом» [33, с. 6]. Дисертант акцентує увагу винятково на кількох видах таємниць, класифікуючи комп'ютерну інформацію з обмеженим доступом за допомогою родового об'єкта злочину на три групи таємниць: 1) приватного життя; 2) комерційну та банківську; 3) державну. Тож виникає логічне питання: чому дослідник обмежився лише цими видами таємниць?

Крім кримінального права, одну із провідних ролей у механізмі правової охорони інформації з обмеженим доступом відіграє цивільне право. Цивільний кодекс України [34] (далі — ЦК України) серед об'єктів цивільних прав закріпив інформацію, що сприяло появі значної кількості робіт за спеціальністю 12.00.03 (цивільне право і цивільний процес; сімейне право; міжнародне приватне право). Серед розвідок цього спрямування слід відмітити дисертаційне дослідження О. О. Кулініч «Інформація з обмеженим доступом як об'єкт цивільних прав», оскільки вона вперше визначила поняття та розробила систему ознак інформації з обмеженим доступом як об'єкта цивільних прав, а саме: недоступність широкому колу осіб; приналежність визначеному суб'єктному складу; обмеження вільного доступу третіх осіб до інфор-

мації внаслідок прийняття власником інформації певних заходів; наявність особливої соціальної цінності інформації в силу її дійсної або потенційної недоступності третім особам; відповідність інформації обмеженням, установленим чинним законодавством [35, с. 9]. Крім того, вперше було визначено цивільно-правовий режим інформації з обмеженим доступом, а саме: це режим таємниці, який встановлюється власником інформації та припускає певний, визначений ним порядок одержання, використання, поширення і зберігання інформації за винятком випадків, визначених чинним законодавством. У дисертації також вказано на особливості цивільно-правового регулювання окремих видів інформації з обмеженим доступом, зокрема: інформації, що становить таємницю приватного життя, комерційну таємницю, професійну та службову таємницю, які залежать від суб'єкта відносин, що виникають з приводу інформації та вимог чинного законодавства, що висуваються до обігу певного виду інформації [35, с. 10].

Додатково обґрунтовуючи позицію, «відповідно до якої необхідно відрізнити таємницю як змістову характеристику інформації, яка охороняється, (таємниця усиновлення, особиста таємниця) від таємниці як правового режиму інформації з обмеженим доступом» [35, с. 10], дисертантка зосередила увагу на особливостях цивільно-правового регулювання окремих видів інформації з обмеженим доступом, зокрема таємниці приватного життя, комерційної, професійної та службової таємниці.

Генезис інституту захисту інформації в Україні та провідних країнах світу детально досліджено в навчальному підручнику, підготовленому А. М. Гузом. Як слушно зауважує автор: «...без глибокого осмислення минулого, яким би складним і суперечливим воно не було, неможливо творити нову систему захисту інформації в Україні. Всесвітня історія свідчить про тісну взаємопов'язаність процесів минулого та сучасного» [36, с. 3]. Дослідником окреслено становлення та розвиток вітчизняної системи захисту інформації, починаючи з доби Київської Русі, Литовсько-польської держави, Запорізької Січі та держави Богдана Хмельницького до формування національної системи захисту в Україні у 1991–2005 рр. Щодо зарубіжного досвіду захисту інформації, то розглянуто особливості системи захисту інформації в Російській Федерації, США, Великій Британії, Франції, Німеччині, Польщі, Чехії, Словаччині, Угорщині, Литві, Латвії, Естонії, Японії та Китаї (1991–2005 рр.). Зважаючи на євроатлантичні прагнення нашої держави, вче-



ний зосередив увагу на критеріях і цінностях захисту інформації в країнах-членах НАТО, а також гармонізації вітчизняного законодавства до стандартів цієї безпекової субрегіональної міжнародної організації.

**На основі дослідження генезису наукових джерел, присвячених захисту інформації з обмеженим доступом, можна дійти таких висновків.**

1. Інформація з обмеженим доступом є предметом дослідження багатьох юридичних наук — теорії держави та права, інформаційного права, адміністративного права, кримінального права, цивільного права та інших.
2. Здебільшого інститут інформації з обмеженим доступом є предметом дослідження наукових праць у рамках інформаційного права та інформаційної безпеки.
3. Адміністративний аспект інформації з обмеженим доступом розкривається в межах адміністративних розвідок, присвячених інформаційній безпеці.
4. Відсутність законодавчого закріплення відповідних дефініцій та видів інформації з обмеженим доступом сприяло неоднозначному баченню видів інформації з обмеженим доступом та наявності розбіжності основних понять, коли один і той самий вид інформації з обмеженим доступом має не тільки різне визначення, а й назву.
5. Серед інформації з обмеженим доступом виокремлюють здебільшого такі види таємниць, як державна, комерційна, таємниця персональних даних. У зв'язку з чим вони найбільш досліджувалися у вітчизняних наукових розвідках.

Беручи до уваги вищезазначені висновки та положення, слід виокремити **три етапи становлення наукової думки, присвяченої інформації з обмеженим доступом, у вітчизняній адміністративній доктрині**. *Перший етап* (1991–2005 рр.) характеризується поверховим розглядом інформації з обмеженим доступом у контексті дослідження різних аспектів інформаційної безпеки та інформаційного права, де захист інформації з обмеженим доступом визначається як важливий напрям інформаційної безпеки чи інститут інформаційного права, а також актуальний напрям наукової діяльності. Для *другого етапу* (2006–2007 рр.) властива поява досліджень монографічного рівня, предметом яких є безпосередньо захист інформації з обмеженим доступом, особливості доступу до зазначеної вище інформації та виділення основних видів таємниць. *Третій етап* (2008 р. — донині) характеризується

ся інтенсивним проведенням наукових досліджень та опублікуванням робіт різної спеціалізації, предметом яких є конкретні види таємниць (банківська, комерційна, персональна таємниця тощо).

## 1.2 МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Інформація з обмеженим доступом може розглядатися з різних ракурсів, зважаючи на мету, завдання і методологію дослідження. Складність і міждисциплінарність предмета дослідження обумовлює необхідність використання різних методологічних підходів і принципів. Тим більше, що інформаційне законодавство України, яке урегульовує суспільні відносини у сфері захисту інформації з обмеженим доступом та є доволі динамічним. Для підвищення його ефективності слід здійснювати комплекс заходів, що розробляються на науковій основі із належним науковим забезпеченням.

Вже стало традиційним пов'язувати подальший розвиток юридичної науки з удосконаленням її методології і методик юридичних наукових досліджень. Саме на це звертають увагу багато науковців<sup>24</sup>.

<sup>24</sup> Жоль К. К. Методы научного познания и логика (для юристов): [учеб. пособ.] / К. К. Жоль. — К. : Атика, 2001. — 288 с.; Жоль К. К. Философия и социология права : [учеб. пособ.] / К. К. Жоль. — К. : Юринком Интер, 2000. — 480 с.; Рабінович П. М. Трансформація методології вітчизняного праводержавознавства: досягнення і проблеми / П. М. Рабінович // Юридична Україна. — 2003. — № 1. — С. 20–25.; Костицький М. Необхідність трансформації юридичної методології як бази розвитку права / М. Костицький // Український правовий часопис. — 2004. — № 7. — С. 16–17.; Козюбра Н. И. Понятие и структура методологии юридической науки / Н. И. Козюбра // Методологические проблемы юридической науки / отв. ред. Н. И. Козюбра. — К., 1990. — С. 5–19.; Рабінович П. М. Проблеми трансформації методології вітчизняного правознавства: досягнення, втрати, перспективи / П. М. Рабінович // Методологічні проблеми правової науки. — Х., 2003. — С. 75–78.; Козюбра М. І. Наукознавчі проблеми загальної теорії держави і права / М. І. Козюбра // Методологічні проблеми правової науки. — Х., 2003. — С. 91–94.; Казимирчук В. П. Право и методы его изучения / В. П. Казимирчук. — М. : Юрид. лит., 1965. — 204 с.; Гусарев С. Д. Юридична деонтологія (Основи юридичної діяльності) : [навч. посіб.] / С. Д. Гусарев, О. Д. Тихомиров. — [4-те вид., стер.]. — К. : Знання, 2010. — С. 66–67.; Тихомиров А. Д. Юридическая компаративистика : философские, теоретические и методологические проблемы / А. Д. Тихомиров. — К. : Знання, 2005. — С. 248–249.



Особливого значення набуває визначення методологічних засад для досліджень, присвячених розгляду різних аспектів інформаційної проблематики, зокрема інформації з обмеженим доступом.

Це пов'язано з тим, що ця проблематика набула актуальності лише наприкінці ХХ сторіччя, тож нині відчутний брак традицій розуміння своєрідності інформаційних процесів і явищ.

Розгляд методологічних засад дослідження адміністративно-правового режиму інформації з обмеженим доступом набуває особливої актуальності ще й тому, що важливим етапом процесу наукового пізнання є обґрунтований вибір методології та методів дослідження.

Дослідження інформації з обмеженим доступом доволі складне завдання через специфічність її природи та циркулювання у різних сферах суспільного буття.

Такі властивості предмета дослідження потребують комплексного використання різних методів у єдності та взаємному доповненні, визначення оптимального співвідношення між методами, «традиційними» для юридичної науки та новими — соціологічними, філософськими, політологічними, психологічними підходами, емпіричними та теоретичними, якісними та кількісними прийомами пізнання, використання яких повинно супроводжуватися відповідною їхньою перебудовою, трансформацією, пристосуванням до специфіки предмета дослідження.

В юридичній науковій літературі викладено різні підходи до виокремлення структури методології юридичної науки, аналіз яких дозволив обрати, виходячи із особливостей генези, властивостей інформації з обмеженим доступом та її адміністративно-правового режиму, такий підхід, який надав можливість дослідити їх у контексті методологічних засад сучасної юридичної науки.

Як слушно зауважують С. Д. Гусарев та О. Д. Тихомиров: «...методологія юридичної науки не зводиться тільки до сукупності наукових методів пізнання правової дійсності і побудови наукових знань, а є складним і багатоплановим утворенням, що охоплює: світоглядні, філософські, теоретичні та наукознавчі засади; проблеми структури юридичного наукового знання взагалі і в особливості його теорій та концепцій; тенденції виникнення, функціонування і зміни наукового знання, а також його класифікації, типологізації; понятійний апарат юридичної науки і її наукову мову; структуру і склад теоретичних та ін-

ших наукових методів, що застосовуються; формалізовані методики і процедури конкретного їх використання»<sup>25</sup>.

Цю думку також підтверджено і іншими вченими, які брали участь у міжнародній науково-теоретичній конференції «Проблеми методології сучасного правознавства». Зокрема ними було зазначено: «...загальний стан розробки методологічних проблем українського правознавства відстає від сучасних потреб, хвибує відчутними недоліками. Поширення набули методологічна невизначеність, еkleктизм, некритичне запозичення певних методів та методичних засобів інших наук поза межами їх можливого використання у дослідженнях соціально-правових проблем. Мають місце непоодинокі прояви абстрактного соціально-беззмістовного визначення державно-правових явищ, нерозбірливого застосування концепцій та норм, що належать до різних, нерідко протилежних зарубіжних правових систем, недооцінки правових принципів...»<sup>26</sup>.

Отже, для дослідження адміністративно-правового режиму інформації з обмеженим доступом доцільно виокремити:

- світоглядні, філософські та наукознавчі засади дослідження;
- методологічні принципи та підходи;
- основні наукові методи, що використовувалися для вивчення предмета та побудови відповідних наукових знань, що склали понятійно-категоріальний апарат дослідження;
- теоретичні наукові юридичні знання, які використовувалися при здійсненні дослідження.

Розуміння понять «методологія», «методи», а також їх співвідношення доволі дискусійне. Оперуючи вищезазначеними поняттями, дослідники не бачать різниці між ними та здебільшого вживають їх як синоніми.

Так, О. Ф. Скакун зазначає: «...*метод юриспруденції* являє собою засіб юридичного пізнання, створення та організації юридичного знання. За допомогою юридичного методу предмет юриспруденції конкретизу-

<sup>25</sup> Гусарев С. Д. Юридична деонтологія (Основи юридичної діяльності) : [навч. посіб.] / С. Д. Гусарев, О. Д. Тихомиров. — [4-те вид., стер.]. — К. : Знання, 2010. — С. 66–67; Тихомиров А. Д. Юридическая компаративистика: философские, теоретические и методологические проблемы / А. Д. Тихомиров. — К. : Знання, 2005. — С. 248–249.

<sup>26</sup> Рекомендації міжнародної науково-теоретичної конференції «Проблеми методології сучасного правознавства» // Вісник Академії правових наук України. — X., 1997. — Вип. 1 (8). — С. 150–154.

ється і оформлюється у відповідну юридичну теорію (юридичну науку) як єдину систему знань про державу та право, висловлену в поняттях»<sup>27</sup>.

В. В. Лазарєв, С. В. Липень визначають *методологію* як сукупність принципів, прийомів, способів наукової діяльності, що застосовується для отримання істинних, та таких, що відображають об'єктивну реальність, знань<sup>28</sup>.

Водночас авторський колектив російських вчених, оперуючи усталеною і консервативною конструкцією, зазначають, що *метод* охоплює способи, прийоми, засоби вивчення<sup>29</sup>.

Привертає увагу підхід колективу вітчизняних науковців: «...методологія — це наука про методи, складне утворення, що характеризує систему різних методологічних рівнів і методів пізнання предмета. В механізмі юридичного пізнання вона може розглядатися як вихідна категорія, а метод у свою чергу — це базова категорія методології, адже вона є не що інше, як теорія методів»<sup>30</sup>.

Здебільшого у вітчизняних наукових колах методологію визначають як концептуальний виклад мети, змісту, методів дослідження, які забезпечують отримання максимально об'єктивної, точної, систематизованої інформації про процеси та явища<sup>31</sup>. Таке трактування цих понять можна знайти у більшості енциклопедичних видань.

Аргументовану позицію з цього приводу ми детально виклали в першій книзі з серії «**ORDO ORDINANS**» — монографії В. А. Ліпкана та В. А. Залізняка «Систематизація інформаційного законодавства»<sup>32</sup>.

Зважаючи на вищевикладене, вважаємо, що ці поняття («метод» і «методологія») слід використовувати в таких значеннях.

**Метод** 1) спосіб досягнення мети, певним чином упорядкована діяльність; 2) спосіб дослідження конкретної сфери об'єктивної реальності

<sup>27</sup> Скакун О. Ф. Теорія держави і права : [підруч.] / О. Ф. Скакун. — Х. : Консул, 2008. — 656 с.

<sup>28</sup> Лазарєв В. В. Теория государства и права : [учеб. для вузов] / В. В. Лазарєв, С. В. Липень. — М. : Спарк, 2004. — 528 с.

<sup>29</sup> Теория государства и права : [курс лекций] / под ред. Н. И. Матузова, А. В. Малько. — М. : Юристъ, 1997. — 672 с.

<sup>30</sup> Гусарев С. Д. Теория права і держави : [навч. посіб.] / С. Д. Гусарев, А. Ю. Олійник, О. Л. Слюсаренко. — К. : Правова єдність, 2008. — 270 с.

<sup>31</sup> Шейко В. М. Організація та методика науково-дослідницької діяльності : [підруч.] / В. М. Шейко, Н. М. Кушнарєнко. — [2-ге вид., переробл. і доповн.]. — К. : Знання-Прес, 2002. — 295 с.

<sup>32</sup> Ліпкан В. А. Систематизація інформаційного законодавства України : [монографія] / В. А. Ліпкан, В. А. Залізник ; за заг. ред. В. А. Ліпкана. — К. : О. С. Ліпкан, 2012. — 304 с.

ті, який надає загальнометодологічним засадам предметної визначеності. Метод як засіб пізнання являє собою спосіб відтворення в розумовій діяльності досліджуваного предмета. *Гегель*: «Метод є рухом самого змісту і через це не може розроблятися поза зв'язком зі змістом».

**Методологія** 1) сукупність принципів, прийомів і методів дослідження будь-якого об'єкта; 2) певним чином сформована ідеологія науково-аналітичної роботи, що базується на певних припущеннях, ідейно-теоретичних засадах, ціннісних настановах, які загалом задають науково-пізнавальний горизонт ставлення людини до світу, суб'єкта до об'єкта, що вивчається та змінюється, в процесі людської діяльності; 3) наука про методи пізнання й перетворення світу.

Наукова значимість і пізнавальна цінність методу та методології, що застосовується при дослідженні, визначається їх евристичним потенціалом, здатністю збагатити науку новим знанням, виявити нові ракурси у досліджуваному явищі, сприяти всебічному його розумінню.

Серед основних методологічних підходів, що використовуватимуться при розкритті адміністративно-правового режиму інформації з обмеженим доступом, є діяльнісний<sup>33</sup>, функціональний<sup>34</sup>, системний<sup>35</sup>.

Діяльнісний підхід базується на засадах «теорії діяльності», використовується в різних соціально-гуманітарних науках, у його межах діяльність інтерпретується як пояснювальний принцип, парадигма, теоретична модель та метод наукових досліджень<sup>36</sup>, що надають можли-

<sup>33</sup> Гусарев С. Д. Юридична діяльність : методологічні та теоретичні аспекти / С. Д. Гусарев. — К. : Знання, 2005. — 375 с.

<sup>34</sup> Гусарев С. Д. Функціональний підхід та функції юридичної практичної діяльності / С. Д. Гусарев // Держава і право : зб. наук. праць. Юридичні і політичні науки. — К., 2005. — Вип. 30. — С. 55–60.

<sup>35</sup> Ганьба Б. П. Системний підхід та його застосування в дослідженні України як демократичної, соціальної, правової держави : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права ; історія політичних і правових вчень» / Б. П. Ганьба ; Нац. ун-т внутр. справ. — Х., 2001. — 19 с.; Сагатовский В. Н. Системная деятельность и ее философское осмысление / В. Н. Сагатовский // Системные исследования. Методологические проблемы. Ежегодник, 1980. — М., 1981. — С. 52–68.; Батишев С. С. Деятельность и ценности. Критика деятельностного подхода к теории интериоризации / С. С. Батишев // Вопросы философии. — 1985. — № 2. — С. 41–44.; Берман Г. Дж. Западная традиция права: эпоха формирования / Г. Дж. Берман ; [пер. с англ.]. — [2-е изд.]. — М. : МГУ ; ИНФРА-М-НОРМА, 1998. — 624 с.

<sup>36</sup> Тодика Ю. М. Тлумачення Конституції і законів України: теорія та практика : [монографія] / Ю. М. Тодика. — Х. : Факт, 2003. — 322 с.; Рожко К. Г. Принцип деятельности / К. Г. Рожко. — Томск : Томск. ун-т, 1983. — 212 с.; Батишев Г. С. Деятельная сущность человека как

вість розглянути навколишній світ як прояв, форму, умову, результат цілеспрямованого впливу людини та суспільства.

Діяльність як категорія високого рівня абстрактності в наукових джерелах по-різному співвідноситься із іншими близькими за змістом поняттями — поведінкою, спілкуванням, активністю, бездіяльністю тощо.

Основними засадами діяльнісного підходу для дослідження адміністративно-правового режиму інформації з обмеженим доступом є:

- забезпечення адміністративно-правового режиму інформації з обмеженим доступом як діяльність здійснюється певними суб'єктами (державними та недержавними), має переважно цілеспрямований характер, передбачає усвідомлення мети та прагнення її досягнення, втілюється в результаті, є соціально (в широкому розумінні) зумовленою, призначене для задоволення відповідних суспільних і індивідуальних інформаційних потреб, реалізується у взаємодії з іншими соціальними суб'єктами;
- оцінка певних конкретно-історичних та соціально-культурних обставин залежить від умов функціонування держави та інститутів громадянського суспільства, стану розвиненості інформаційного суспільства, інформаційних процесів і технологій, інформаційної культури населення тощо;
- впорядкування різноманітними соціальними регуляторами, домінуючим серед яких, проте не єдиним, є правове забезпечення, а також власне нормами інформаційного спілкування, внутрішніми переконаннями суб'єктів;
- використання різноманітних засобів, вибір яких залежить від природи об'єкта діяльності, його мети, властивостей суб'єкта, а послідовність використання — складає процедуру діяльності або його окремих фрагментів — діянь.

Здебільшого в юридичній науці діяльнісний підхід пов'язується з функціональним підходом, виходячи із того, що поняття функцій є однією із центральних категорій, за допомогою якої в науковій літературі розкриваються питання сутності соціального призначення явищ, висвітлюється спрямованість впливу<sup>37</sup>.

философский принцип / Г. С. Батищев // Проблема человека в современной философии. — М., 1969. — С. 73–144.

<sup>37</sup> Функция государства в независимых странах Африки. — М. : Наука, 1972. — 324 с.; Популярна юридична енциклопедія. — К. : Юрінком Інтер, 2002. — С. 503; Онопенко П. В. Правоохо-

Деякі автори їх ототожнюють<sup>38</sup>, але найчастіше розрізняють<sup>39</sup>.

Останнім часом методи системного аналізу та функціональний дедалі частіше використовуються для вивчення окремих явищ правової дійсності, особливо, якщо вони мають складну будову та пов'язані з іншими явищами. Розповсюдженими є також поняття системно-функціонального методу або принципу, системного та функціонального підходу. Оскільки право, держава, їх структурні підрозділи, а особливо інформаційний простір — це відкриті системи, то вони перебувають у стані постійної взаємодії із зовнішнім середовищем, внаслідок чого взаємозмінюються, а це, зокрема, визначає актуальність використання системного та функціонального підходів у пізнанні цих складних явищ.

Своєрідністю функціонального підходу до дослідження адміністративно-правового режиму інформації з обмеженим доступом є виокремлення елементів взаємодій різноманітних суб'єктів або елементів його забезпечення і визначення їх місця, ролі, значення. Така площина розуміння предмета дослідження відповідає основним положенням функціонального підходу, запропонованого Р. Мертоном, а саме:

ронні функції держави Україна / П. В. Онопенко. — К. : Варта, 2003. — 128 с.

<sup>38</sup> Сагатовский В. Н. Системная деятельность и ее философское осмысление / В. Н. Сагатовский // Системные исследования. Методологические проблемы. Ежегодник, 1980. — М., 1981. — С. 52–68; Батишев С. С. Деятельность и ценности. Критика деятельностного подхода к теории интериоризации / С. С. Батишев // Вопросы философии. — 1985. — № 2. — С. 41–44; Берман Г. Дж. Западная традиция права: эпоха формирования / Г. Дж. Берман; [пер. с англ.]. — [2-е изд.]. — М. : МГУ ; ИНФРА.М-НОРМА, 1998. — 624 с.; Казимирчук В. П. Право и методы его изучения / В. П. Казимирчук. — М. : Юрид. лит., 1965. — 204 с.; Дмитренко В. А. О методологическом значении деятельностного подхода к науке / В. А. Дмитренко // Вопросы методологии наук. — М., 1975. — Вып. 5. — С. 3–20.

<sup>39</sup> Кудрявцев В. Н. Правовое поведение: его субъекты и пределы / В. Н. Кудрявцев, Н. С. Маленин // Изв. вузов. Правоведение. — 1980. — № 3. — С. 31–40; Нурпеисов Е. К. Психология правомерного поведения / Е. К. Нурпеисов. — Алма-Ата : «Наука» Казахской ССР, 1984. — 127 с.; Щербакова Н. В. Социально-психологические основы правомерного поведения личности в СССР : [учеб. пособие] / Н. В. Щербакова. — Ярославль : ЯрГУ, 1984. — 80 с.; Тихомиров А. Д. Профессиональное поведение работников органов внутренних дел: социально-правовой анализ : дисс. ... канд. юрид. наук : 12.00.01 / Александр Деонисович Тихомиров ; Ин-т государства и права им. В. М. Корецкого. — К., 1990. — 270 с.; Ломов Б. Ф. Методологические и теоретические проблемы психологии / Б. Ф. Ломов. — М. : Наука, 1984. — 445 с.; Каган М. С. Человеческая деятельность (Опыт системного анализа) / М. С. Каган. — М. : Политиздат, 1974. — 328 с.; Николов Л. Структуры человеческой деятельности / Л. Николов. — М. : Прогресс, 1984. — 176 с.; Гусарев С. Д. Юридична діяльність: методологічні та теоретичні аспекти / С. Д. Гусарев. — К. : Знання, 2005. — 375 с.



функціональної єдності цілого (узгодженого функціонування всіх його частин); універсального функціоналізму (функціональність притаманна всім соціальним явищам і відбиває їх корисність); функціональної необхідності (будь-яке явище існує, коли функціонує, взаємодіє).

Використання функціонального та діяльнісного підходів надало можливість проаналізувати наукові позиції вчених стосовно розуміння функцій держави та права, розкрити особливості окремих форматів їх розуміння, розробити й обґрунтувати авторську інтерпретацію завдань адміністративно-правового режиму інформації з обмеженим доступом тощо

Поряд з діяльнісним та функціональним, третім фундаментальним методологічним підходом дослідження є системний підхід, який дає змогу розглянути предмет дослідження і як певну систему, і як елемент (підсистему) інших систем (інформації).

Органічне поєднання діяльнісного та системного підходів застосовано у численних юридичних наукових працях. Так, у своїх роботах Н. М. Онищенко на підставі широкого кола праць зарубіжних та вітчизняних вчених — системників, філософів, соціологів, політологів, юристів — проаналізувала основні правила та прийоми системного підходу та відповідним чином трансформувала їх стосовно особливостей правової реальності. Внаслідок чого було визначено сутність, структуру, функції правової діяльності як елемента правової системи, форми її функціонування, зокрема надано системоутворювальне значення у зв'язку з залежністю від неї генези, стану та перспектив розвитку правової системи <sup>40</sup>.

При використанні методології системного підходу досліджувалися статичні, динамічні, структурні компоненти та властивості адміністративно-правового режиму інформації з обмеженим доступом, його внутрішні та зовнішні прояви, генетичні та функціональні зв'язки, взаємодія з соціальним і інформаційним середовищем.

<sup>40</sup> Онищенко Н. М. *Правова система: проблеми теорії* : [монографія] / Н. М. Онищенко. — К. : Ін-т держави і права ім. В. М. Корецького НАН України, 2002. — 352 с.; Онищенко Н. М. *Розвиток соціальності сучасних державних і правових систем* / Н. М. Онищенко // *Держава і право* : зб. наук. пр. Юридичні і політичні науки. — К., 2001. — Вип. 14. — С. 3–11; Ліпкан В. А. *Системний підхід до побудови еталонної моделі системи забезпечення національної безпеки* / В. А. Ліпкан // *Науковий вісник Національної академії внутрішніх справ України*. — К., 2002. — № 2. — С. 19–24; Ліпкан В. А. *Міждисциплінарний підхід до формування національної безпеки* / В. А. Ліпкан // *Право України*. — 2005. — № 1. — С. 94–99; Ліпкан В. А. *Синергетичний і гомеостатичний підходи до системи національної безпеки* / В. А. Ліпкан // *Науковий вісник Національної академії внутрішніх справ України*. — К., 2003. — № 2. — С. 104–111.

До загально визнаних методологічних положень системного підходу у застосуванні до проблематики дослідження належать такі:

- державно-правові явища й окремі їх компоненти, що, своєю чергою, розглядаються як системи (підсистеми); повинні мати цілісний характер, що зумовлює їх виокремленість із зовнішнього середовища;
- елементи системи, взаємопов'язані між собою так само, як і кожне явище з множиною інших явищ (систем), причому властивості елементів (підсистем) залежні від властивостей цілого, частиною якого вони є, тому забезпечення адміністративно-правового режиму інформації з обмеженим доступом усвідомлюється залежно від особливостей його взаємодій з іншими складовими певних системних утворень, як залежне від своєрідності природи тієї чи іншої системи, що завдає як певний ракурс його вивчення, так й відповідні властивості;
- кожне державно-правове явище в контексті забезпечення адміністративно-правового режиму інформації з обмеженим доступом має динамічну природу, тобто йому властиві процеси виникнення, становлення, розвитку, зміни та припинення існування;
- функціонування та розвиток цих явищ здійснюється в результаті взаємодії з зовнішнім середовищем при домінуванні внутрішніх закономірностей (його саморозвитку) над зовнішніми чинниками та закономірностями.

Наступною складовою методики осмислення адміністративно-правового режиму інформації з обмеженим доступом є методи вивчення предмета дослідження як сукупність принципів, правил, прийомів, способів і засобів пізнання інформації з обмеженим доступом та формування теоретичного наукового знання<sup>41</sup>.

Методологічна основа будь-якого дослідження загалом і даного зокрема складається із сукупності наукових методів, які за умови їх комплексного використання, вирішують поставлені завдання.

<sup>41</sup> Бигич О. Л. Місце порівняльного методу в правовій методології / О. Л. Бигич // Правова держава : щорічник наук. праць / Ін-т держави і права ім. В. М. Корецького НАН України. — К., 2002. — Вип. 13. — С. 448–454; Луць Л. А. Методологія порівняльного правознавства / Л. А. Луць // Проблеми державотворення і захисту прав людини в Україні : матеріали III регіон. наук. конф. — Львів, 1997. — С. 29–34.



При дослідженні адміністративно-правового режиму інформації з обмеженим доступом було використано такі методи.

1. **Загальні методи пізнання** — порівняння, аналізу, синтезу, абстрагування, узагальнення, моделювання тощо. Зокрема порівняння використовувалося для з'ясування загального та специфічного в нормативно-правовому регулюванні інформації з обмеженим доступом в міжнародних документах, НПА інших країн, співставлення різних позицій вчених щодо розуміння специфіки адміністративно-правового режиму інформації з обмеженим доступом чи окремих його елементів, аналіз та синтез як взаємопов'язані методи спрямовувалися на вивчення властивостей інформації з обмеженим доступом тощо, узагальнення та моделювання — для виокремлення необхідних і достатніх властивостей тих державно-правових явищ, що досліджувалися у зв'язку із осмисленням забезпечення інформації з обмеженим доступом та їх логічного формулювання у наведених в монографії визначеннях, конструювання їх теоретичних моделей, наприклад, конфіденційна інформація, таємна інформація, інформація з обмеженим доступом і таке інше.
2. **Філософські методи** — такі, що розроблені в певних філософських системах наукових знань (*феноменологічний, діалектичний, герменевтичний, аксіологічний, гуманістичний* тощо). Так, діалектичний метод надав можливість розглянути забезпечення інформації з обмеженим доступом як процес, основою якого є взаємодія, взаємозумовленість, взаємовплив різних суб'єктів, форм і методів та інших складових, що розгортаються у часі та в різних площинах, тоді як використання аксіологічного методу спрямовувалося на з'ясування і визначення суспільної небезпечності загроз у сфері інформації з обмеженим доступом та суспільну корисність державної діяльності щодо їх подолання. Герменевтичний — на залежність тлумачення нормативно-правових актів чи положень, що викладені у наукових текстах від суб'єкта тлумачення, розкриття змісту норм права та наукових знань виходячи з особливостей юридичної нормативно-правової та наукової мови, а гуманістичний — на розгляд інформаційного простору, інформаційної безпеки, державної діяльності як таких, що мають людську природу, тобто створені, діють і при-

значені для забезпечення потреб суспільства і людини, а також на взаємозумовленість захисту інформації з обмеженим доступом і природних прав людини.

3. **Загальнонаукові методи**, які використовуються всіма науками (*структурний, синергетичний, історичний тощо*). Так, структурний спрямовувався на визначання складових адміністративно-правового режиму інформації з обмеженим доступом та зв'язків між ними («горизонтальними» та «вертикальними»), синергетичний — для визначення саморганізаційної природи інформаційних процесів та самозабезпечення інформації з обмеженим доступом. Слід нагадати, що **першим в Україні, хто застосував і методологічно обґрунтував застосування синергетики до права у сфері безпеки був В. А. Ліпкан**. Адже нині чимало дослідників-компіляторів, переписуючи один в одного, просто забувають звернутися до першоджерела, в якому була викладена синергетична парадигма безпекознавства, детально розписано та науково обґрунтовано застосування синергетики до формування правових систем<sup>42</sup>. Саме роботи В. А. Ліпкана, його активна наукова та життєва позиція, наукова пропаганда синергетики сприяли усвідомленню молодим поколінням науковців її можливостей, необхідності поглиблювати власний методологічний інструментарій, не занурюючись лише в площину системного або діалектичного методів. Історичний метод використовувався при визначенні генези (процесів та умов виникнення, становлення, розвитку та припинення існування) забезпечення інформації з обмеженим доступом, так і власно адміністративно-правового режиму тощо.
4. **Частково-наукові методи**, які мають певні обмеження, а тому застосовуються окремими групами наук та для дослідження певних предметів і їх властивостей (*статистичні, математичні, конкретно-соціологічні, психологічні та інші*) були використані

<sup>42</sup> Ліпкан В. А. Теоретичні основи та елементи національної безпеки України: [монографія] / В. А. Ліпкан — К.: Текст, 2003. — 600 с.; Ліпкан В. А. Безпекознавство: [навч. посіб.] / В. А. Ліпкан. — К.: Європ. ун-т, 2003. — 208 с.; Ліпкан В. А. Синергетичний і гомеостатичний підходи до системи національної безпеки / В. А. Ліпкан // Науковий вісник Національної академії внутрішніх справ України. — К., 2003. — № 2. — С. 104–111; Ліпкан В. А. Основи терорології (синергетична теорія тероризму) / В. А. Ліпкан. — К.: КНТ, 2006. — 84 с. — (Серія: Національна і міжнародна безпека).

для виокремлення і усвідомлення психологічних особливостей забезпечення інформації з обмеженим доступом, статистичні — для аналізу реального стану інформаційних загроз та діяльності щодо їх подолання, конкретно-соціологічні — з'ясування особливостей окремих характеристик суспільної думки щодо забезпеченості інформації з обмеженим доступом.

5. *Спеціальні методи*, які притаманні окремим наукам або дослідженням, зокрема у нашому випадку — це: *формально-юридичний метод*, який використовувався для визначення особливостей нормативно-правового регулювання суспільних відносин у сфері інформації з обмеженим доступом, *порівняльний*: порівняльно-історичний, порівняльно-структурний, порівняльно-функціональний, порівняльно-аксіологічний, порівняльно-типологічний, порівняльно-лінгвістичний, порівняльно-семіотичний, порівняльно-правовий, порівняльно-філософський, порівняльно-політичний для вивчення загального й особливого та унікального між декількома державними і правовими явищами.

Розкриття питання методологічних засад дослідження адміністративно-правового режиму інформації з обмеженим доступом дає змогу дійти таких висновків:

- 1) адміністративно-правовий режим інформації з обмеженим доступом — це складний та багатоаспектний правовий феномен;
- 2) при дослідженні слід ураховувати його зв'язки з іншими правовими феноменами та, загалом, із соціально-економічним, політико-правовим, культурним розвитком країни тощо;
- 3) лише комплексне використання методологічних підходів і методів дослідження сприятимуть об'єктивному, всебічному розкриттю предмета дослідження.

Таким чином, для забезпечення комплексності, обґрунтованості та достовірності наукових результатів дослідження адміністративно-правового режиму інформації з обмеженим доступом визначені світоглядні, філософські, наукові та теоретичні засади, використані різні загальні методи пізнання, загальнонаукові, конкретно-наукові та спеціальні методи, вибір і характер застосування яких зумовлено особливостями предмета, мети та завдань дослідження, а також які забезпечують цілісне сприйняття захисту інформації з обмеженим доступом у контексті її зумовленості реальним станом суспільного, державного та правового життя.

### 1.3 ПОНЯТІЙНО-КАТЕГОРІЙНИЙ АПАРАТ ДОСЛІДЖЕННЯ

У демократичній державі інститут інформації з обмеженим доступом є особливо важливим та складним з багатьох причин. Однією із ознак демократичності є транспарентність діяльності органів державної влади, відкритість та доступність інформації. Втім, держава зобов'язана забезпечити безпеку особистості, суспільства та національні інтереси. Як слушно зауважив А. А. Фат'янов, держава зобов'язана взяти на себе формування продуманого механізму захисту різних видів інформації і встановлення рамок дії інститутів таємниць. З одного боку, ці вимоги виходять із потреби сучасного суспільства бути більш відкритим і доступним, з іншого — диктуються необхідністю гарантування безпеки особистості, суспільства і держави [37, с. 5–6].

Захист інформації з обмеженим доступом досліджується і юридичними, і неюридичними науками. Багатоаспектність цього феномена обумовлює його розгляд з багатьох ракурсів — загальнотеоретичного, історичного, управлінського, філософського, економічного, технічного, політологічного, геополітичного, цивільно-правового, кримінально-правового тощо. Розмаїття визначень поняття «інформація з обмеженим доступом» є об'єктивно обумовлене, оскільки кожна з цих наук використовує власний методологічний інструментарій, висвітлює лише той аспект, що відповідає специфіці предмета даної науки, а також залежить від суб'єктивних поглядів дослідників. Плюралізм тлумачення цього явища як неюридичної категорії надає можливість скласти більш об'єктивне уявлення про нього. Наявність полісемії чи синонімії юридичних категорій негативно впливає на ефективність правового регулювання будь-яких соціальних відносин, оскільки винятково однозначне безальтернативне розуміння норми права як правила поведінки можливо реалізувати без порушень.

В «інформаційній складовій» сучасного права України останнім часом доволі широко вживаються визначення і терміни, поява яких зумовлена стрімкими темпами науково-технічного розвитку, впливом процесу інформатизації та інформаційних технологій на соціальну діяльність, становленням інформаційних відносин і, нарешті, формуванням міжгалузевих наукових знань [38, с. 69]. Використання законодавцем у нормативно-правових актах понять, запозичених з «технічних» галузевих наук

без визначення їх дефініцій детермінують різне розуміння і трактування змісту потенційними реалізаторами та, як наслідок, вчиненню правопорушень. Така тенденція властива і для законодавства, що регулює суспільні відносини у сфері захисту інформації з обмеженим доступом.

### **Поняття «інформація з обмеженим доступом» у нормативно-правових актах**

Поняття «інформація з обмеженим доступом» та інші суміжні поняття («державна таємниця», «конфіденційна інформація», «таємна інформація» тощо) стали важливими дефініціями, що використовуються в значній кількості нормативно-правових актів.

Аналіз цієї сфери вітчизняного законодавства надав можливість дійти висновку про відсутність законодавчого закріплення поняття «інформація з обмеженим доступом».

У Законі України «Про інформацію» лише зазначено, що в Україні весь масив інформації за режимом доступу класифікується на два види: відкрита інформація та інформація з обмеженим доступом, остання з яких поділяється на конфіденційну, таємну та службову [39].

У Законі України «Про державну таємницю» також бракує дефініції інформації з обмеженим доступом як більш широкої, родової категорії щодо державної таємниці. Хоча **державна таємниця** визначається у ст. 1 цього акта як вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [40].

На відміну від внутрішньодержавних нормативно-правових актів України, де відсутнє визначення поняття «інформація з обмеженим доступом», в окремих міжнародних угодах, учасницею яких є Україна, дане визначення закріплено. Зокрема у ст. 1 Угоди між Кабінетом Міністрів України та Урядом Республіки Білорусь про співробітництво в галузі технічного захисту інформації, а також у ст. 1 Угоди між Кабінетом Міністрів України та Урядом Республіки Таджикистан про співробітництво в галузі технічного захисту інформації визначено, що «інформація з обмеженим доступом — інформація, право доступу до якої обмежено відповідно до національних законодавств держав Сторін» [41; 42].

Цікаво, що однією із перших подібних угод була Угода між урядом України та урядом Російської Федерації, де взагалі будь-яка дефініція інформації з обмеженим доступом відсутня. Натомість ця Угода містить визначення конфіденційної інформації як інформації, на поширення якої згідно з законодавством держав Сторін накладаються обмеження і для захисту якої вживаються належні заходи з огляду на її цінність і невідомість третім особам [43].

Вважаємо, що таке застереження має достатнє важливе значення для розуміння інформації з обмеженим доступом, оскільки на відміну від загальнодоступної інформації, вона є цінною лише через «обмежене» коло користувачів та доступ, регламентований спеціальними правилами. Водночас аналіз даного положення дозволяє дійти висновку про відсутність розмежування понять «інформація з обмеженим доступом» та «конфіденційна інформація», а також співвідношення їх між собою, що суперечить нормам Закону України «Про інформацію», ст. 21 якого закріплює, що інформація з обмеженим доступом поділяється за своїм правовим режимом на конфіденційну, таємну та службову [39]

Крім вищезазначених угод, є чимала кількість міжнародних документів, що встановлюють правила обігу інформації з обмеженим доступом між Україною та іншими державами, обмін якою здійснюється між ними чи між державними органами та приватними установами під їх юрисдикцією, або спільно створеними ними. Слід зауважити, що назва такої інформації також є неусталеною: в одних угодах зазначається про взаємну охорону «інформації з обмеженим доступом», в других — про взаємну охорону «секретної інформації», в третіх — про взаємну охорону «таємної інформації». Аналіз змісту норм вищезазначених документів дозволяє дійти висновку, що, незважаючи на різну назву, йдеться саме про встановлення міжнародного співробітництва України та іншої держави у сфері інформації з обмеженим доступом як більш широкої категорії.

На 2010 рік Україна підписала угоди, що закріплюють правила обігу інформації з обмеженим доступом, з Йорданським Хашимітським Королівством, Румунією, Македонією, Словенією, Угорською Республікою, Алжирською Народною Демократичною Республікою, Словацькою Республікою, Литовською Республікою тощо.

На 2012 рік Україна має такі угоди ще зі значним колом країн, а саме: Грецькою Республікою, Республікою Польща, Республікою Кіпр,



Естонською Республікою, Португальською Республікою, Демократичною Соціалістичною Республікою Шрі-Ланка, Великою Соціалістичною Народною Лівійською Арабською Джамагірією тощо.

Так, першою такою угодою була Угода між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом від 5 червня 2003 року, де інформація з обмеженим доступом визначається як інформація та матеріали незалежно від їх форми, природи та способу передачі, яким встановлені певні ступені обмеження доступу та надані відповідні грифи обмеження доступу, і які в інтересах національної безпеки та згідно з національним законодавством Сторін підлягають охороні від несанкціонованого доступу [44].

В Угоді між Кабінетом Міністрів України та Урядом Словацької Республіки про взаємну охорону інформації з обмеженим доступом закріплено інше визначення: «інформація з обмеженим доступом» — інформація у будь-якій формі та будь-які документи, матеріали, вироби, речовини або фізичні поля, на/в яких представлена інформація, яка в інтересах національної безпеки держав Сторін та відповідно до їх національного законодавства підлягає охороні від несанкціонованого доступу, включаючи інформацію, яку спільно створено юридичними особами держав Сторін в рамках співробітництва та доступ до якої обмежено на основі вимог національного законодавства держав Сторін та відповідно до критеріїв цієї Угоди [45].

Угода між Україною та Угорською Республікою про взаємну охорону інформації з обмеженим доступом також містить визначення поняття «інформація з обмеженим доступом», згідно з яким це будь-які дані незалежно від їхньої форми представлення, виду та умов відтворення, що потребують охорони від несанкціонованого доступу та доступ до яких обмежено будь-якою з Договірних сторін відповідно до свого національного законодавства [46].

Більш стисле визначення інформації з обмеженим доступом містить Угода між Україною та Республікою Словенія про обмін та взаємну охорону інформації з обмеженим доступом: інформація, яка за законодавством кожної Договірної сторони потребує охорони від розголошення, незаконного заволодіння чи втрати, та визначена такою незалежно від її форми [47].

Інший підхід до визначення цього поняття використаний в Угоді між Кабінетом Міністрів України та Урядом Алжирської Народної

Демократичної Республіки про охорону інформації з обмеженим доступом, де закріплено, що інформація з обмеженим доступом означає будь-який документ, рисунок, план, карту, фотографію, звукову чи відеоплівку або інший документ чи інший носій інформації, що містять інформацію, якою обмінюються Сторони в рамках їхньої діяльності, і розголошення якої може завдати шкоди відповідним інтересам та/або безпеці однієї з двох держав [48].

В одній із останніх угод — Угоді між Кабінетом Міністрів України та Урядом Республіки Македонія про взаємну охорону інформації з обмеженим доступом закріплено, що інформація з обмеженим доступом — це інформація, відображена в будь-якій формі, що охороняється відповідно до національного законодавства Договірних сторін та передана в порядку, встановленому кожною з Договірних сторін і цією Угодою, розголошення якої може завдати шкоди безпеці та інтересам держав Договірних сторін [49].

В Угоді між Кабінетом Міністрів України та Урядом Йорданського Хашимітського Королівства про взаємну охорону інформації з обмеженим доступом від 14 березня 2011 року інформація з обмеженим доступом визначається як будь-яка інформація незалежно від її фізичної форми, носія та способу запису, якій згідно з національним законодавством надано відповідний ступінь обмеження доступу та яка охороняється відповідним чином [50].

Серед останніх таких угод є Угода між Кабінетом Міністрів України та Урядом Грецької Республіки про взаємну охорону секретної інформації у сфері оборони, що ратифіковано Законом України від 16 жовтня 2012 року, де визначається «секретна інформація у сфері оборони» (секретна інформація) означає будь-яку секретну одиницю, будь-то усне або письмове повідомлення секретного змісту, або електричну чи електронну (технічну) передачу секретного повідомлення, або секретний матеріал, які стосуються військової або військово-технічної галузей. «Матеріал» означає будь-яку одиницю механізму або обладнання, або озброєння, виготовлену чи таку, що знаходиться в процесі виготовлення, або документ. «Документ» означає будь-який лист, запис, протокол, звіт, меморандум, сигнал (повідомлення), ескіз, фотографію, плівку, карту, схему, план, записник, шаблон, копіювальний папір, машинку, що пише, стрічку, дискету тощо або іншу форму запи-



саної інформації (наприклад, запис на плівку, магнітний запис, перфокарта, перфострічка тощо)»<sup>43</sup>.

Ураховуючи вищезазначені визначення інформації з обмеженим доступом (інформація та матеріали незалежно від їх форми, природи та способу передачі; інформація у будь-якій формі та будь-які документи, матеріали, вироби, речовини або фізичні поля, на/в яких представлена інформація; будь-який документ, рисунок, план, карта, фотографія, звукова чи відеоплівка або інший документ чи інший носій інформації, що містять інформацію; інформація, відображена в будь-якій формі), можна дійти висновку, що здебільшого в міжнародних документах акцентується увага на певних матеріальних носіях, де може міститися інформація, а не на визначенні сутності такої інформації.

Отже, відповідно до цих міжнародних угод можна виділити *широке та вузьке розуміння інформації з обмеженим доступом*. Відповідно до *вузького розуміння* — інформацію з обмеженим доступом складають «будь-який документ, рисунок, план, карта, фотографія, звукова чи відеоплівка або інший документ чи інший носій інформації, що містять інформацію», тобто інформацією з обмеженим доступом є лише та інформація, що перебуває на певних матеріальних носіях. Саме вузьке трактування інформації з обмеженим доступом закріплене і у вітчизняному законодавстві, зокрема у ст. 1 Закону України «Про інформацію» інформація визначається як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [39]. Згідно з *широким розумінням* таку інформацію складає інформація незалежно від «форми, природи, способу передачі» чи «виду і умов відтворення».

Вважаємо, що саме широке трактування відповідає сучасним реаліям, оскільки специфіка інформації як феномена полягає в тому, що вона має певну автономність від матеріального носія.

Беручи до уваги положення згаданих вище угод, основною загрозою інформації з обмеженим доступом є «несанкціонований доступ» та, як наслідок, «розголошення». Водночас виникає питання: чи буде порушенням законодавства ушкоджена цілісність інформації (спотворення, руйнування, знищення тощо) чи унеможливлення санкціонова-

<sup>43</sup> Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Грецької Республіки про взаємну охорону секретної інформації у сфері оборони [Електронний ресурс] : Закон України від 16 жовт. 2012 р. — Режим доступу : <http://zakon1.rada.gov.ua>.

ного доступу до неї? Вважаємо, що так, але такі загрози містить лише Угода між Україною та Республікою Словенія про обмін та взаємну охорону інформації з обмеженим доступом, де зазначено, що інформація з обмеженим доступом «потребує охорони від розголошення, незаконного заволодіння чи втрати» (Підкреслено нами. — Авт.).

Дані міжнародні угоди містять норму, що інформація з обмеженим доступом є такою внаслідок надання інформації відповідно до національного законодавства певних ступенів обмеження доступу та наявності грифів обмеження доступу. Перелік же такої інформації для кожної держави власний та залежить від багатьох об'єктивних і суб'єктивних факторів.

Є застереження, що охорона такої інформації здійснюється «в інтересах національної безпеки», оскільки може завдати «шкоди безпеці та інтересам держав Договірних сторін». Хоча перелік інтересів та розуміння національної безпеки для кожної країни є також власним. Більш того, основоположний нормативно-правовий акт, що визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності, — Закон України «Про основи національної безпеки України» — не містить конструкції «інтереси національної безпеки», натомість законодавець у цьому акті оперує такими поняттями як «національні інтереси», «пріоритети національних інтересів», «життєво важливі інтереси» тощо [51].

Ураховуючи положення згаданих вище угод, можемо виділити *характерні риси нормативного розуміння інформації з обмеженим доступом*.

1. Це будь-яка інформація незалежно від форми, природи та способу передачі; інформація у будь-якій формі та будь-які документи, матеріали, вироби, речовини або фізичні поля, на/в яких представлена інформація; будь-які дані незалежно від форми представлення, виду та умов відтворення; будь-який документ, рисунок, план, карта, фотографія, звукова чи відеоплівка або інший документ чи інший носій інформації, що містять інформацію; інформація, відображена в будь-якій формі.
2. Охорона такої інформації здійснюється з метою забезпечення національної безпеки, інтересів кожної з країн.
3. Основною загрозою такій інформації є несанкціонований доступ, що призводить до її розголошення.

4. Зміст і перелік такої інформації, а також ступені та грифи обмеження доступу визначаються кожною країною самостійно відповідно до національного законодавства.

Правовий режим інформації з обмеженим доступом покликаний охороняти відомості, вільний обіг яких може порушити права та інтереси держави, суспільства й окремої особи, забезпечити інформаційну незалежність суб'єктів приватного права у відносинах із державою і між собою, узгодити публічну потребу у свободі інформації та право кожного на збереження таємниці [35, с. 3–4].

Саме тому характерною рисою для більшості розвинених країн є наявність відповідних законодавчих актів, що встановлюють принципи, критерії, механізми класифікації інформації з обмеженим доступом, а також процедуру її охорони з боку держави чи власника.

Як ми зауважували раніше, нині в Україні відсутній такий нормативно-правовий акт, який закріплював би правові засади захисту інформації з обмеженим доступом. Лише суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України, урегульовані на рівні окремого законодавчого акта — Закону України «Про державну таємницю», а також суспільні відносини, пов'язані з захистом персональних даних, нормативно урегульовані Законом України «Про захист персональних даних».

Слід зауважити, що така тенденція властива більшості пострадянських країн. Поряд з державною таємницею законодавством цих країн закріплено правові засади захисту інших видів інформації з обмеженим доступом: комерційна таємниця, службова таємниця, банківська таємниця, таємниця персональних даних.

У цьому ракурсі варто відмітити закони Азербайджану «Про державну таємницю», «Про інформацію, інформатизацію і захист інформації», «Про комерційну таємницю», закони Вірменії «Про державну та службову таємницю», «Про банківську таємницю», закон Білорусі «Про державні секрети», закон Грузії «Про державну таємницю», закон Казахстану «Про державні секрети», закони Киргизії «Про захист державних секретів Киргизької Республіки», «Про комерційну таємницю», «Про гарантії і свободу доступу до інформації», «Про доступ до інформації, що знаходиться в віданні державних органів і органів місцевого самоуправління Киргизької Республіки», закони Латвії «Про державну таємницю», «Про

захист персональних даних», «Про свободу інформації», закони Литви «Про державну і службову таємницю», «Про правовий захист особистих даних», «Про суспільну інформацію», «Про право на отримання інформації від державних установ і установ самоуправління», закони Молдови «Про державну таємницю», «Про комерційну таємницю», «Про доступ до інформації», закони Таджикистану «Про державну таємницю», «Про захист інформації», «Про перелік відомостей, що становлять державну таємницю», закони Туркменістану «Про захист державних секретів», «Про комерційну таємницю», закони Узбекистану «Про захист державних секретів», «Про гарантії і свободу доступу до інформації», «Про принципи і гарантії свободи інформації».

### ***Поняття «інформація з обмеженим доступом» в доктринальних джерелах***

Інформація загалом та інформація з обмеженим доступом є новим предметом дослідження юридичних наук. Внаслідок чого визначення цього поняття чи виокремлення його характерних ознак не знайшло адекватного розгляду в доктринальних дослідженнях.

Слід зауважити, що воно відсутнє навіть у спеціалізованих роботах, предметом яких є безпосередньо інформація з обмеженим доступом.

Зокрема, доктринальну дефініцію інформації з обмеженим доступом ми знаходимо лише в декількох роботах.

Так, О. О. Кулініч у своєму цивільно-правовому дослідженні пише: «...інформація з обмеженим доступом як доступні певному колу осіб відомості, дані і знання, що мають особливу цінність для осіб, у володінні яких знаходяться, та щодо яких уживаються заходи, спрямовані на обмеження вільного доступу третіх осіб, поширення яких може заподіяти істотну шкоду зацікавленим особам (власникам чи добросовісним користувачам)» [35, с. 74].

Таке визначення викликає ряд заперечень. По-перше, авторка зауважує, що інформацію з обмеженим доступом складають лише ті «відомості, дані і знання, які доступні певному колу осіб». (Підкреслено нами. — Авт.) Та чи не буде, наприклад, комерційною таємницею винахід, автором якого є одна особа? Тому більш доречним є визначення: через коло осіб чи одну особу. По-друге, у визначенні зазначено, що цими особами вживаються заходи з метою обмеження доступу третіх

осіб. На нашу ж думку, слід зауважити, що ці заходи мають бути винятково правовими, тобто відповідати чинному законодавству. По-третє, дослідниця вказує, що основною загрозою такій інформації є її поширення. Тобто, якщо трапиться її повне чи часткове знищення внаслідок несанкціонованого доступу без поширення, то це не завдає шкоди власникам чи добросовісним користувачам? Останнє, з чим ми не погоджуємось, це наявність у визначенні нечітких категорій, які можуть слугувати для зловживання інтерпретатора залежно від його суб'єктивізму, наприклад — «істотна шкода». Які критерії визначення шкоди як істотної чи неістотної?

З метою доведення тези про те, що інформація з обмеженим доступом має самостійне правове значення і наділена властивостями, що істотно відрізняють її від інших видів інформації, О. О. Кулініч окреслює і ознаки інформації з обмеженим доступом:

- 1) зміст інформації з обмеженим доступом складають знання, повідомлення, відомості про соціальну форму руху матерії і про всі інші її форми тією ж мірою, якою вони використовуються суспільством, особою;
- 2) відомості, що складають зміст інформації з обмеженим доступом, сутнісно ідеальні (нематеріальні);
- 3) інформація з обмеженим доступом існує винятково в рамках взаємодії суб'єктів суспільних відносин: окремих індивідуумів, їх груп, а також таких соціальних утворень, як держава, муніципальні утворення і юридичні особи;
- 4) інформація з обмеженим доступом не пов'язана нерозривно з матеріальним носієм. Вона є самостійним об'єктом правового регулювання, що не залежить від конкретної форми її матеріального носія;
- 5) інформація з обмеженим доступом має кількісні і якісні характеристики. Співвідношення кількісних і якісних властивостей інформації має нелінійний характер (якість інформації з обмеженим доступом не залежить від її кількості);
- 6) інформація з обмеженим доступом не є загальнодоступною;
- 7) інформація з обмеженим доступом відома і використовується чітко визначеним колом осіб;
- 8) суб'єкт інформації вживає заходів, що спрямовані на обмеження вільного доступу третіх осіб до інформації;

- 9) інформація з обмеженим доступом має особливу соціальну цінність у силу її дійсної або потенційної невідомості третім особам. Поширення такої інформації може спричинити заподіяння істотної шкоди зацікавленим особам;
- 10) зміст інформації з обмеженим доступом відповідає обмеженням, установленим законодавством [35, с. 72–73].

У цілому підтримуючи виокремлені ознаки інформації з обмеженим доступом О. О. Кулініч, які доводять тезу про її самостійне правове значення і наділена властивостями, що істотно відрізняють її від інших видів інформації, вважаємо, що ряд ознак потребують уточнення.

По-перше, інформацією, до якої може буде застосований обмежений режим доступу, є така, що не суперечить чинному законодавству України. Кожна країна має власний перелік інформації, до якої не може бути застосований обмежений режим доступу в силу її соціальної цінності. У п. 4 ст. 21 Закону України «Про інформацію» до інформації з обмеженим доступом не можуть бути віднесені такі відомості:

- 1) про стан довкілля, якість харчових продуктів і предметів побуту;
- 2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;
- 3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;
- 4) про факти порушення прав і свобод людини і громадянина;
- 5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;
- 6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України [39].

По-друге, крім власника цієї інформації, доступ до такої інформації мають лише ті, хто, не порушуючи норм чинного законодавства, отримав дозвіл від власника на доступ до такої інформації, тобто є добросовісним користувачем.

По-третє, інформація з обмеженим доступом має особливу цінність для вищезазначеної категорії суб'єктів (моральну, матеріальну, особисту тощо) в силу невідомості її іншим, стороннім суб'єктам.



По-четверте, власники та добросовісні користувачі інформації з обмеженим доступом мають здійснювати певні адекватні заходи з метою унеможливлення доступу сторонніх осіб. При чому ці заходи також мають ґрунтуватися на правових приписах, тобто бути законними.

По-п'яте, порушення заходів, що спрямовані на обмеження вільного доступу третіх осіб до інформації, які вживаються суб'єктом такої інформації (власником чи добросовісним користувачем), тягне за собою юридичну відповідальність (цивільно-правову, кримінальну, адміністративну тощо). У разі відсутності юридичної відповідальності неможливо говорити про порушення режиму доступу.

Екстраполюючи цивільно-правове дослідження О. О. Кулініч на предмет дослідження, а також беручи до уваги зазначені нами вище коментарі, *конститутивними ознаками інформації з обмеженим доступом у адміністративно-правовому контексті є:*

- 1) інформація з обмеженим доступом — це, насамперед, відомості, дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;
- 2) інформацією, до якої може буде застосований обмежений режим доступу, є така, що не суперечить чинному законодавству України;
- 3) певне коло користувачів отримують доступ до неї винятково на законних підставах (добросовісні користувачі);
- 4) інформація з обмеженим доступом має особливу цінність для вищезазначеної категорії суб'єктів (моральну, матеріальну, особисту тощо) в силу невідомості її іншим суб'єктам;
- 5) власники та добросовісні користувачі інформації з обмеженим доступом здійснюють адекватні законні заходи з метою унеможливлення доступу сторонніх суб'єктів;
- 6) за порушення вищезазначених заходів встановлена юридична відповідальність [52, с. 264].

Ураховуючи положення чинного законодавства України, які закріплюють правові підстави та процедури обмеження доступу до інформації певних категорій, інформацію з обмеженим доступом А. І. Марущак визначає як відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України, які визнані такими відповідно до встановлених юридичних процедур і доступ до яких обмежений власником таких відомостей [19, с. 19].

В іншій своїй роботі А. І. Марущак децю інакше визначив поняття «інформація з обмеженим доступом», а саме: відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України, які визнані такими відповідно до встановлених юридичних процедур і право на обмеження доступу до яких надає власнику таких відомостей [24, с. 23]. (Підкреслено нами. — Авт.).

Зважаючи на прийняття Закону України «Про доступ до публічної інформації» та внесення змін до Закону України «Про інформацію» дані визначення втратили актуальність, оскільки відповідно до чинного законодавства інформація з обмеженим доступом поділяється на конфіденційну, службову та таємну.

У ст. 1 Закону України «Про інформацію» є визначення поняття інформації як будь-яких відомостей та/або даних, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [39] та у ст. 20 міститься визначення конфіденційної інформації як «інформації про фізичну особу, а також інформації, доступ до якої обмежено фізичною або юридичною особою» [39], які співвідносяться з поняттям інформація з обмеженим доступом як загальне та часткове.

Ураховуючи проаналізовані вище нормативні та доктринальні дефініції інформації з обмеженим доступом, а також її характерні риси, пропонуємо авторську позицію розуміння інформації з обмеженим доступом: **будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, доступ до яких обмежено відповідно до законодавства України її власником чи добросовісним користувачем (суб'єктом владних повноважень, фізичною або юридичною особою) у зв'язку з її особливою цінністю для них на законних підставах** [53, с. 126].

Поряд зі жвавою науковою дискусією навколо поняття «інформація з обмеженим доступом», не менш неоднозначним в адміністративній доктрині є визначення видів такої інформації. Саме тому наступний підрозділ буде присвячений класифікації інформації з обмеженим доступом.



# **КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ**

---

---

- 2.1 КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ  
У ВІТЧИЗНЯНОМУ ЗАКОНОДАВСТВІ
  
- 2.2 КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ  
В ДОКТРИНАЛЬНИХ ДЖЕРЕЛАХ





## 2.1 КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У ВІТЧИЗНЯНОМУ ЗАКОНОДАВСТВІ

У вітчизняному законодавстві застосовується кілька десятків термінів на позначення того чи іншого виду інформації з обмеженим доступом (секретна інформація, таємна інформація, конфіденційна інформація, конфіденціальна інформація, нерозкрита інформація, незагальновідома інформація тощо), що ускладнює реалізацію норм права в практичній діяльності, оскільки їх правовий режим не забезпечений необхідним правовим регулюванням.

На законодавчому рівні також не визначено критерії, за допомогою яких можна однозначно кваліфікувати ті чи інші відомості (дані) як інформацію з обмеженим доступом чи виділити основні її види. Закон України «Про доступ до публічної інформації» лише містить норму, згідно з якою інформацією з обмеженим доступом є: 1) конфіденційна інформація; 2) таємна інформація; 3) службова інформація.

В окремих статтях вищезазначеного Закону надається легальна дефініція конфіденційної та таємної інформації, а також деталізується законодавцем розуміння службової інформації. Так, «*конфіденційна інформація* визначається як інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов» [59]. «*Таємна інформація* — це інформація, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу, передбачену законом таємницю» [59]. «*До службової* може належати така інформація: 1) що міститься в документах суб'єктів владних

повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою на пряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; 2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці» [59].

Акцентуємо, що визначення дефініції конфіденційної інформації, що містив Закон України «Про інформацію» до прийняття згаданого вище Закону, дещо схоже, зокрема «відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов» (ст. 30).

Згідно з цими визначеннями єдиний критерій віднесення інформації до режиму конфіденційної — це розповсюдження її за бажанням фізичної або юридичної особи та у відповідності до передбачених ними умов [60, с. 187–188].

Ю. М. Капіца вважає, що закріплене в законодавстві визначення конфіденційної інформації дуже складне для практичного застосування. При цьому вчений справедливо зауважує, що коли така інформація не розповсюджується або у випадку розповсюдження не обумовлюється її конфіденційність, то не зрозуміло, як буде визначатися режим конфіденційності такої інформації (наприклад, інформації про приватне життя).

Таким чином, чи буде визнаватись деяка інформація, наприклад, персональні дані конфіденційною інформацією, якщо їх власник не забезпечує під час її розповсюдження режим конфіденційності? Друге, на що слід звернути увагу для з'ясування бачення законодавцем видів інформації з обмеженим доступом, це на дефініцію таємної інформації.

У ст. 21 Закону України «Про інформацію» лише закріплено, що «порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами» [39]. Нині немає нормативно-правових актів, у яких би чітко та повно було розкрито особливості цих видів інформації з обмеженим доступом.

У ст. 6 Закону України «Про доступ до публічної інформації» зазначено, що «*таємна інформація* — це інформація, розголошення якої може завдати шкоди особі, суспільству і державі» [59].

Отже, у дефініції таємної інформації визначається, що її розголошення завдає шкоди особі, суспільству і державі. Проте виникає питання: хіба власник конфіденційної інформації встановлює обмежений режим доступу не у зв'язку з тим, що, на його думку, при її розголошенні третім особам завдається шкода його інтересам? Тим більше, що заподіяння шкоди інтересам окремій особі як суб'єкту права, певним правовідносинам негативно впливає в цілому на правопорядок в країні, а отже, безпосередньо завдається шкода інтересам держави та суспільства.

Таким чином, класифікація інформації з обмеженим доступом за критерієм заподіяння шкоди певним інтересам, визначена у вищезазначених нормативних актах України, є хибною.

Наприклад, у Російській Федерації законодавчо закріплена класифікація інформації з обмеженим доступом на конфіденційну та таємну інформацію, до останньої належить державна таємниця. Щодо переліку конфіденційної інформації, то він доволі значний: комерційна, банківська, професійна та службова.

Таку саму позицію підтримують і деякі вітчизняні вчені, які до змісту конфіденційної інформації включають всю інформацію, що складає будь-яку таємницю [61, с. 6–7].

Відомий російський дослідник В. Лопатін до складу конфіденційної інформації відносить комерційну, банківську, професійну та службову таємницю [62–63].

І. Зенін погоджується з ним, проте зазначає, що конфіденційна інформація існує ще й у вигляді ноу-хау [64, с. 574].

Г. Андрощук до конфіденційної відносить інформацію ділового, виробничого, торгового та іншого характеру, що не підлягає розголошенню у зв'язку з її секретністю [65, с. 27–32].

Аналіз норм вітчизняного чинного законодавства надав можливість дійти висновку, що, зважаючи на визначення конфіденційної інформації, до неї можна віднести лише інформацію особистого характеру (персональні дані) та, можливо, комерційну таємницю через те, що, як було зазначено вище, законодавець закріпив, що інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу, передбачену законом таємницю, визнається таємною.

Абсолютно незрозуміло, чому саме ці види таємниць законодавець зарахував до таємної інформації. Дослідження вітчизняного законодавства

показало, що і службова, і військова, і медична таємниці, а також таємниці нарадчої кімнати слід відносити до таємної інформації у зв'язку з тим, що держава в обов'язковому порядку вимагає таємності таких відомостей.

До того ж доволі дискусійними є питання щодо співвідношення службової та професійної таємниць.

Слід зазначити, що в законодавстві України термін «таємниця» є часто вживаним, зокрема існує медична, військова, комерційна, адвокатська таємниці, таємниця нарадчої кімнати, страхування, вчинюваних нотаріальних дій, усиновлення, листування, телефонних розмов, телеграфної та іншої кореспонденції тощо.

Однак не кожен з цих видів інформації можна віднести до категорії таємної. Наприклад, комерційна таємниця чи усиновлення відповідно до вітчизняного законодавства за умов бажання власника цієї таємниці може бути розголошена. Тобто закон не вимагає таємності інформації в силу її існування, а обмеження доступу виникає з моменту прийняття власником рішення про це, означає, що незалежно від назви, за змістом така інформація є конфіденційною.

Це доводить, що термін «таємниця» не є визначальним при віднесенні певної інформації до таємної інформації.

Виходячи з цього, вважаємо, що вкрай необхідно законодавчо закріпити вичерпний перелік видів інформації, що становить «іншу, передбачену законом таємницю», або перелік засад віднесення інформації до категорії таємної. Щодо вичерпного переліку конфіденційної інформації, то, зважаючи на її легальну дефініцію, це неможливо, оскільки її власник (фізична чи юридична особа, крім суб'єкта владних повноважень) уповноважений відносити будь-яку інформацію до категорії конфіденційної, крім законодавчо закріплених обмежень.

Водночас вважаємо за доцільне встановити хоча б приблизний перелік відомостей, які можуть бути віднесені до категорії конфіденційної інформації. «Це, однак, не повинно означати відсутності загальних принципів законності віднесення інформації до категорії конфіденційності. Якщо закон встановить окремі види конфіденційної інформації та характер відомостей, що до них належать (наприклад, комерційна таємниця), з метою визначення порядку її обігу та функціонування, це не означатиме вичерпності видів такої інформації та порушення диспозитивності норми (наприклад, якщо інформація не відповідає ви-

значенню комерційної таємниці, це не означає того, що вона не може бути визнана конфіденційною взагалі)»<sup>44</sup>.

У цьому контексті звернімося до досвіду Російської Федерації. Відповідно до Указу Президента Російської Федерації «Про затвердження переліку відомостей конфіденційного характеру» від 6 березня 1997 року в редакції від 23 вересня 2005 року було затверджено такий перелік відомостей конфіденційного характеру.

1. Відомості про факти, випадки та обставини приватного життя громадянина, що дозволяють ідентифікувати його особистість (персональні дані), за винятком відомостей, які підлягають розповсюдженню в засобах масової інформації у встановлених федеральними законами випадках.
2. Відомості, що становлять таємницю слідства і судочинства, а також відомості про осіб, яких захищають, і заходи державного захисту, що здійснюються відповідно до Федерального Закону від 20 серпня 2004 року «Про державний захист потерпілих, свідків та інших учасників кримінального судочинства» та іншими нормативними правовими актами Російської Федерації.
3. Службові відомості, доступ до яких обмежений органами державної влади відповідно до Цивільного кодексу Російської Федерації і федеральних законів (службова таємниця).
4. Відомості, пов'язані з професійною діяльністю, доступ до яких обмежений відповідно до Конституції Російської Федерації і федеральних законів (лікарська, нотаріальна, адвокатська таємниця, таємниця листування, телефонних переговорів, поштових відправлень, телеграфних чи інших відомостей тощо).
5. Відомості, пов'язані з комерційною діяльністю, доступ до яких обмежений відповідно до Цивільного кодексу Російської Федерації і федеральних законів (комерційна таємниця).
6. Відомості про сутність винаходу, корисної моделі чи промислового зразка до офіційної публікації інформації про них [66].

Аналіз вищезазначених норм правового акта надав можливість дійти висновку, що на законодавчому рівні встановлено вичерпне коло конфіденційної інформації та зміст відомостей, які до неї належать, з

<sup>44</sup> Беляков К. І. Інформація з обмеженим доступом: проблеми законодавчого регулювання / К. І. Беляков // Науковий вісник Національної академії внутрішніх справ. — К., 2004. — № 6. — С. 267–277.



метою визначення порядку їх обігу та унеможливлення незаконних обмежень права на інформацію.

Крім того, зазначений перелік конфіденційної інформації ще раз доводить безпомилковість нашого міркування з приводу того, що галузь застосування конфіденційної інформації або коло її суб'єктів не має значення. Тож інформація, яка містить професійну, банківську таємницю, таємницю слідства та іншу, передбачену законом таємницю, має становити зміст конфіденційної інформації, а таємною є винятково та інформація, яка містить державну таємницю.

Отже, **конфіденційною інформацією**, на нашу думку, слід визнавати будь-яку інформацію з обмеженим доступом, що не має ознак державної таємниці, а **таємною** — будь-яку інформацію з обмеженим доступом, що має ознаки державної таємниці.

Саме розподіл інформації з обмеженим доступом на ці два види є більш обґрунтованим.

Такий підхід до розуміння інформації з обмеженим доступом вже апробований в Російській Федерації, де в Законі РФ «Про інформацію, інформатизацію та захист інформації» [67] інформація з обмеженим доступом поділяється на державну таємницю та конфіденційну інформацію, до останньої, своєю чергою, належать усі таємниці, крім державної.

## 2.2 КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В ДОКТРИНАЛЬНИХ ДЖЕРЕЛАХ

Зважаючи на багатоаспектність і відсутність адекватного законодавчого закріплення видів інформації з обмеженим доступом, кожен із дослідників виокремлює різні види таємниць та критерії класифікації інформації з обмеженим доступом, сприяючи полісемії та синонімії понять.

Проблема класифікації інформації з обмеженим доступом одержала широкий резонанс у юридичній літературі. Дослідники пропонують різноманітні підходи та критерії її класифікації.

Варіанти класифікації на доктринальному рівні свого часу пропонували такі вчені, як Б. Ахлібінінський, О. Кохановська, Л. Кураков, В. Лопатін, С. Смірнов, Ф. Тарасенко та інші [54–58].

Л. Л. Фат'янов пропонує класифікацію за ступенем соціальної цінності окремого виду інформації з обмеженим доступом (залежно від передбачуваного збитку від поширення інформації) [37, с. 10]. За даним критерієм найбільшого соціального значення набуває державна таємниця, оскільки вона має загальнодержавне, загальнонаціональне значення. Щодо усіх інших таємниць, то за цією ознакою вони мають другорядне значення, і їх розподіл має умовний, почасти суб'єктивний характер. Отже, згідно з позицією Л. Л. Фат'янова розрізняється інформація з обмеженим доступом, що належить державі (державна таємниця), юридичним (банківська, комерційна таємниця і т. ін.) і фізичним особам (особиста, сімейна і т. ін.).

Слід зауважити, що такий критерій класифікації інформації з обмеженим доступом доволі розповсюджений в наукових колах. З цього приводу зауважимо, що він потребує деякого уточнення. На нашу думку, доречніше говорити не про соціальну цінність, а про цінність для її власника чи добросовісного користувача (суб'єкта інформації з обмеженим доступом), оскільки така інформація може не мати жодної соціальної цінності для суспільства, а для її власника навпаки має значну цінність через невідомість іншим. Історичні події свідчать, що навіть інформація, якій надано статус державної таємниці, є цінною винятково для окремих високопосадовців.

Серед інших критеріїв класифікації інформації з обмеженим доступом виділяють і *способи її придбання*. Так, за цим критерієм розрізняють таємниці, придбані на підставі цивільно-правового договору та під час здійснення професійної діяльності [35, с. 75–77]. Якщо критерій розподілу не викликає заперечення, то виокремлення видів інформації з обмеженим доступом за цим критерієм є, на нашу думку, дискусійними. Більш адекватним є поділ на таку, що придбана безоплатно, та таку, що придбана за гроші.

Доволі цікава пропозиція О. О. Кулініч, яка зауважує, що «слід класифікувати всю сукупність відомостей, що складають інформацію з обмеженим доступом, за складною підставою, що одночасно об'єднує декілька підстав, а саме: особливості суб'єктного складу, спосіб виникнення правового режиму, зміст (характер) відомостей, що складають інформацію з обмеженим доступом. З використанням даної підстави класифікації весь обсяг інформації з обмеженим доступом представлений складною системою різних видів інформації з обмеженим доступом, об'єднаних у

дві великі групи: державна таємниця і конфіденційна інформація. При цьому конфіденційною інформацією визнається будь-яка інформація з обмеженим доступом, що не має ознак державної таємниці. Конфіденційна інформація, своєю чергою, представлена такими видами: таємниця приватного життя (у т.ч. особиста і сімейна таємниця), комерційна таємниця, професійна та службова таємниці» [35, с. 77].

На нашу думку, таку класифікацію не можна вважати досконалою. І насамперед тому, що не досить зрозуміло, як використовувати інтегративний критерій (особливості суб'єктного складу, спосіб виникнення правового режиму, зміст (характер) відомостей, що складають інформацію з обмеженим доступом) для виокремлення того чи іншого виду інформації з обмеженим доступом.

Наприклад, у Російській Федерації таємниця листування, телефонних розмов, поштових, телеграфних та інших відправлень згідно з п. 2 ст. 17 Конституції РФ визнається невід'ємним правом людини і громадянина. Отже, виникає питання: чи визнавати таємницю листування, телефонних розмов, поштових, телеграфних та інших відправлень як професійну таємницю працівників систем зв'язку чи особисту таємницю людини і громадянина, оскільки п. 1 тієї ж ст. 17 Конституції РФ встановлюється право на недоторканність приватного життя, особисту та сімейну таємницю.

Тим більше, що автором не визначається, що саме є інформацією з обмеженим доступом, хоча «конфіденційна інформація визнається як будь-яка інформація з обмеженим доступом, що не має ознак державної таємниці» [35, с. 77].

Як показало дослідження друкованих джерел з цієї теми, здебільшого дослідники проблематики інформації з обмеженим доступом класифікують інформацію з обмеженим доступом на певні види таємниць без визначення критеріїв.

Зокрема, О. В. Ботвінкін та В. П. Ворожко серед видів інформації з обмеженим доступом, що не є державною таємницею, виокремлюють такі види таємниць, як конфіденційна інформація про особу, адвокатська, банківська, військова, комерційна, лікарська, професійна, службова таємниці, а також таємниця голосування, кореспонденції, листування, наради суддів, нотаріальних дій, страхування, телефонних розмов, усиновлення, вкладів (рахунків), заповіту, слідства, інформації у поштовому зв'язку, про стан здоров'я, псевдонім тощо [23, с. 5].

А. І. Марущак зауважує, що інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну. До останньої, своєю чергою, відноситься державна, комерційна, службова, професійна, військова, банківська, адвокатська, лікарська таємниці, а також таємниця страхування, усиновлення, голосування, нотаріальних дій, листування, телефонних розмов, телеграфної та іншої кореспонденції [24, с. 23–25].

Таким чином, відсутність критеріїв класифікації інформації з обмеженим доступом не дозволяє адекватно пояснити багатоаспектність порушеної проблематики. Хоча об'єктивно окрема інформація, що має обмежений режим доступу, за одним і тим самим критерієм класифікації може належати до різних груп.

Наприклад, беручи за критерій *сферу реалізації інформації з обмеженим доступом*, військова, банківська, адвокатська, лікарська таємниці, а також таємниці страхування, усиновлення, голосування, нотаріальних дій являють собою професійну чи службову таємниці, оскільки фахівці вищезазначеної діяльності мають забезпечувати режим конфіденційності інформації, яку вони отримали внаслідок реалізації своїх професійних потреб. Хоча таємниця листування, лікарська таємниця, таємниця усиновлення тощо пов'язана насамперед із захистом особистих даних, а вже потім із виконанням певного роду діяльності щодо надання різноманітних послуг. Крім того, виокремлення поряд з вищезазначеними видами таємниць, професійної та службової таємниці потребує додаткового пояснення критеріїв їх розрізнення.

На думку російського дослідника В. А. Копилова: «...аналіз основних видів інформації, що виробляється, надає можливість поділити їх на дві групи: відкриту, яка вільно розповсюджується в інформаційній сфері, і обмеженого доступу, розповсюдження якої можливе лише на умовах конфіденційності або таємності.

До відкритої інформації належать:

- інформація, що створюється в процесі творчості (витвори науки та мистецтва, відкриті патенти та авторські свідоцтва);
- документована інформація, що надається обов'язковою;
- офіційні документи;
- масова інформація, що розповсюджується ЗМІ;
- інша інформація необмеженого доступу.

До інформації обмеженого доступу належить:

- документована інформація про державну та службову таємницю (в порядку захисту інтересів держави);
- документована інформація, що містить відомості про ноу-хау та ноу-ноу ( в порядку захисту секретів виробництва і науки);
- персональні дані ( в порядку захисту особистої таємниці)» [21, с. 35–36].

Отже, в основі поділу інформації з обмеженим доступом лежить такий критерій, як *інтереси осіб, які потребують захисту у зв'язку з такою інформацією*.

З цього приводу доволі влучно зауважив Б. А. Кормич: «Схема «відкритої та закритої інформації» не може до кінця розкрити особливості існуючих її винятків та обмежень. Так, наприклад, подібна схема не робить різниці між інформацією, яка містить державну таємницю і доступ до якої може бути наданий лише обмеженому колу осіб, та інформацією, яка може бути передана будь-яким зацікавленим особам за відповідну винагороду ( ті ж самі ноу-хау). Причому це може бути як передача копії цієї інформації, так і повна передача усіх прав на подібну інформацію» [9, с. 274].

Не менш дискусійна позиція М. В. Рудика щодо визначення видів інформації з обмеженим доступом, який зазначив, що: «розглянувши диспозиції статей Особливої частини Кримінального кодексу України, предметом злочину в яких виступає інформація з обмеженим доступом, визначилися декілька ознак, за якими їх можна об'єднати в групи з метою їх подальшої класифікації для полегшення їх теоретичного дослідження та практичного застосування:

1. *За ступенем таємності комп'ютерна інформація* поділяється на конфіденційну та таємну.
2. *За суб'єктом інформаційних відносин, якому фактично належить така інформація:* державні органи (спеціально уповноважені посадові особи і службовці), що мають доступ до таємної інформації; юридичні та фізичні особи, які є власниками конфіденційної інформації (суб'єкти господарювання та приватні підприємці)» [33, с. 55].

Формулювання, що державні органи в особі спеціально уповноважених посадових осіб і службовців мають доступ до таємної інформації, а юридичні та фізичні особи є власниками конфіденційної інформації (суб'єкти господарювання та приватні підприємці) (Підкреслено нами. — Авт.)

Та чи завжди органи державної влади мають доступ до інформації з обмеженим доступом, не будучи власниками цієї інформації? Чи уся інформація, що належить юридичним та фізичним особам, є їх власністю? На нашу думку, ні. Як державні органи можуть бути власником інформації з обмеженим доступом, так і юридичні та фізичні особи мають доступ до такої інформації через надання власником цієї інформації права користуватися нею, забезпечуючи режим таємності на відповідних умовах.

Як слушно зазначив російський юрист Ю. С. Пилипенко: «Если речь идет, например, о поверенных тайнах, то по крайней мере один из их субъектов, а именно поверенный, — не собственник конфиденциальной информации. Имеющееся у него право распоряжения ею, как правило, строго ограничено целями его деятельности, а также интересами открыто заявленной волей доверителя, который, в свою очередь, может быть и не быть собственником конфиденциальной информации» [68, с. 21].

Дане положення також підтверджується і нормами першої редакції Закону України «Про інформацію», де інформація з обмеженим доступом за своїм правовим режимом поділялась на конфіденційну і таємну, при чому конфіденційна інформація визначалася як відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов, а стосовно інформації, що є власністю держави і перебуває в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, зауважувалось, що з метою її збереження може бути відповідно до закону встановлено обмежений доступ — надано статус конфіденційної [39].

Хоча заради об'єктивності маємо зазначити, що деякі фахівці цивільного права заперечують право власності на інформацію. Таке визначення суперечить самій природі інформації.

Цікаву наукову позицію щодо системи правового регулювання обігу інформації має Б. А. Кормич. Так, дослідник зауважує, що вона складніша за режими доступу до інформації або правові режими інформаційних ресурсів, які лише складові цього регулювання [69, с. 165]. Згідно з його міркуваннями: «основою класифікації можуть бути методи правового регулювання, які застосовують в регулювання суспільного обі-



гу того чи іншого виду інформації, — диспозитивний та імперативний» [69, с. 165]. Застосування двох правових методів регулювання створюють «три можливі види правового обігу інформації: відкритий, що регулюється диспозитивним методом (виключно цивільно-правовими нормами); закритий, що регулюється імперативним методом (адміністративно-правовими нормами); і обмежений, до якого застосовуються обидва види правового регулювання. До цих методів також долучається вільний обіг інформації, який безпосередньо правом не врегульований, але щодо якого можуть виникати охоронні правовідносини у разі порушення певних заборон чи обмежень. Причому інформація, змінюючи свою суспільну цінність, може переходити з одного виду обігу до іншого (зняття грифів «таємно», або «для службового користування», закінчення строку дії авторських прав тощо)» [69, с. 166].

Беручи до уваги вищезазначену класифікацію, інформація з обмеженим доступом, на думку Б. А. Кормича, належить до інформації закритого обігу, який, своєю чергою, має такі основні характеристики:

- інформація вилучена з вільного обігу на підставі закону;
- законодавство надає інформації статус конфіденційної або таємної;
- власник інформації здійснює заходи щодо її захисту;
- надання такої інформації третім особам або допуск до неї можливий лише у разі проведення певної процедури;
- отримання такої інформації пов'язане, як правило, із виконанням службових або професійних обов'язків.

Підтримуючи у цілому концепцію класифікації правового регулювання обігу інформації, маємо певні зауваження щодо характерних рис інформації з обмеженим доступом. Ми вже висловлювали свої міркування з приводу «власника інформації», який не завжди збігається із суб'єктом інформації з обмеженим доступом. А тому доречніше говорити не лише про власника такої інформації, який здійснює заходи щодо її захисту, а й розширити це коло до добросовісних користувачів. Сумнівним видається і твердження автора про те, що «отримання такої інформації пов'язане, як правило, із виконанням службових або професійних обов'язків», оскільки конфіденційна інформація про особу не завжди виникає у зв'язку із виконанням службових або професійних обов'язків. Процедура надання такої інформації або допуск до неї третім особам також різняться залежно від виду таємниці.



Інша думка Б. А. Кормича, на якій слід наголосити, це характеристика інформації в обмеженому обігу. Як зауважує автор: «Специфічною є інформація в обмеженому обігу, тобто така, щодо якої не встановлено обмеженого режиму доступу, але разом з тим існують певні заборони або обмеження в її розповсюдженні, які встановлено зазвичай з метою захисту суспільної моралі та здоров'я і запобігання негативно-інформаційному впливу на суспільство або окремі, найбільш вразливі його групи» [69, с. 168].

На нашу думку, доречніше виділяти інформацію, яка є взагалі забороненою для розповсюдження в конкретній країні та така, розповсюдження якої має обмеження в силу певних обставин, наприклад потенційної шкідливості такої інформації для певних категорій осіб. Так, у ст. 28 Закону України «Про інформацію» заборонено використовувати будь-де, будь-ким інформацію для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини [39].

Яскравим прикладом другого виду інформації є норми Закону України «Про захист суспільної моралі», в ст. 7 якого визначено, що з метою захисту морального та фізичного життя неповнолітніх забороняється:

- втягнення неповнолітніх у діяльність з виробництва й обігу продукції сексуального чи еротичного характеру, порнографічних матеріалів, надання послуг, а також організації й проведення видовищних заходів сексуального чи еротичного характеру;
- розповсюдження продукції сексуального чи еротичного характеру, порнографічних матеріалів, надання послуг і проведення видовищних заходів сексуального чи еротичного характеру серед неповнолітніх;
- використання образів неповнолітніх у будь-якій формі в продукції сексуального чи еротичного характеру і проведенні видовищних заходів сексуального чи еротичного характеру;
- виготовлення (виробництво), зберігання, реклама, розповсюдження, придбання продукції, що містить дитячу порнографію, ввезення, вивезення, транзит через територію України, поштова пересилка такої продукції;

- пропонування або надання доступу до продукції, що містить дитячу порнографію [70].

Деякими дослідниками класифікація інформації з обмеженим доступом здійснюється *залежно від захисту майнових чи особистих інтересів*. Відповідно до цього критерію така інформація поділяється на комерційну таємницю (захист майнових інтересів) та конфіденційну інформацію про особу, банківську таємницю тощо (захист різного роду публічних інтересів або особистих прав).

Аргументуючи свою позицію, автори зауважують, що «на відміну від комерційної таємниці, інші таємниці, як правило, мають за мету не охорону визначених майнових благ, а захист різного роду публічних інтересів або особистих прав. Всі вказані види таємниць можуть представляти комерційну цінність для осіб, однак вони всі, крім комерційної таємниці, відповідними законами виключені із цивільного обігу (наприклад: неможливо уявити існування чинного договору про передачу інформації, яка становить державну таємницю)» [35, с. 77].

Таким чином, багатоаспектність інформації з обмеженим доступом дозволяє поряд з вищезазначеними критеріями виділяти й інші *критерії її класифікації, зокрема залежно: від правомірного чи неправомірного доступу до неї, володіння чи користування, від сфери, де циркулює така інформація* тощо.

Зважаючи на те, що в Законі України «Про доступ до публічної інформації» наявна норма, згідно з якою інформація з обмеженим доступом поділяється на конфіденційну, таємну та службову інформацію, в цій науковій роботі будемо користуватися саме таким поділом. Хоча ряд нормативно закріплених засад потребують, як було зауважено вище, змін та доповнень, оскільки викладені положення, також як і в Законі України «Про інформацію», унеможливають чітке розмежування конфіденційної, таємної та службової інформації, а отже, непридатні для практичного застосування.

З цього приводу є конструктивними пропозиції К. І. Белякова, який зауважив про потребу і невичерпну актуальність, як мінімум, продовження дослідження Проекту<sup>45</sup> та прийняття Закону України «Про ін-

<sup>45</sup> Матеріали до «круглого» столу «Обговорення проекту Закону України «Про інформацію з обмеженим доступом, що не становить державної таємниці» // Правове, нормативне та методологічне забезпечення системи захисту інформації в Україні : третя наук.-практ. конф., (м. Київ, 8–10 жовт. 2001 р.). — К., 2001. — С. 1–24.

формацію з обмеженим доступом, що не становить державної таємниці», розпочато Науково-дослідним центром «ТЕЗІС» НУТУ «КПІ» ще у 1998 році на замовлення колишнього Держкомсекретів України, а як максимум, розробки та прийняття Основ Кодексу України про інформацію (чи Кодексу, що регулює суспільні інформаційні відносини, під іншою назвою)<sup>46</sup>.

---

<sup>46</sup> Беляков К. І. Інформація з обмеженим доступом : проблеми законодавчого регулювання / К. І. Беляков // Науковий вісник Національної академії внутрішніх справ. — К., 2004. — № 6. — С. 267–277.



# **ПОНЯТТЯ ТА СТРУКТУРА АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ**

---

- 3.1 ЗМІСТ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ
- 3.2 ХАРАКТЕРИСТИКА ЕЛЕМЕНТІВ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ
- 3.3 УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ





### **3.1 ЗМІСТ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ**

Перед тим як окреслити особливості адміністративно-правового режиму інформації з обмеженим доступом в Україні слід з'ясувати розуміння понять «режим», «правовий режим», «адміністративно-правовий режим».

#### ***Поняття «режим»***

Термін «режим» доволі розповсюджений як у повсякденному житті, так і серед науковців.

Дедалі більше він використовується не лише в технічних, економічних науках, а й в юридичних науках і різноманітних вітчизняних нормативно-правових актах, зокрема в Господарському кодексі України [71], Митному кодексі України [72], законах України «Про правовий режим земель охоронних зон об'єктів магістральних трубопроводів» [73], «Про землі енергетики та правовий режим спеціальних зон енергетичних об'єктів» [74], «Про правовий режим воєнного стану» [75], «Про правовий режим надзвичайного стану» [76] закріплено певні види правового режиму. Аналіз вищезазначених нормативно-правових актів надає можливість дійти висновку, що здебільшого певний правовий режим розкривається через порядок його введення та припинення дії, особливості діяльності органів державної влади та органів місцевого самоврядування, підприємств, установ і організацій в умовах цього режиму, додержання прав і свобод людини і громадянина, а також прав і законних інтересів юридичних осіб і відповідальність за порушення вимог або невиконання заходів правового режиму.



Не менш вживаним поняття «режим» є в міжнародних документах, наприклад Угода СНД про правовий режим інформаційних ресурсів Прикордонних військ держав-учасниць Співдружності Незалежних Держав [77] від 25 листопада 1998 року, Договір між Україною і Республікою Польща про правовий режим українсько-польського державного кордону, співробітництво та взаємну допомогу з прикордонних питань Україна від 12 січня 1993 року, ратифікований Постановою Верховної Ради України «Про ратифікацію Договору між Україною і Республікою Польща про правовий режим українсько-польського державного кордону, співробітництво та взаємну допомогу з прикордонних питань» від 14 липня 1993 року [78].

Хоча легальна дефініція цього поняття у вітчизняному законодавстві досі не закріплена. Відсутня єдність у розумінні цього поняття і серед фахівців теорії держави та права, галузевих юридичних наук, зокрема адміністративного права.

Розуміння цього терміна від першооснови до сучасного трактування значно відрізняється. Якщо вдатися до етимології, то слово походить від французького «regime» [79, с. 722] і латинського «regimen» [80, с. 493], що в перекладі означає управління.

Тлумачні словники надають цьому терміну кілька пояснень. Так, у С. І. Ожегова режим це: 1. Державний лад. 2. Встановлений порядок будь-чого. 3. Умови діяльності, праці, існування будь-чого [81, с. 665]. Новий тлумачний словник української мови розкриває поняття слова режим так: 1. Державний лад, спосіб правління. 2. Точно встановлений розпорядок життя, праці, відпочинку і т. ін. 3. Система заходів, правил, запроваджуваних для досягнення певної мети [82, с. 888].

Таке саме пояснення в «Словнику іншомовних слів» за редакцією О. С. Мельничука [83].

Інші джерела так трактують це поняття: а) державний лад, сукупність засобів, методів, способів здійснення влади; б) строго встановлений розпорядок життя, праці; в) система обов'язкових правил, вимог, норм, принципів, встановлених для якого-небудь виду діяльності; г) умови діяльності, існування чого-небудь; певний стан, положення, статус [84, с. 1005].

Щодо розуміння цього терміна в галузевих наукових дослідженнях, то воно також дискусійне. Так, на думку О. О. Крестянінова, режим — це сукупність правил, норм, заходів, необхідних для досягнен-

ня тієї або іншої мети [85, с. 90]. Іншу точку зору відстоюють С. В. Ківалов, Л. Р. Біла, які під режимом розуміють державний лад, спосіб правління; точно встановлений розпорядок життя, праці, відпочинку тощо; систему правил, законів, запроваджуваних для досягнення мети; умови діяльності, існування [86, с. 37].

Деякі з науковців зауважують, що поняття «режим» можна тлумачити в широкому і вузькому розумінні. Режим у широкому розумінні охоплює всю систему заходів, які використовуються для досягнення поставлених перед ними цілей [87, с. 113–114]. Режим у вузькому розумінні слова – сукупність правил поведінки [88, с. 176].

### Поняття «правовий режим»

Немає у наукових колах єдиної думки і щодо розуміння поняття «правовий режим», причому позиція авторів здебільшого залежить від того, яку саме галузь юридичної науки репрезентує той чи той дослідник.

З метою більш повного й об'єктивного визначення поняття «правовий режим» вважаємо за необхідне дослідити позиції у цьому контексті як фахівців теорії держави та права, так і галузевих наук — адміністративного, цивільного права.

Серед фахівців теорії держави та права, які займались порушеною проблематикою слід відмітити С. С. Алексеєва, Н. І. Матузова, А. В. Малька, В. М. Корельського, В. Д. Перевалова.

На думку С. С. Алексеєва, *правовий режим* – порядок регулювання, який виражений у комплексі правових засобів, що характеризують особливе сполучення взаємодіючих між собою дозволів та заборон, а також позитивних зобов'язань, які утворюють особливу направленість регулювання [89, с. 185].

Н. І. Матузов та А. В. Малько розглядають *правовий режим* як особливий порядок правового регулювання, який виражається у певному поєднанні юридичних засобів і створює бажаний соціальний стан і конкретний ступінь сприятливості або несприятливості для задоволення інтересів суб'єкта права. Тобто *режим* — це система умов і методів здійснення правового регулювання, так би мовити, «розпорядок» дії права, його функціональна характеристика [90, с. 17–18].

На думку Е. Ф. Шамсумової, *правовий режим* — це особливий порядок законодавчого регулювання діяльності суб'єктів права у різнома-

нітних сферах суспільних відносин або на певних об'єктах, який складається зі встановлення механізму забезпечення фактичної реалізації системи стимулів, нормативів, гарантій, заборон, зобов'язань, обмежень, а також їх виконання, застосування заходів примусу та притягнення винних до відповідальності [91, с. 71–72].

В. М. Корельський, В. Д. Перевалов під *правовим режимом* розуміють специфіку юридичного регулювання певної сфери суспільних відносин за допомогою різних юридичних засобів [92, с. 265].

З позиції інших фахівців теорії держави та права *правовий режим* — це певний порядок правового регулювання, який забезпечується через особливе поєднання залучених для його здійснення способів, методів і типів правового регулювання [93, с. 410].

В. Б. Ісаков визначає правовий режим як соціальний режим певного об'єкта (явища, процесу, соціальної підсистеми), закріплений нормами права й забезпечений сукупністю юридичних засобів [94, с. 34–39].

Таким чином, здебільшого фахівцями теорії держави та права правовий режим визначається як певний порядок правового регулювання окремих суспільних відносин, тобто правовий режим ототожнюється з методом правового регулювання.

Щодо фахівців адміністративного права, то серед дослідників цієї проблематики слід відмітити таких, як Д. М. Бахрах, І. С. Розанов, В. Б. Рушайло, С. В. Ківалов, Л. Р. Біла та інших.

Так, попервах Д. М. Бахрах визначав правовий режим як систему норм права, яка регулює людську діяльність, відносини між людьми з приводу певних об'єктів [95, с. 13]. Згодом Д. М. Бахрах під правовим режимом вже вбачає офіційно встановлений особливий порядок правового регулювання, який відображає сукупність юридичних і організаційних засобів, які використовуються для закріплення соціально-правового стану об'єктів впливу і спрямований на забезпечення їх сталого функціонування [96, с. 478].

І. С. Розанов під *правовим режимом* розуміє сукупність правових актів та організаційно-технічних заходів, що утворюють у відповідній сфері безпеки своєрідний комплексний юридико-організаційний інститут [97, с. 84].

На думку В. Б. Рушайла, *правовий режим* — це закріплені в законодавстві права, обов'язки та відповідальність; система заходів, які використовуються для досягнення поставлених цілей; система правопо-

го впливу, що полягає у специфіці прийомів регулювання та його механізму [98, с. 14].

С. В. Ківалов, Л. Р. Біла *правовий режим* тлумачать як сукупність правил, закріплених юридичними нормами, що регулюють певну діяльність людей [86, с. 37].

У найзагальнішій формі поняття «правовий режим» визначається Ю. П. Битяком як порядок регулювання, комплекс правових засобів, що характеризують особливе поєднання взаємодіючих дозволів, заборон, а також позитивних зобов'язань, який створює особливу спрямованість регулювання [99, с. 276].

Таким чином, усі ці визначення поняття «правовий режим» мають загальнотеоретичну спрямованість, а тому в них не відображається галузева специфіка права. Кожній галузі права притаманний свій специфічний режим регулювання, яким і обумовлюється юридична особливість певної галузі [99]. Кожна галузь права використовує більш вузьке поняття з позицій специфіки своєї галузі: адміністративне право — адміністративно-правовий режим, цивільне право — цивільно-правовий режим тощо.

### ***Етапи становлення вчення про адміністративно-правовий режим***

У формуванні теорії адміністративно-правових режимів у адміністративній науці можна виокремити два етапи. *На першому етапі* адміністративне право розглядало адміністративно-правовий режим винятково як вид адміністративно-правового регулювання суспільних відносин, що виникають у надзвичайних ситуаціях або за воєнного стану. Адміністративно-правовий режим в наведеному контексті пов'язаний з легальними обмеженнями прав і свобод людини, які закріплені Конституцією України, і не може розповсюджуватися на звичайне нормальне функціонування держави та суспільства.

Саме в такому контексті колектив авторів підручника з адміністративного права за редакцією Ю. М. Козлова та Л. Л. Попова визначають адміністративно-правовий режим — як комплекс державно-управлінських та організаційно-правових засобів, що істотно відрізняються від тих, які застосовуються органами державної влади в нормальних (звичайних) умовах функціонування. З їхньої точки зору, адміністра-

тивно-правові режими являють собою заснований на нормах адміністративного права особливий порядок функціонування його суб'єктів, спрямований на подолання негативних явищ у відповідній сфері державного управління [100, с. 467].

Таку саму позицію відстоює І. С. Розанов, розглядаючи зазначений режим як встановлену в законодавчому порядку сукупність правил діяльності, дій або поведінки громадян і юридичних осіб, а також порядок реалізації ними своїх прав за певних умов (ситуацій) забезпечення і підтримки суверенітету та оборони держави, інтересів безпеки й охорони громадського порядку спеціально створеними для цієї мети службами державного управління [97, с. 85].

*На другому, сучасному етапі* теорія адміністративно-правових режимів уже має більш широке трактування. «У його основу покладено припущення, що сутність адміністративно-правових режимів знаходиться у плоскості об'єктивних закономірностей управління, які забезпечують досягнення його цілей, підтримання усталеного стану системи управління й управлінських процесів, що відбуваються у її межах. У межах державного управління об'єктивні закономірності, що визначають сутність та зміст управління соціального, отримують предметне відбиття, яке відповідає владній природі виконавчої влади та її специфіці в системі розподілу влади» [101, с. 97].

На наше глибоке переконання, адміністративно-правові режими необхідні не лише для здійснення управлінської діяльності в надзвичайних ситуаціях, а й для розв'язання поточних проблем у певних сферах, зокрема захисту інформації з обмеженим доступом.

Введення адміністративно-правових режимів обумовлено тим, що держава з метою забезпечення національних інтересів громадян, суспільства і власних інтересів не може залишити без уваги певні сфери суспільних відносин. Порушення встановлених державою особливих правил у певних сферах може спричинити істотну шкоду правам та свободам людини, інтересам держави та суспільства в цілому.

Отже, сучасне бачення теорії адміністративно-правового режиму пов'язане з окресленням специфіки державного управління в конкретних сферах суспільного життя.

## *Поняття «адміністративно-правовий режим»*

Плюралізм наукових поглядів на визначення поняття «правий режим» сприяв багатоманіттю його розуміння. Слід зазначити, що це поняття знайшло своє відображення в численних доктринальних джерелах з адміністративного права. Хоча адміністративно-правовий режим є різновидом правового режиму, спостерігається неоднозначне визначення цих понять, використання різних підходів при їх трактуванні одними й тими самими авторами.

Ю. О. Тихомиров тлумачить адміністративно-правовий режим як специфічний порядок діяльності суб'єктів права в різних сферах державного життя, який встановлюється в законах та підзаконних актах і спрямований на їх суворо цільову та функціональну діяльність у тій царині, де необхідні додаткові засоби для підтримки необхідного державного ладу [102, с. 325].

На думку С. В. Ківалова та Л. Р. Білої, адміністративно-правовий режим – це поєднання адміністративно-правових засобів регулювання, що виявляється в централізованому порядку, імперативному методі правового впливу та юридичній нерівності суб'єктів правовідносин [86, с. 38].

Підтримує згадану позицію і Ю. П. Битяк, зазначаючи, що адміністративно-правовий режим визначає певне поєднання адміністративно-правових засобів регулювання, що виявляється в централізованому порядку, імперативному методі правового впливу та юридичній нерівності суб'єктів правовідносин [99, с. 268].

Схожу позицію має і О. О. Крестьянінов, який зауважує, що адміністративно-правовий режим – це певна сукупність адміністративно-правових засобів регулювання, встановлених в централізованому порядку, які характеризуються імперативним методом юридичного впливу, котрий проявляється в тому, що завжди в адміністративно-правових відносинах присутній владний суб'єкт і підлегла особа. Тобто суб'єкти правовідносин перебувають у юридично нерівних позиціях [103, с. 91].

Така сама позиція спостерігається в першому в Україні академічному курсі з адміністративного права під редакцією В. Б. Авер'янова як найбільш розповсюджена в наукових колах, а саме: адміністративно-правовий режим – певне поєднання адміністративно-правових за-



собів регулювання, опосередкованого імперативним методом юридичного впливу, який виявляється в тому, що суб'єкти правовідносин займають юридично нерівні позиції [104, с. 9].

Таким чином, при визначенні поняття адміністративно-правового режиму здебільшого наголошують на трьох аспектах: застосуванні адміністративно-правових засобів регулювання, наявності юридично нерівних позицій між учасниками певних відносин та наявності імперативного методу юридичного впливу.

Виникає запитання: що мають на увазі дослідники, вказуючи про юридичну нерівність суб'єктів адміністративних правовідносин? Чому в одній і тій самій праці автори вказують на «новий погляд на сутність адміністративного права в демократичному суспільстві», зазначаючи при цьому, що «запровадження необхідних змін в адміністративному праві означає зрештою створення якісно нового, відмінного від колишнього, правового режиму регулювання відносин між органами виконавчої влади, їх посадовими особами і громадянами», «цей правовий режим відносин робить громадянина набагато більш рівноправним партнером у стосунках з державою, її органами і посадовими особами» [104, с. 9].

Чи можна говорити про юридичну нерівність учасників правових відносин, якщо вони мають взаємні права та обов'язки? Тим більше, в умовах становлення правової, демократичної держави та громадянського суспільства в Україні змінилось бачення відносин громадянина та держави в особі її компетентних органів чи уповноважених осіб у напрямі пріоритету прав і свобод людини та громадянина, а також взаємної їх відповідальності.

Таким чином, на сучасному етапі становлення адміністративного права відносини між особою та державою мають бути рівноправними.

Наявність такої тези у визначенні поняття «адміністративно-правовий режим» порушує такий важливий загальноправовий принцип сучасного права, як принцип рівноправності учасників правових відносин, серед яких виділяють і окрему людину, і державу в цілому.

Говорячи про юридичну нерівність суб'єктів адміністративних правовідносин, оскільки відносини між ними урегульовані на основі імперативного методу, не зовсім є правильним, оскільки імперативний метод вказує, що регулювання здійснюється згори, тобто на владно-імперативній основі.



Слід також усвідомлювати, як слушно зауважує С. О. Магда, «що реалізація того чи іншого адміністративно-правового режиму пов'язана з досягненням визначених цілей, досить часто обумовлена наявністю певних обставин або специфікою відповідної сфери суспільних відносин. Разом з цим, реалізація адміністративно-правового режиму обумовлює і чітку визначеність та порядок дій суб'єктів правовідносин, котрі виникають у зв'язку з його введенням чи реалізацією» [105, с. 68].

Зважаючи на вищевикладене, можна виділити такі **основні підходи до розуміння поняття «адміністративно-правовий режим»:**

- 1) специфічний порядок діяльності суб'єктів права в різних сферах державного життя, який встановлюється в законах та підзаконних актах і спрямований на їх суворо цільову та функціональну діяльність у тій царині, де необхідні додаткові засоби для підтримки необхідного державного ладу (Ю. О. Тихомиров);
- 2) сукупність (комплекс, певне поєднання) адміністративно-правових засобів регулювання, що виявляється в централізованому порядку, імперативному методі правового впливу та юридичній нерівності суб'єктів правовідносин (В. Б. Авер'янов, Ю. П. Битяк, О. О. Крестьянінов та інші).

Отже, у доктринальних визначеннях поняття «адміністративно-правовий режим» здебільшого визначається як особлива форма регулювання, в межах якої використовується комплекс (сукупність, система) юридичних, організаційних та інших засобів з метою забезпечення адекватного упорядкування суспільних відносин у відповідній сфері.

### **Ознаки адміністративно-правового режиму**

У науці адміністративного права здебільшого виділяють такі **ознаки адміністративно-правових режимів:**

- 1) застосування у сфері діяльності публічної адміністрації у зв'язку з виконанням органами державної влади, місцевого самоврядування своїх обов'язків, заходів щодо забезпечення безпеки, охорони, захисту об'єктів правового регулювання;
- 2) наявність у розпорядженнях, що утворюють режимні правила, адміністративно-правових норм, які забороняють, зобов'язують, а також обмежують загальну правосуб'єктність фізичних та юридичних осіб;

- 3) обов'язкова участь у якості основних суб'єктів органів виконавчої влади або місцевого самоврядування, які реалізують державні повноваження;
- 4) застосування адміністративно-правових методів впливу;
- 5) наявність заходів адміністративного та дисциплінарного впливу [106, с. 104–105].

### ***Поняття «адміністративно-правовий режим інформації з обмеженим доступом»***

Адміністративно-правовий режим інформації з обмеженим доступом — це урегульований у вітчизняному законодавстві порядок діяльності уповноважених суб'єктів права шляхом імперативного методу правового впливу та системи спеціальних засобів з метою захисту й охорони суспільних відносин у сфері інформації з обмеженим доступом.

Деякі вчені зауважують, що визначити правовий режим інформації дуже складно, а іноді майже неможливо [107, с.19], оскільки — не може існувати єдиного правового режиму для різних видів інформації [108, с.32].

Якщо відкрита інформація не має чітко визначеного правового режиму в силу своєї доступності, відкритості, свободи циркулювання тощо, то для інформації з обмеженим доступом правовий режим має бути встановлений як важливий засіб її захисту.

Інформація з обмеженим доступом цінна насамперед тому, що вона — не є загальновідомою та недоступна для кожного охочого. Відповідно особа, яка фактично контролює таку інформацію, може надати до неї доступ або обмежити доступ сторонніх осіб. Саме тому адміністративно-правовий режим інформації з обмеженим доступом, поряд з іншими правовими режимами, є важливим засобом її захисту.

### ***Ознаки адміністративно-правового режиму інформації з обмеженим доступом***

***Ознаки адміністративно-правового режиму інформації з обмеженим доступом:***

- 1) це діяльність уповноважених органів державної влади, інших уповноважених державою інституцій, органів місцевого само-

- врядування, окремих громадян щодо захисту інформації з обмеженим доступом;
- 2) ця діяльність урегульована у вітчизняному законодавстві шляхом визначення режимних правил, відповідно до яких вказуються права, обов'язки людини і громадянина, повноваження відповідних інституцій, адміністративна відповідальність за їх порушення тощо у сфері захисту інформації з обмеженим доступом;
  - 3) наявність імперативного методу правового впливу між учасниками відносин у сфері захисту інформації з обмеженим доступом;
  - 4) здійснюється за допомогою відповідної системи різноманітних спеціальних засобів;
  - 5) метою такої діяльності є забезпечення захисту суспільних відносин у сфері захисту інформації з обмеженим доступом, тобто відповідних прав і свобод людини та громадянина, інтересів держави та суспільства.

### ***Класифікація адміністративно-правових режимів***

Класифікація адміністративно-правових режимів стала предметом дослідження таких адміністративістів, як: Д. М. Бахрах, М. В. Білоконь, П. В. Дерев'янка, С. В. Ківалов, О. О. Крестьянінов, С. О. Кузніченко, С. С. Маїлян, Ю. М. Оборотов, І. С. Розанов, В. Б. Рушайло, Ю. О. Тихомиров [110, с. 416–418; 111, с. 41–44; 112, с. 72; 113, с. 160–161; 85, с. 250; 103, с. 93–94; 114, с. 247–252; 115, с. 24–27; 116, с. 41–42; 97, с. 87–88; 98, с. 37–50; 109, с. 327] та ін.

*За ступенем належності до забезпечення зовнішньої і внутрішньої безпеки держави* [97, с. 87] В. Б. Рушайло та С. С. Маїлян поділяють адміністративно-правові режими на три групи. До першої групи входять режими, спеціально націлені на забезпечення інтересів національної безпеки країни – безпеки держави. Це адміністративно-правовий режим захисту державної таємниці, прикордонний режим, режим в'їзду на територію країни та виїзду з її території. Другу групу складають режими, які встановлюються переважно з метою забезпечення суспільної безпеки. До них належать режими ліцензійно-дозвільної системи, паспортно-візової системи, санітарний режим та митний режим. Третя

група — це комплексні режими, що переслідують мету підтримки обороноздатності країни, суспільної безпеки та безпеки громадян в умовах настання надзвичайних ситуацій [98, 115].

Найбільш розповсюджені критерії класифікації адміністративно-правових режимів — це критерії за: *масштабом волі громадян і організацій у використанні своїх можливостей для реалізації суб'єктивних прав (пільгові та обмежувальні режими); глибиною змін у конституційному статусі громадян і організацій (звичайні та надзвичайні режими); часом дії (постійні або короткочасні, ситуаційні режими), територією їх дії (режими, що діють на всій території України або в окремих її регіонах чи місцях), окремими об'єктами (режими заповідників, вогнепальної зброї, отруйних речовин тощо), видами діяльності (режими оперативно-розшукової діяльності, окремих видів підприємницької діяльності та ін).*

Д. Н. Бахрах виділяє найбільш загальні, універсальні режими і похідні від них — вторинні режими. Він розрізняє їх за *територіальним критерієм*, детально розглядає загальнодержавні спеціальні режими, режими забезпечення законності, режими надзвичайного, воєнного, особливого положення, режими таємності, загальні й особливі митні режими, прикордонний режим і регіональні режими (закритого адміністративного утворення тощо); за терміном дії виділяє постійні та тимчасові ситуаційні режими (надзвичайного положення), розмежовує також режими за об'єктом, засобами діяльності (заповідників, отрут, валюти тощо) [117, с. 201–237].

І. С. Розанов пропонує поділити адміністративно-правові режими на п'ять груп. Так, до першої групи він відносить режими, спеціально націлені на забезпечення інтересів державної безпеки країни: адміністративно-правові режими захисту державної таємниці, прикордонний режим, режим в'їзду і виїзду із країни. Заходи цих режимів спрямовані на усунення причин і перекриття каналів витоку таємних відомостей з сфери, яка охороняється, на недоторканність та належну охорону державного кордону, на недопущення на територію країни членів терористичних та інших злочинних організацій. До другої групи входять режими, які передбачають рівною мірою інтереси забезпечення безпеки держави та охорони громадського порядку. Типовими представниками цього виду режиму є адміністративно-правовий режим проживання і пересування іноземців територією країни,

а також режим забезпечення безпеки цивільної авіації від актів незаконного втручання. Третя група режимів встановлюється переважно з метою охорони громадського порядку. До неї входять режими, що належать до так званої дозвільної системи (порядок придбання, збереження, використання вогнепальної зброї, вибухових речовин, радіоактивних ізотопів, отрути, отрутохімікатів, наркотичних препаратів та ін.), паспортна система тощо. Четверту групу складають адміністративно-правові режими, які сприяють досягненню мети та завдань інших галузей управління, а також окремі режимні заходи щодо забезпечення зовнішньої і внутрішньої безпеки (митний режим, санітарний режим та ін.). До останньої, п'ятої групи, відносяться комплексні режими, що мають на меті збереження обороноздатності країни, державної безпеки, громадського порядку, здоров'я і безпеки громадян в умовах настання виняткових обставин (воєнна загроза, стихійні лиха, епідемії, епізоотії, масові безпорядки та ін.). Такими режимами, які вирішують комплексні завдання, є правовий режим надзвичайного стану та режим воєнного стану [97, с. 87–88].

Ю. А. Тихомиров пропонує класифікувати адміністративно-правові режими *залежно від їх мети*: адміністративно-правові режими забезпечення стабільності держави; адміністративно-правові режими, що покликані забезпечувати функції управління і сфери діяльності (податковий, санітарний тощо); адміністративно-правові режими для громадян (реалізація прав громадян на охорону здоров'я, оплати праці, охорону праці та техніку безпеки, права на підприємницьку діяльність тощо); обліково-легалізуючі режими (державна реєстрація фізичних та юридичних осіб, реєстрація правочинів з нерухомістю, реєстрація зброї, ліцензування підприємницької діяльності); адміністративно-функціональні режими [102, с. 404–440].

Аналіз вищезазначених критеріїв класифікації адміністративно-правових режимів, а також їх види, отримані внаслідок аналізу надає можливість дійти висновку про деяку суперечність. Зокрема, адміністративно-правовий режим захисту державної таємниці не можна за запропонованими критеріями віднести до конкретного виду адміністративно-правового режиму, оскільки внаслідок його порушення завдається шкода не лише інтересам держави, а й національним інтересам загалом.

Таким чином, ми не зовсім згодні із позицією, наприклад, І. С. Розанова, який до першої групи відносить режими, спеціально націлені

переважно на забезпечення інтересів державної безпеки країни, де виділяє адміністративно-правовий режим захисту державної таємниці, а до другої — режими, які передбачають рівною мірою інтереси забезпечення безпеки держави та охорони громадського порядку.

Тим більше, що порушником цього режиму є не тільки іноземні служби чи іноземці, а й громадяни України, які внаслідок, наприклад, необережності сприяли порушенню встановлених правил захисту державної таємниці та розголошенню відповідної інформації. Таким чином, доречно говорити про адміністративно-правовий режим захисту інформації з обмеженим доступом, в рамках якого слід виділяти вже адміністративно-правовий режим захисту державної таємниці.

У цілому запропоновані різними авторами класифікації адміністративно-правових режимів, незважаючи на свою відмінність, не вступають у протиріччя, а навпаки взаємодоповнюють одна одну. Більше того, для всебічного й обґрунтованого визначення конкретного адміністративно-правового режиму, на нашу думку, найбільш доречним є використання інтегративного підходу.

### ***Класифікація адміністративно-правового режиму інформації з обмеженим доступом***

Зважаючи на окреслені вище підходи щодо класифікації адміністративно-правових режимів та, екстраполюючи їх на предмет дослідження, а також норми законів України «Про інформацію», «Про захист публічної інформації», де виокремлено види інформації з обмеженим доступом, вважаємо, що адміністративно-правовий режим інформації з обмеженим доступом можна класифікувати таким чином:

- 1) *адміністративно-правовий режим таємної інформації;*
- 2) *адміністративно-правовий режим конфіденційної інформації;*
- 3) *адміністративно-правовий режим службової інформації.*

Кожен з цих адміністративно-правових режимів, своєю чергою, може бути також поділено на підкласи. Так, адміністративно-правовий режим таємної інформації може бути класифіковано на:

- *адміністративно-правовий режим державної таємниці;*
- *адміністративно-правовий режим банківської таємниці;*
- *адміністративно-правовий режим професійної таємниці;*
- *адміністративно-правовий режим таємниці слідства тощо.*



### 3.2 ХАРАКТЕРИСТИКА ЕЛЕМЕНТІВ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ

Здебільшого в наукових розвідках з адміністративного права зауважується, що зміст кожного адміністративно-правового режиму розкривається через характеристику його елементів. Тому розгляд елементів адміністративно-правового режиму інформації з обмеженим доступом в Україні сприятиме всебічному та об'єктивному розкриттю предмета дослідження.

Наскільки дискусійними є питання визначення поняття «режим», «правовий режим», «адміністративно-правовий режим», настільки дискусійні й позиції адміністративістів щодо структури (елементів) адміністративно-правових режимів.

#### *Підходи щодо розуміння структури адміністративного режиму*

Однією із ознак адміністративно-правового режиму інформації з обмеженим доступом є те, що він здійснюється за допомогою відповідної системи різноманітних спеціальних засобів.

*Система спеціальних засобів*, що застосовуються для регулювання суспільних відносин у межах певних адміністративно-правових режимів, детально була окреслена Ю. А. Тихомировим. Так, дослідник до таких засобів відносить:

- 1) правові акти та норми, що встановлюють особливий порядок діяльності у тих або інших сферах;
- 2) уповноважені державні органи, що спеціально створені або наділені повноваженнями формувати та підтримувати відповідний режим;
- 3) детальну «операційну» регламентацію дій суб'єктів права та їх взаємовідносин;
- 4) систему контролю та відповідальності за діяльністю у межах адміністративно-правового режиму;
- 5) більш широке використання обмежено-дозвільних та заборонних методів, які у необхідних випадках поєднуються з чітко визначеним цільовим стимулюванням суб'єктів права;



б) наявність спеціальних організаційних, технічних, матеріальних і фінансових засобів (техніки, ресурсів тощо) [109, с. 401–402].

На думку Ю. П. Битяка та Б. Я. Бляхмана, до **основних елементів адміністративно-правових режимів** слід відносити:

- 1) метод правового регулювання, який в адміністративному праві побудований на централізованому способі та імперативно-му типі регулювання і відображається в юридичній нерівності суб'єктів правовідносин;
- 2) особливі адміністративно-правові способи встановлення та форми виникнення прав та обов'язків, способи юридичного впливу, захисту прав, процедурно-процесуальні форми та ін.;
- 3) принципи адміністративного права;
- 4) адміністративне законодавство, що характеризується наявністю великої кількості правових норм, які регулюють різноманітні соціальні відносини, пов'язані з державним управлінням [99, с. 277; 118, с. 40].

Інші фахівці з адміністративного права зазначають, що до **основних елементів адміністративно-правових режимів належить**, передусім, мета встановлення правового режиму, правові принципи, об'єкт адміністративно-правового регулювання, метод правового регулювання, «режимні правила», спеціальні державні органи, відповідальність за порушення «режимних норм», визначення просторово-часових меж дії адміністративно-правових режимів [104, 105].

**Зроблений нами аналіз деяких чинних нормативно-правових актів України, які встановлюють різні види правового режиму, надав можливість дійти висновку, що здебільшого певний правовий режим розкривається через визначення мети, правових основ, організаційно-функціональної структури органів державної влади, інших інституцій, а також правового статусу громадянам в умовах цього режиму, відповідальності за порушення «режимних норм», просторово-часових меж дії правового режиму.**

Так, у Законі України «Про правовий режим воєнного стану» закріплено, що «цей Закон визначає зміст правового режиму воєнного стану (порядок його введення та скасування, правові засади діяльності органів державної влади, військового командування, органів місцевого самоврядування, підприємств, установ та організацій в умовах воєнного стану, гарантії прав і свобод людини і громадянина та прав і закон-

них інтересів юридичних осіб) та відповідальність за порушення вимог або невиконання заходів правового режиму воєнного стану» [75].

У Законі України «Про правовий режим надзвичайного стану» також зазначається, що «цей Закон визначає зміст правового режиму надзвичайного стану, порядок його введення та припинення дії, особливості діяльності органів державної влади та органів місцевого самоврядування, підприємств, установ і організацій в умовах надзвичайного стану, додержання прав і свобод людини і громадянина, а також прав і законних інтересів юридичних осіб та відповідальність за порушення вимог або невиконання заходів правового режиму надзвичайного стану» [76].

Таким чином, саме друга позиція, на нашу думку, найбільш повно відображає елементний склад адміністративно-правового режиму, а тому буде використана нами задля окреслення специфіки адміністративно-правового режиму інформації з обмеженим доступом.

Отже, розглянемо детальніше кожен із елементів адміністративно-правового режиму (мета встановлення правового режиму, правові принципи, об'єкт адміністративно-правового регулювання, метод правового регулювання, «режимні правила», спеціальні державні органи, відповідальність за порушення «режимних норм», визначення просторово-часових меж дії адміністративно-правових режимів), екстраполюючи на специфіку предмета дослідження.

### ***Мета адміністративно-правового режиму інформації з обмеженим доступом***

У літературі з адміністративного права здебільшого зазначається, що єдиною метою для всіх адміністративно-правових режимів є забезпечення загальної безпеки в державі [85, с. 270].

Але виникають запитання на кшталт: що таке «загальна безпека в державі», як вона співвідноситься з національною безпекою, чи всі адміністративно-правові режими опосередковані цією метою.

Не менш дискусійною, на нашу думку, є позиція І. С. Розанова, який під загальною метою і основним призначенням адміністративно-правових режимів розуміє створення на шляху іноземних розвідок, злочинних організацій і осіб надійних правових бар'єрів та розроблення організаційних заходів для забезпечення останніх, які б серйозно

ускладнювали, а то й унеможливлювали досягнення злочинної мети у сфері зовнішньої і внутрішньої безпеки [97, с. 86].

Такий підхід значно звужує поняття адміністративно-правового режиму, оскільки віддзеркалює радянську парадигму адміністративно-права як винятково каральний інститут. На сучасному етапі розвитку адміністративної науки роль та мета цієї галузі значно розширились: від каральної до обслуговуючої.

У цьому контексті більш адекватною новітнім реаліям є думка В. Б. Рушайла про те, що адміністративно-правовий режим встановлюються з метою забезпечення взаємодії державної адміністрації і приватних осіб на основі права, оскільки він супроводжує діяльність органів і посадових осіб державної адміністрації при їх взаємодії з громадянами й організаціями, а також між її ланками при реалізації ними своїх функціональних обов'язків та регулюванні різноманітних соціальних об'єктів і процесів [98, с. 28].

На нашу ж думку, більш прийнятно говорити не просто про взаємодію державної адміністрації і приватних осіб, а про співробітництво між ними, оскільки введення певного режиму визначає правові засади функціонування органів державної влади чи інших уповноважених державою інституцій, а також конкретних осіб шляхом окреслення взаємних прав і обов'язків.

Крім того, як слушно зауважує С. О. Магда, аналізуючи позицію В. Б. Рушайла, «все ж з поля зору дослідника випадає один із найбільш важливих, на наш погляд, аспектів цього поняття. Мова йде про те, що запровадження та реалізація адміністративно-правових режимів пов'язані не лише з забезпеченням загальної безпеки та взаємодії державної адміністрації та приватних осіб. Термін «взаємодія» характеризує лише один аспект взаємовідносин органів держави та громадян і більшою мірою пов'язаний зі сприянням останнім в реалізації їх прав і свобод. Але при цьому слід мати на увазі, що для громадян важлива не тільки належна реалізація відповідних прав і свобод, а й їх реальний захист та поновлення, що є суттєвою обставиною при визначенні мети встановлення адміністративно-правових режимів» [105, с. 102].

Використання державою адміністративно-правових режимів різного роду інформації з обмеженим доступом не має на меті порушення права на інформацію, що закріплене Конституцією України. Однак їх (режимів) запровадження призводить до певного «порушення» цього

права через необхідність пошуку балансу з іншими конституційними правами (право на невтручання в особисте і сімейне життя (ст. 32 Конституції України), таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31 Конституції України) та інші).

Таким чином держава, встановлюючи необхідність обмежень права на інформацію за допомогою адміністративно-правових режимів, забезпечує реалізацію інших, не менш важливих конституційних прав.

Отже, враховуючи вищевикладені зауваження, вважаємо, що *метою будь-якого адміністративно-правового режиму* є забезпечення співробітництва державної адміністрації і окремих осіб у відповідній сфері задля повнішої реалізації прав і свобод, а також дієвого захисту і поновлення у разі їх порушення. *Метою ж адміністративно-правового режиму інформації з обмеженим доступом* є забезпечення співробітництва державної адміністрації і окремих осіб у сфері захисту інформації з обмеженим доступом задля задоволення національних інтересів держави та суспільства, повнішої реалізації громадянами інформаційних прав і свобод у цій сфері, а також дієвого захисту і поновлення у разі їх порушення.

### ***Правові принципи адміністративно-правового режиму інформації з обмеженим доступом***

Правові принципи як елемент адміністративно-правового режиму широко розглядається багатьма науковцями [119, с. 76].

Принципи ж адміністративно-правового режиму інформації з обмеженим доступом детерміновані загальноправовими, а також галузевими принципами права, зокрема адміністративного й інформаційного. Крім того, в силу специфіки суспільних відносин у сфері інформації з обмеженим доступом обумовлюють формування деяких додаткових принципів права. У зв'язку з чим вважаємо за необхідне зупинитися саме на них.

Аналіз вітчизняної нормативної бази (Закон України «Про інформацію», Закон України «Про державну таємницю» тощо) у цій сфері надав можливість дійти висновку, що на законодавчому рівні не було закріплено принципів як інформаційних відносин загалом, так і в окремих сферах, зокрема, у сфері інформації з обмеженим доступом. Хоча, як відомо, принципи — це висхідні ідеї, основоположні засади, на яких

формується відповідне правове поле, правове регулювання відповідних суспільних відносин.

У цьому контексті вважаємо конструктивним досвід Російської Федерації, яка в концептуальному нормативно-правовому акті, що регулює суспільні відносини в інформаційній сфері, — Законі РФ «Про інформацію, інформаційні технології і про захист інформації» від 27 липня 2006 року — закріпила принципи правового регулювання відносин у сфері інформації, інформаційних технологій і захисту інформації, зокрема:

- 1) свободі пошуку, отримання, передачі, виробництва і розповсюдження інформації будь-яким законним способом;
- 2) встановлення обмежень доступу до інформації лише федеральними законами;
- 3) відкритість інформації о діяльності державних органів і органів місцевого самоврядування і вільний доступ до такої інформації, крім випадків, встановлених федеральними законами;
- 4) рівноправність мов народів Російської Федерації при створенні інформаційних систем і їх експлуатації;
- 5) забезпечення безпеки Російської Федерації при створенні інформаційних систем, їх експлуатації і захисту інформації, що в них міститься;
- 6) достовірність інформації і своєчасність її надання;
- 7) недоторканність приватного життя, неприпустимість збирання, зберігання, використання і розповсюдження інформації про приватне життя особи без її згоди;
- 8) неприпустимість встановлення нормативними актами будь-яких переваг застосування одних інформаційних технологій щодо інших, якщо лише обов'язковість застосування конкретних інформаційних технологій для створення і експлуатації державних інформаційних систем не встановлена федеральними законами [67].

Не менш конструктивним для запозичення українським законодавцем є закріплення на рівні федерального закону і принципів забезпечення доступу до інформації, зокрема до інформації про діяльність державних органів і органів місцевого самоврядування.

Так, Закон РФ «Про забезпечення доступу до інформації про діяльність державних органів і органів місцевого самоврядування» від 9 лю-

того 2009 року встановив, що основними принципами забезпечення доступу до інформації про діяльність державних органів і органів місцевого самоврядування є відкритість, доступність, достовірність інформації про діяльність державних органів і органів місцевого самоврядування, своєчасність її надання, свобода пошуку, отримання, передачі та розповсюдження інформації про діяльність державних органів і органів місцевого самоврядування будь-яким законним способом, а також додержання прав громадян на недоторканність приватного життя, особисту і сімейну таємницю, захист їх честі і ділової репутації, права організацій на захист їх ділової репутації при наданні інформації про діяльність державних органів і органів місцевого самоврядування [120].

Щодо України, то лише з прийняттям Закону України «Про доступ до публічної інформації» в 2011 році та, як наслідок, затвердження нової редакції Закону України «Про інформацію» така прогалина знайшла своє нормативне заповнення.

Зокрема у ст. 2 нової редакції Закону України «Про інформацію» закріплено, що основними принципами інформаційних відносин є:

- гарантованість права на інформацію;
- відкритість, доступність інформації, свобода обміну інформацією;
- достовірність і повнота інформації;
- свобода вираження поглядів і переконань;
- правомірність одержання, використання, поширення, зберігання та захисту інформації;
- захищеність особи від втручання в її особисте та сімейне життя [39].

У ст. 4 Закону України «Про доступ до публічної інформації» затверджено, що доступ до публічної інформації відповідно до цього Закону здійснюється на принципах:

- 1) прозорості та відкритості діяльності суб'єктів владних повноважень;
- 2) вільного отримання та поширення інформації, крім обмежень, встановлених законом;
- 3) рівноправності, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак [59].



Екстраполюючи нормативно закріплені принципи на предмет дослідження, а також зважаючи на загально визнані принципи адміністративного права як-от: ієрархічність побудови суб'єктів адміністративного права та їх відносин, підзаконність діяльності, функціонально-спеціалізований характер діяльності, участь громадян та їх об'єднань у державному управлінні, здійснення владних повноважень професійним, спеціально створеним апаратом і його службовцями [109, с. 72], можна виділити такий *основний принцип адміністративно-правового регулювання відносин у сфері інформації з обмеженим доступом (адміністративно-правовий режим інформації з обмеженим доступом)*: баланс між прозорістю (відкритістю, прозорістю) діяльності органів державної влади й органів місцевого самоврядування, свободою пошуку, отримання, передачі, виробництва і розповсюдження відкритої інформації будь-яким законним способом, крім закріплених на законодавчому рівні обмежень, з метою забезпечення національної безпеки особи, суспільства і держави, тобто принцип паритету прозорості безпеки з безпечною прозорістю.

***Отже, принципи адміністративно-правового режиму інформації з обмеженим доступом — це висхідні ідеї, основоположні засади, на яких ґрунтується захист інформації з обмеженим доступом у конкретній країні.***

### ***Об'єкт адміністративно-правового режиму інформації з обмеженим доступом***

Об'єкт режиму охоплює тільки ті відносини у сфері інформації з обмеженим доступом, які фактично потрапили під дію адміністративно-правових норм.

Режим інформації з обмеженим доступом здійснюється з позиції адміністративного права, тобто в контексті реалізації функцій виконавчої влади з метою упорядкування суспільних відносин, що виникають у сфері інформації з обмеженим доступом як об'єкта адміністративно-правового регулювання. Щодо розгляду цих самих суспільних відносин з позиції цивільного, кримінального чи інших галузей права, то він буде мати зовсім інше забарвлення, обумовлене специфікою конкретної галузі права.



Приватноправові відносини у сфері інформації з обмеженим доступом (інтелектуальна власність, комерційна таємниця, ноу-хау і т.д.) не являють собою об'єкта адміністративно-правового режиму інформації з обмеженим доступом, оскільки становлять об'єкт, насамперед, цивільно-правового режиму.

На цю обставину звертали увагу й інші дослідники, які зауважували, що «відомі випадки, коли у сферу впливу режиму потрапляли приватноправові за характером відносини (власності, договірні зобов'язання), що призводило до зміни їх внутрішнього змісту» [98, с. 31–32].

«При цьому деякі цивільно-правові можливості (які надаються суб'єкту цивільним правом) можуть бути поглинуті відповідними заборонами, які встановлені, наприклад, засобами адміністративного або кримінального права. Таким чином, можливою є ситуація застосування цивільно-правових способів захисту проти необґрунтовано (з точки зору цивільного права) встановлених адміністративних заборон, кримінально-правових обмежень та ін.» [30, с. 18].

Користуючись нормативно закріпленою термінологією (Закон України «Про доступ до публічної інформації»), вважаємо, що *введення адміністративно-правового режиму інформації з обмеженим доступом спрямовано на врегулювання насамперед відносин у зв'язку з необхідністю реалізації права на інформацію та захистом національних інтересів між різного роду запитувачами інформації (фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи) та розпорядниками інформації* відповідно до ст. 13 вищезгаданого Закону, серед яких:

- 1) суб'єкти владних повноважень – органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади Автономної Республіки Крим, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання;
- 2) юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим, – стосовно інформації щодо використання бюджетних коштів;
- 3) особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг, — стосовно інформації, пов'язаної з виконанням їхніх обов'язків;

- 4) суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями, – стосовно інформації щодо умов постачання товарів, послуг та цін на них [59].

### ***Метод адміністративно-правового режиму інформації з обмеженим доступом***

Здебільшого метод адміністративно-правового регулювання визначають як головний елемент адміністративно-правового режиму. Як відомо, характерним для адміністративного права методом є імперативний, який ґрунтується на засадах панування й підкорення.

У цьому контексті лише зазначимо, що ми підтримуємо зауваження В. Б. Рушайла, що недостатньо говорити лише про відносини «влада — підпорядкування», адже зміст адміністративно-правових відносин набагато різноманітніший, а субординація, що їх складає, реалізується за допомогою різних юридичних прийомів: безпосередній (прямий) наказ – існує у відносинах організаційної підпорядкованості (керівник – підлеглий); функціональне зобов'язання, характерне для відносин юридичної підконтрольності (інспектор – контрольований); координаційне зобов'язання, що існує у відносинах між органами виконавчої влади, які здійснюють міжгалузеву координацію і регулювання не підлеглими їм органами виконавчої влади; дозвільний припис, що існує при реалізації невідладними суб'єктами прав і свобод, пов'язаних із забезпеченням безпеки, а також при отриманні ними різного роду ліцензій для зайняття певними видами діяльності; обов'язкове узгодження, що існує у випадках, коли виникає необхідність прийняття суб'єктами управління спільного рішення та ін. Адміністративно-правовий режим передбачає і дозвільний тип правового регулювання, що стосується здійснення громадянами певних конституційних прав у сфері управління. Їм кореспондує обов'язок державних органів забезпечити для цього належні умови [98, с. 32–33].

**«Режимні правила» адміністративно-правового режиму інформації з обмеженим доступом**

Основним елементом будь-якого адміністративно-правового режиму є «режимні правила».

Погоджуємось з позицією С. О. Магди, яка визначила «режимні правила» як встановлену в законодавчому порядку сукупність правил діяльності, дій або поведінки громадян, юридичних осіб, а також державних органів, їх посадових осіб та реалізацію ними своїх прав у певних ситуаціях (умовах) [105, с. 111]. Лише додамо, що, по-перше, така діяльність встановлена в законодавчому порядку, що охоплює не лише закони, а й підзаконні нормативно-правові акти. Тим більше зважаючи на те, що адміністративно-правовий режим захисту інформації з обмеженим доступом здебільшого урегульовано на рівні підзаконних нормативно-правових актів.

По-друге, дії є складовою частиною діяльності.

По-третє, доречніше говорити не лише про громадян, юридичних осіб, а також державні органи, їх посадових осіб, але розширити це коло суб'єктів до фізичних і юридичних осіб, оскільки особи без громадянства, особи з подвійним громадянством, іноземці відповідно до вітчизняного законодавства мають право доступу до певного виду інформації.

Так, у ст. 12 Закону України «Про доступ до публічної інформації» серед суб'єктів відносин у сфері доступу до публічної інформації є запитувачі інформації — фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи [59].

По-четверте, режимні правила встановлюють не лише порядок реалізації своїх прав, а й закріплюють свободи й обов'язки.

Отже, під **режимними правилами як елемента адміністративно-правового режиму слід розуміти встановлену в законодавчому порядку сукупність правил діяльності юридичних осіб, а також державних органів їх посадових чи службових осіб або поведінки фізичних осіб та реалізація ними своїх прав, свобод та обов'язків у чітко визначених ситуаціях (умовах).**

Чітка правова регламентація порядку соціальної діяльності в режимних сферах є важливою гарантією законності при запровадженні будь-якого адміністративно-правового режиму [85, с. 249].

*Серед основних правил адміністративно-правового режиму інформації з обмеженим доступом слід виділити такі:*

- обґрунтування про необхідність віднесення інформації до інформації з обмеженим доступом шляхом окреслення можливої шкоди від її розголошення національній безпеці, інтересам окремих громадян, суспільству;
- визначення відомостей, які не можуть бути віднесені до інформації з обмеженим доступом;
- віднесення відомостей до інформації з обмеженим доступом, тобто прийняття рішення про віднесення категорії відомостей або окремих відомостей до інформації з обмеженим доступом з установами її виду;
- окреслення прав, свобод і обов'язків учасників правовідносин у зв'язку з доступом до інформації з обмеженим доступом;
- визначення правового статусу органів державної влади у сфері захисту інформації з обмеженим доступом;
- визначення системи контролю і нагляду за виконанням режимних вимог фізичними, юридичними, а також посадовими особами тощо.

До системи контролю і нагляду за виконанням режимних вимог відноситься суцільна і вибіркова перевірка дотримання правил, оперативно-розшукові заходи, заходи припинення та заходи відповідальності; організаційно-технічне забезпечення встановлених режимних правил, які надають можливість ефективно попереджувати, виявляти і припиняти їх порушення (використання транспортних засобів, засобів зв'язку, спеціального устаткування) [96, с. 484–485].

Лише враховуючи вид інформації з обмеженим доступом, компетентний орган чи інший зацікавлений суб'єкт (розпорядник інформації) повинен обрати саме той юридичний інструментарій, за допомогою якого буде досягнута стабілізація обстановки [115, с. 26].

Таким чином, *режимні правила адміністративно-правового режиму інформації з обмеженим доступом здебільшого знаходять свій прояв у визначенні правового становища інформації з обмеженим доступом як виду інформації; створення спеціальних постійних або тимчасових органів, наділених компетенцією з підтримки режиму, або наділення компетенцією з підтримки режиму вже існуючих органів, на які покладаються обов'язки із застосування адміністра-*

*тивних заходів для забезпечення дотримання режимних правил, контролювання процесу реалізації прав і обов'язків іншими учасниками та його корекції у випадку відхилення від встановлених вимог; закріплення порядку отримання фізичними чи юридичними особами доступу до інформації з обмеженим доступом, порядку користування такою інформацією, переліку прав і обов'язків поводження з такою інформацією.*

### **Спеціальні державні органи як елемент адміністративно-правового режиму інформації з обмеженим доступом**

Не менш важливим елементом адміністративно-правового режиму інформації з обмеженим доступом є визначення спеціальних державних органів, основним завданням яких є забезпечення реалізації мети адміністративно-правового режиму.

Щодо конкретного адміністративно-правового режиму, то ці органи наділені відповідними повноваженнями, зумовленими правом здійснювати контроль за додержанням режимних правил в охоронюваній сфері, причому дуже важливо, щоб коло прав, якими наділені відповідні державні органи, кореспондувалося з відповідними обов'язками і певною відповідальністю за свої дії [121, с. 271–272].

Зважаючи на те, що адміністративно-правовий режим інформації з обмеженим доступом має певну специфіку, що знаходить свій прояв у тому, що обов'язки щодо захисту інформації покладаються не лише на державні органи, а й на широке коло інших суб'єктів адміністративного права, то доцільним буде з'ясування саме кола суб'єктів забезпечення захисту інформації з обмеженим доступом.

Так, В. К. Колпаков та О. В. Кузьменко розрізняють такі види суб'єктів адміністративного права:

- а) Президент України;
- б) органи виконавчої влади;
- в) державі службовці як суб'єкти, у діяльності яких об'єктивуються повноваження державних органів управління;
- г) громадяни України, іноземці, особи без громадянства;
- г) органи місцевого самоврядування;
- д) об'єднання громадян;

е) суб'єкти підприємницької діяльності [122, с. 117].

Інші фахівці адміністративного права виокремлюють такі основні види суб'єктів адміністративного права:

- фізичні особи — громадяни України, іноземці, особи без громадянства;
- юридичні особи — органи виконавчої влади, будь-які інші державні органи, органи місцевого самоврядування, об'єднання громадян, підприємства, установи, організації (в особі їх керівників, які очолюють органи управління цих підприємств, установ, організацій);
- колективні суб'єкти (управління), які не мають ознак юридичної особи, але тією чи іншою мірою наділені нормами адміністративного права певними правами й обов'язками: структурні підрозділи державних і недержавних органів підприємств, установ, організацій, деякі інші громадські утворення (на кшталт загальних зборів громадян за місцем проживання) [104, с. 185].

Відаючи належне наведеним позиціям, С. Г. Стеценком пропонується дещо інший варіант класифікації суб'єктів адміністративного права на два види за критерієм кількісного показника у поєднанні з мірою належності до держави, а саме:

1) індивідуальні:

- громадяни України;
- іноземці;
- особи без громадянства;

2) колективні:

а) державні:

- Президент України;
- органи виконавчої влади;
- інші державні органи та організації;

б) недержавні:

- органи місцевого самоврядування;
- об'єднання громадян;
- релігійні організації;
- інші недержавні органи та організації [123, с. 92].

Отже, враховуючи вищезазначені класифікації суб'єктів адміністративного права та екстраполюючи норми нормативно-правових актів, що регулюють суспільні відносини у сфері захисту інформації з об-

меженим доступом, вважаємо за необхідне визначити таких *суб'єктів захисту інформації з обмеженим доступом*:

- 1) державні інституції:
  - Президент України;
  - Верховна Рада України;
  - Рада національної безпеки і оборони України;
  - органи виконавчої влади;
  - інші державні органи та організації;
- 2) недержавні інституції:
  - органи місцевого самоврядування;
  - об'єднання громадян;
  - інші недержавні інституції;
- 3) фізичні особи:
  - громадяни України;
  - іноземці;
  - особи без громадянства.

**Коло суб'єктів захисту інформації з обмеженим доступом в Україні являє собою багаторівневу систему, в якій суб'єкти об'єднані спільною метою, але мають при цьому різні повноваження, можливості, засоби тощо.**

**При чому суб'єктами адміністративно-правового режиму конфіденційної інформації може бути фізична або юридична особа, яким належить така інформація, чи за їх уповноваженням будь-хто з розпорядників.**

**Суб'єктами адміністративно-правового режиму таємної інформації є здебільшого державні та недержавні інституції.**

Так, у ст. 37 Закону України «Про державну таємницю» від 21 січня 1994 року закріплено, що керівники державних органів, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль за забезпеченням охорони державної таємниці [40].

Хоча згідно зі ст. 3 цього ж Закону: «Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші державні органи, Верховну Раду Автономної Республіки Крим, Раду міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі — державні органи, орга-



ни місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці» [40].

Слід також зауважити, що нині на законодавчому рівні відсутній механізм співробітництва громадських об'єднань і державних органів у сфері інформації з обмеженим доступом. Хоча законодавець закріпив у Законі України «Про участь громадян в охороні громадського порядку і державного кордону» [124] механізм співробітництва громадських об'єднань (окремих громадян) з державними інституціями щодо охорони громадського порядку і державного кордону.

З цього приводу доволі влучно зауважив Б. А. Кормич, що необхідно у законодавчих актах, присвячених проблемам національної безпеки та захисту інформації та інформаційної інфраструктури розробити сам механізм співпраці громадських об'єднань в напрямі захисту інформаційної безпеки [10, с. 181].

Встановлення ж на законодавчому рівні механізму співробітництва громадських об'єднань і державних органів у сфері інформації з обмеженим доступом дозволило б першим брати участь у захисті інформації з обмеженим доступом України разом з іншими суб'єктами; вживати заходів спільно з іншими суб'єктами по припиненню адміністративних правопорушень і злочинів, що мають інформаційний характер; взаємодіяти з іншими органами громадської самодіяльності, що беруть участь у заходах, спрямованих на ведення індивідуально-профілактичної роботи з особами, схильними до вчинення адміністративних правопорушень і злочинів, що мають інформаційний характер; вносити до органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, незалежно від форм власності, пропозиції щодо запобігання адміністративним правопорушенням і злочинам інформаційного характеру, виникненню причини і умов, що сприяють їх вчиненню; підтримувати зв'язки з відповідними громадськими організаціями інших країн з метою обміну досвідом роботи у сфері захисту інформації з обмеженим доступом.

Де-факто: найбільш дієвим суб'єктом захисту інформації з обмеженим доступом є державні інституції. Коло цих суб'єктів є доволі значним, а саме:

- 1) Верховна Рада України;
- 2) Президент України;
- 3) Кабінет Міністрів України;
- 4) Рада національної безпеки і оборони України;
- 5) міністерства, державні комітети, інші центральні органи виконавчої влади, а також спеціально уповноважені органи державної влади, яким надані відповідні повноваження.

### ***Верховна Рада України як суб'єкт захисту інформації з обмеженим доступом***

Верховна Рада України як суб'єкт захисту інформації з обмеженим доступом має кадрові, законодавчі та контрольні повноваження.

Конкретизація конституційних повноважень Верховної Ради України як суб'єкта захисту інформації з обмеженим доступом знаходить своє відображення в Законі України «Про комітети Верховної Ради України», де в розділах 2 і 3 чітко визначено функції комітетів ВР України (законопроектна, організаційна, контрольна) та їх права і обов'язки при здійсненні законопроектної, організаційної, контрольної функцій.

Відповідно до ст. 1 цього нормативно-правового акта для здійснення за окремими напрямками законопроектної роботи, підготовки і попереднього розгляду питань, віднесених до повноважень Верховної Ради України, виконання контрольних функцій, Верховна Рада України з числа народних депутатів може утворювати відповідні комітети [125].

Дослідження системи комітетів Верховної Ради України дає змогу визначити, що окремі аспекти захисту інформації з обмеженим доступом є предметом діяльності декількох комітетів ВР України: Комітету з питань національної безпеки і оборони, Комітету з питань свободи слова та інформації, Комітету з питань інформатизації та інформаційних технологій, а також Комітету з питань прав людини, національних меншин і міжнародних відносин.

Відповідно до Постанови Верховної Ради України від 25 грудня 2012 року<sup>47</sup> до предметів відання Комітету з питань національної безпеки і оборони віднесені:

- національна безпека України;
- законодавче забезпечення діяльності органів служби безпеки, розвідки і контррозвідки, органів прикордонної служби, захист державної таємниці (Підкреслено нами. — Авт.);
- правовий режим державного кордону, воєнного та надзвичайного станів;
- оборонно-промисловий комплекс, державна система страхового фонду документації, військово та військово-технічне співробітництво України з іншими державами, а також участь України в міжнародних миротворчих операціях;
- державна політика у сфері оборони;
- боротьба з тероризмом;
- здійснення цивільного, у тому числі парламентського контролю над Воєнною організацією держави;
- військова служба, Збройні сили України та їх реформування;
- військові формування, утворені відповідно до законів України;
- альтернативна (невійськова) служба;
- соціальний і правовий захист військовослужбовців та членів їх сімей;
- військова наука та освіта.

У межах цього Комітету виділено ряд підкомітетів, серед яких:

- Підкомітет з питань воєнної безпеки та оборони;
- Підкомітет з питань оборонно-промислового комплексу та військово-технічного співробітництва;
- Підкомітет з питань соціального і правового захисту військовослужбовців та членів їх сімей;
- Підкомітет з питань державної безпеки;
- Підкомітет з питань інформаційної безпеки.

До останнього Підкомітету, своєю чергою віднесені такі питання, як:

- інформаційна безпека держави;
- кібернетична безпека держави;

<sup>47</sup> Про комітети Верховної Ради України сьомого скликання [Електронний ресурс] : постан. Верховної Ради України від 25 груд. 2012 р. — Режим доступу : <http://komnbo.rada.gov.ua>.

- захист інформацій в інформаційно-телекомунікаційних системах;
- спеціальний зв'язок держави;
- національна система конфіденційного зв'язку України;
- електронний цифровий підпис;
- національний інформаційний простір та протидія його монополізації;
- право власності держави на стратегічні об'єкти інформаційної інфраструктури;
- інформація з обмеженим доступом, яка є власністю держави та її захист (Підкреслено нами. — Авт.);
- фінансування сфер інформаційної та кібернетичної безпеки держави;
- фінансування потреб, спрямованих на заміну застарілих та зношених зразків спеціальної техніки, термін яких перевищує 20 років;
- наука та підготовка кадрів у сфері інформаційної, кібернетичної безпеки та спеціального зв'язку;
- практика застосування центральними органами виконавчої влади нормативно-правових актів на виконання положень законів у сфері інформаційної безпеки;
- здійснення парламентського контролю за практикою застосування державними органами законодавства України у сфері відання підкомітету;
- вивчення та використання досвіду інших країн з питань законодавчого врегулювання проблем інформаційної та кібернетичної безпеки<sup>48</sup>.

*Комітет Верховної Ради України з питань свободи слова та інформації* займається такими питаннями, як:

- державна політика у сфері інформації;
- свобода слова;
- права громадян на інформацію;
- друковані та електронні засоби масової інформації;
- висвітлення діяльності Верховної Ради України;

<sup>48</sup> Питання, віднесені до відання підкомітетів Комітету Верховної Ради України з питань національної безпеки і оборони [Електронний ресурс] : рішення Комітету Верховної Ради України, протокол № 2 від 09 січ. 2013 р. — Режим доступу : <http://komnbo.rada.gov.ua>.

- засади здійснення рекламної діяльності<sup>49</sup>.

У чому ж розмежування предмета відання цих комітетів? Вважаємо, що одним із аспектів інформаційної безпеки є безпека права на інформацію, що забезпечується шляхом неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за їхні політичні позиції тощо.

Отже, сфера діяльності підкомітету з питань інформаційної безпеки охоплює сферу діяльності Комітету з питань свободи слова та інформації, оскільки інформаційна безпека є поняттям ширшим за поняття права на інформацію чи свободи слова.

Щодо *Комітету з питань інформатизації та інформаційних технологій*, то до предмета його відання належить:

- Національна програма інформатизації;
- захист інформації та персональних даних в інформаційно-телекомунікаційних системах (Підкреслено нами. — Авт.);
- електронні документи та електронний документообіг;
- масові телекомунікації<sup>50</sup>.

*Комітет з питань прав людини, національних меншин і міжнаціональних відносин* має як предмет відання питання регулювання збирання і використання персональних даних про особу (крім захисту інформації та персональних даних в інформаційно-телекомунікаційних системах) (Підкреслено нами. — Авт.).

Отже, питання захисту інформації з обмеженим доступом є предметом відання кількох комітетів Верховної Ради України. Відсутність системного розгляду такої інформації може призводити до унеможливлення ефективного її захисту. Більше того, віднесення інформаційної проблематики до компетенції різних комітетів ускладнює реалізацію контрольних і законотворчих повноважень цих комітетів. Саме тому, на нашу думку, логічним було б розглядати питання Комітету з

<sup>49</sup> Про комітети Верховної Ради України сьомого скликання [Електронний ресурс] : постан. Верховної Ради України від 25 груд. 2012 р. — Режим доступу : <http://komnbo.rada.gov.ua>.

<sup>50</sup> Про виклики та загрози національній безпеці України у 2011 році [Електронний ресурс] : Рішення Ради національної безпеки і оборони України від 17 лист. 2010 р. — Режим доступу : <http://zakon2.rada.gov.ua>.

питань свободи слова та інформації, Комітету з питань інформатизації та інформаційних технологій, Комітету з питань прав людини, національних меншин і міжнародних відносин у рамках підкомітету з питань інформаційної безпеки.

Таким чином, Верховна Рада України як безпосередньо, так і за допомогою своїх органів у силу специфіки своїх повноважень є одним із важливих суб'єктів захисту інформації з обмеженим доступом, оскільки це єдина законодавча інституція в системі інших органів державної влади в Україні.

Деякі дослідники визнають законодавчий орган України головним суб'єктом забезпечення як національної безпеки, так і інформаційної (в межах якої слід виділяти інститут захисту інформації з обмеженим доступом) [10, с. 187]. Ми дану думку не поділяємо. І ось чому.

Справді, у Конституції України у ст. 92 сказано, що основи національної безпеки визначаються винятково законами України [126]. Проте в п. 1 ст. 106 Основного Закону вже визначено, що Президент України забезпечує національну безпеку, та згідно з ч.1 ст. 107 цього ж акта Рада національної безпеки і оборони України є координаційним органом з питань національної безпеки і оборони при Президентові України.

Контент-аналіз законодавства у сфері національної безпеки надає можливість дійти висновку, що найважливіші засади як національної, так і інформаційної безпеки урегульовані нормативно-правовими актами, затвердженими саме Президентом України, зокрема Стратегія національної безпеки України, Доктрина інформаційної безпеки України.

Більш того, в Законі України «Про основи національної безпеки України» визначено, що Стратегія національної безпеки України, Воєнна доктрина України, доктрини, концепції, стратегії і програми, якими визначаються цільові настанови та керівні принципи воєнного будівництва, а також напрями діяльності органів державної влади в конкретній обстановці з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз національним інтересам України розробляються і затверджуються Президентом України [51].

Отже, у зв'язку з колізійністю конституційних норм щодо визначення суб'єкта нормотворення у сфері національної безпеки на сьогодні норми Закону України «Про основи національної безпеки

України» є чинними та слугують правовим фундаментом для прийняття нормативно-правових актів, що регулюють суспільні відносини у сфері національної безпеки України, саме Президентом України.

### ***Президент України як суб'єкт захисту інформації з обмеженим доступом***

Повноваження Президента України закріплені в ст. 106 Конституції України. Норми цієї статті мають не тільки уповноважувальний, а й зобов'язувальний характер. Таким чином, Президент України має також необхідні правотворчі (видання указів і розпорядження, обов'язкові для виконання на території України), кадрові (утворює суди у визначеному законом порядку; створює у межах коштів, передбачених у Державному бюджеті України здійснення своїх повноважень, консультативні, дорадчі та інші допоміжні органи і служби; призначає на посади та звільняє з посад вище командування Збройних сил України, інших військових формувань; вносить до ВР України подання про призначення міністра оборони України, міністра закордонних справ України; призначає на посаду та звільняє з посади за згодою Верховної Ради України Генерального Прокурора України; призначає на посади та звільняє з посад половину особового складу Національної ради України з питань телебачення і радіомовлення; вносить до Верховної Ради України подання про призначення на посаду та звільнення з посади Голови Служби безпеки України тощо) та контрольні (зупиняє дію актів Кабінету Міністрів України з мотивів невідповідності Конституції з одночасним зверненням до Конституційного Суду України щодо їх конституційності; скасовує акти Ради Міністрів Автономної Республіки Крим; має право вето щодо прийнятих Верховною Радою України законів (крім законів про внесення змін до Конституції України) з наступним поверненням їх на повторний розгляд Верховної Ради України тощо) повноваження.

Як слушно зазначив Б. А. Кормич: «У руках Президента зосереджені ключові функції щодо організаційного забезпечення інформаційної безпеки» [10, с. 198].



У наукових колах доволі дискусійним залишається питання щодо адміністративно-правового статусу Президента України як суб'єкта забезпечення інформаційної безпеки.

Одні вчені [10, с. 194] визначають, що основне завдання Президента України — це загальне керівництво над іншими суб'єктами забезпечення інформаційної безпеки та забезпечення визначених Верховною Радою України внутрішніх і зовнішніх засад інформаційної безпеки, оскільки дані повноваження визначені в п. 17 ст. 106 Конституції України, відповідно до якого він здійснює керівництво у сферах національної безпеки та оборони держави, тобто і в інформаційній сфері, та в п. 1 ст. 106 Основного Закону, де чітко закріплено, що Президент України забезпечує національну безпеку (інформаційну безпеку).

Інші ж науковці [127, с. 124] стверджують, що Президент формує політику національної безпеки, визначає пріоритетні цілі, напрями забезпечення національної безпеки, а також сили, засоби тощо.

Ми підтримуємо думку останніх, оскільки, як зазначали раніше, конституційні норми в цьому контексті колізійні. Хоча нормотворча діяльність Президента України порівняно з нормотворчою діяльністю Верховної Ради України активніша. Саме тому, на нашу думку, Президент України як суб'єкт забезпечення інформаційної безпеки загалом та захисту інформації з обмеженим доступом зокрема визначає зовнішні та внутрішні засади інформаційної безпеки України, а також координує і контролює в силу специфіки своїх повноважень всі гілки влади, тобто діяльність інших суб'єктів захисту інформації з обмеженим доступом.

### ***Рада національної безпеки і оборони України (РНБО України) та Кабінет Міністрів України як суб'єкти захисту інформації з обмеженим доступом***

Координація та контроль діяльності органів виконавчої влади у сфері захисту інформації з обмеженим доступом здійснюється завдяки Раді національної безпеки і оборони України (РНБО України), головою якої є Президент України.

Правові засади організації та діяльності Ради національної безпеки і оборони України, її склад, структура, компетенція і функції закріпле-

ні в Законі України «Про Раду національної безпеки і оборони України» [128].

*Основними функціями Ради національної безпеки і оборони України є:*

- 1) внесення пропозицій Президентові України щодо реалізації за-  
сад внутрішньої і зовнішньої політики у сфері національної без-  
пеки і оборони;
- 2) координація та здійснення контролю за діяльністю органів вико-  
навчої влади у сфері національної безпеки і оборони у мирний час;
- 3) координація та здійснення контролю за діяльністю органів вико-  
навчої влади у сфері національної безпеки і оборони в умовах  
воєнного або надзвичайного стану та при виникненні кризових  
ситуацій, що загрожують національній безпеці України.

Зокрема за останні роки саме завдячуючи плідній роботі цього ор-  
гану було ухвалено ряд концептуальних нормативно-правових актів у  
сфері національної безпеки України: Закон України «Про основи наці-  
ональної безпеки України», Стратегія національної безпеки України,  
Доктрина інформаційної безпеки України тощо.

Слід також зазначити, що діяльність у цьому напрямі щороку ак-  
тивізується, про що свідчать нові редакції ряду важливих правових ак-  
тів у сфері національної безпеки: Рішення Ради національної безпеки  
і оборони України від 8 червня 2012 року «Про виклики та загрози на-  
ціональній безпеці України у 2011 році»<sup>51</sup>, Рішення Ради національної  
безпеки і оборони України від 8 червня 2012 року «Про нову редак-  
цію Воєнної доктрини України»<sup>52</sup>, Рішення Ради національної безпеки  
і оборони України від 8 червня 2012 року «Про нову редакцію Страте-  
гії національної безпеки України»<sup>53</sup> тощо.

Водночас ряд закріплених повноважень РНБО України збігаються  
з повноваженнями Кабінету Міністрів України. Загалом, повноважен-  
ня КМ України як вищого органу в системі органів виконавчої влади

<sup>51</sup> Про нову редакцію Воєнної доктрини України [Електронний ресурс] : рішення Ради національ-  
ної безпеки і оборони України від 8 черв. 2012 р. — Режим доступу : <http://zakon2.rada.gov.ua>.

<sup>52</sup> Про нову редакцію Стратегії національної безпеки України [Електронний ресурс] : рішення  
Ради національної безпеки і оборони України від 8 черв. 2012 р. — Режим доступу : <http://zakon2.rada.gov.ua>.

<sup>53</sup> Про нову редакцію Стратегії національної безпеки України [Електронний ресурс] : рішення  
Ради національної безпеки і оборони України від 8 черв. 2012 р. — Режим доступу : <http://zakon2.rada.gov.ua>.

визначено в ст. 116 Конституції України та деталізовано в Законі України «Про Кабінет Міністрів України» [129].

Таким чином, як і РНБО України, КМ України також має координаційні повноваження щодо роботи міністерств, інших органів виконавчої влади (п. 9 ст. 116 Конституції України).

Крім того, доволі складно вирізнити відмінність між окремими повноваженнями Президента України і Кабінету Міністрів України. Зокрема, згідно з п. 1 ст. 106 Конституції України Президент України забезпечує національну безпеку України. Відповідно ж до п. 7 ст. 116 Кабінет Міністрів України здійснює заходи щодо забезпечення національної безпеки України.

У зв'язку з чим важливим є уточнення повноважень суб'єктів забезпечення національної безпеки у ст. 9 Закону України «Про основи національної безпеки України», а саме: *Президент України як глава держави*, гарант державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина, Верховний Головнокомандувач Збройних сил України і Голова Ради національної безпеки і оборони України здійснює загальне керівництво у сферах національної безпеки та оборони України; Верховна Рада України в межах повноважень, визначених Конституцією України, визначає засади внутрішньої та зовнішньої політики, основи національної безпеки, формує законодавчу базу в цій сфері, схвалює рішення з питань введення надзвичайного і воєнного стану, мобілізації, визначення загальної структури, чисельності, функцій Збройних сил України та інших військових формувань, створених відповідно до законів України; *Рада національної безпеки і оборони України* координує та контролює діяльність органів виконавчої влади у сферах національної безпеки і оборони; з урахуванням змін у геополітичній обстановці вносить Президенту України пропозиції щодо уточнення Стратегії національної безпеки України та Воєнної доктрини України; *Кабінет Міністрів України* як вищий орган у системі органів виконавчої влади забезпечує державний суверенітет і економічну самостійність України, вживає заходів щодо забезпечення прав і свобод людини і громадянина, обороноздатності, національної безпеки України, громадського порядку і боротьби з злочинністю [51].

Екстраполюючи вищезазначене на предмет нашої роботи, можна дійти висновку, що **Президент України здійснює загальне керівни-**

цтво у сфері інформації з обмеженим доступом; Верховна Рада України визначає засади внутрішньої та зовнішньої інформаційної політики, основи захисту інформації з обмеженим доступом, формує законодавчу базу в цій сфері; Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері захисту інформації з обмеженим доступом; Кабінет Міністрів України спрямовує та координує роботу міністерств, інших органів виконавчої влади у сфері захисту інформації з обмеженим доступом.

Даний висновок підтверджується вітчизняним законодавством. Так, компетенцію державних органів у сфері захисту державної таємниці, яка є одним із видів інформації з обмеженим доступом, чітко визначено у ст. 4 Закону України «Про державну таємницю», а саме:

- Президент України, забезпечуючи національну безпеку, видає укази та розпорядження з питань охорони державної таємниці;
- Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці;
- Кабінет Міністрів України спрямовує та координує роботу міністерств, інших органів виконавчої влади щодо забезпечення здійснення державної політики у сфері охорони державної таємниці;
- Центральні та місцеві органи виконавчої влади, Рада міністрів Автономної Республіки Крим та органи місцевого самоврядування здійснюють державну політику у сфері охорони державної таємниці в межах своїх повноважень, передбачених законом;
- Спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці є Служба безпеки України [40].

### ***Органи виконавчої влади як суб'єкти захисту інформації з обмеженим доступом***

Крім Кабінету Міністрів України як вищого органу в системі органів виконавчої влади, важливими суб'єктами захисту інформації з обмеженим доступом є й інші органи виконавчої влади.

У розділі 4 Указу Президента України «Про Доктрину інформаційної безпеки України» передбачено, що реалізація напрямів державної полі-

тики у сфері інформаційної безпеки України здійснюється через діяльність органів виконавчої влади. Тобто відповідно до вищезазначеного нормативно-правового акта єдиним державним суб'єктом забезпечення інформаційної безпеки є саме органи виконавчої влади (ОВВ).

Цікавою є думка В. О. Логінова, який систему органів державного управління розглядає крізь призму діяльності та функціонування органів виконавчої влади, бо, на його погляд, зазначена ланка найбільшою мірою забезпечує функціонування інформаційної сфери держави [130, с. 32].

Як ми зазначали раніше, в Законі України «Про основи національної безпеки України» доволі дивний перелік суб'єктів забезпечення національної безпеки. Згідно з ст. 9 цього Закону поряд з міністерствами, Службою безпеки України та іншими центральними органами виконавчої влади виокремлено Воєнну організацію держави та правоохоронні органи.

Так, міністерства, Служба безпеки України та інші центральні органи виконавчої влади в межах своїх повноважень забезпечують виконання передбачених Конституцією і законами України, актами Президента України, Кабінету Міністрів України завдань, здійснюють реалізацію концепцій, програм у сфері національної безпеки, підтримують у стані готовності до застосування сили та засоби забезпечення національної безпеки; Воєнна організація держави забезпечує оборону України, захист її суверенітету, територіальної цілісності і недоторканності кордонів; протидіє зовнішнім загрозам воєнного характеру; правоохоронні органи ведуть боротьбу з злочинністю і протидіють тероризму, забезпечують захист і врятування населення в разі виникнення надзвичайних ситуацій техногенного і природного характерів.

Здебільшого фахівцями адміністративного права зазначається, що ієрархічна організація виконавчої влади формується відповідно до ієрархічних систем цих органів, що закріплені у Конституції України й уособлюються окремими видами органів виконавчої влади, а саме: вищий рівень, центральний рівень та місцевий або територіальний [131, с. 22–24]. Так, В. Авер'янов поділяє органи виконавчої влади на структурні ланки трьох організаційно-правових рівнів, зокрема:

- вищий рівень — Кабінет Міністрів України (у функціональній взаємодії з президентом);

- центральний рівень — міністерства, державні комітети та інші підвідомчі Кабінету Міністрів України органи виконавчої влади;
- місцевий або територіальний рівень, на якому діють:
- органи виконавчої влади загальної компетенції — Рада Міністрів Автономної Республіки Крим, обласні, районні, Київська і Севастопольська міські державні адміністрації;
- органи спеціальної — галузевої та функціональні — компетенції, котрі перебувають у подвійному підпорядкуванні [132, с. 50].

Оскільки адміністративно-правовий статус Кабінету Міністрів України як суб'єкта захисту інформації з обмеженим доступом було вже розглянуто, вважаємо за необхідне окреслити адміністративно-правовий статус суб'єктів забезпечення інформаційної безпеки України центрального рівня, тобто міністерств, державних комітетів та інших органів виконавчої влади підвідомчих Кабінету Міністрів України.

Як слушно зазначає Б. А. Кормич, більшість органів публічної влади виступають лише суб'єктами інформаційних відносин і їхній вплив на ці відносини є опосередкованим: інформаційні відносини не є об'єктом їхньої діяльності, а лише одним із інструментів, засобів виконання своїх функцій у різних сферах суспільного та державного життя [10, с. 205]. Саме тому кожен ОБВ має право одержувати в установленому законодавством порядку від центральних та місцевих органів виконавчої влади, Автономної Республіки Крим, місцевого самоврядування інформацію, документи та матеріали, необхідні для виконання покладених на нього завдань.

Проте з іншого боку, на всі ОБВ покладений обов'язок щодо захисту інформації з обмеженим доступом, зокрема у сфері охорони тієї інформації, що циркулює в межах ОБВ задля виконання покладених на них завдань та має статус державної таємниці.

Беручи до уваги вищезазначене, буде досліджений адміністративно-правовий статус тих ОБВ, для яких захист такої інформації є або основною, або однією із головних функцій.

Аналіз нормативно-правових актів, що регламентують діяльність центральних органів державної виконавчої влади, свідчить про те, що в Україні на цьому рівні державного управління є кілька міністерств та відомств, що здійснюють безпосередні заходи щодо забезпечення інформаційної безпеки.



Згідно з Указом Президента України «Про оптимізацію системи центральних органів виконавчої влади» від 9 грудня 2010 року [133] з метою оптимізації системи центральних органів виконавчої влади, усунення дублювання їх повноважень, забезпечення скорочення чисельності управлінського апарату та витрат на його утримання, підвищення ефективності державного управління та відповідно до пункту 15 частини першої статті 106 Конституції України було ліквідовано, реорганізовано чи створено ряд нових ОВВ. Аналіз вищезазначеного нормативно-правового акта надав можливість дійти висновку, що серед ОВВ як суб'єктів захисту інформації з обмеженим доступом є такі, як:

- *Міністерство внутрішніх справ України;*
- *Служба безпеки України;*
- *Державна служба спеціального зв'язку та захисту інформації України;*
- *Державна архівна служба України, що була утворена внаслідок реорганізації Державного комітету архівів України;*
- *Державна служба України з питань захисту персональних даних;*
- *Державна служба інтелектуальної власності України.*

Тож розглянемо основні завдання та повноваження найважливіших ОВВ як суб'єктів захисту інформації з обмеженим доступом.

**Основними завданнями МВС як суб'єкта захисту інформації з обмеженим доступом** є захист інформаційних прав і свобод, законних інтересів громадян; запобігання інформаційним правопорушенням та їх припинення; виявлення та розкриття інформаційних правопорушень, розшук осіб, що їх вчинили; виконання кримінальних покарань і адміністративних стягнень; участь у поданні соціальної та правової допомоги громадянам, сприяння у межах своєї компетенції державним органам, підприємствам, установам і організаціям у виконанні покладених на них законом обов'язків.

11 вересня 2009 року у структурі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, МВС України створено відділ боротьби з кіберзлочинністю. На цей підрозділ покладаються завдання із формування та реалізації державної політики у цій сфері правоохоронної діяльності, напрацювання методичних рекомендацій протидії злочинам такої категорії, організація міжнародного співробітництва у справах про комп'ютерні правопорушення, розробка та внесення відповідних змін до чинного законодавства. Крім того, до обов'язків цьо-



го відділу належить виявлення та документування організованих груп транснаціонального та регіонального характеру, учасники яких спеціалізуються на вчиненні злочинів із використанням високих технологій та телекомунікаційних систем.

Згідно з Указом Президента України «Про оптимізацію системи центральних органів виконавчої влади» було ліквідовано Державний департамент інтелектуальної власності, який відповідно до Постанови Кабінету Міністрів України «Про створення Державного департаменту інтелектуальної власності» від 4 квітня 2000 року № 601 був урядовим органом державного керування у складі Міністерства освіти і науки України [134].

Його функції було передано Державній службі інтелектуальної власності України. Зважаючи на те, що нині бракує відповідного законодавства, яке визначало б повноваження, структуру тощо цієї Служби, вважаємо, що основні завдання цієї інституції збігаються з тими, що мала попередня. Таким чином, **основним завданням Державної служби інтелектуальної власності України як суб'єкта захисту інформативності з обмеженим доступом** є організаційне забезпечення охорони прав на об'єкти інтелектуальної власності.

Крім того, ця Служба здійснює ряд координаційно-контрольних функцій, зокрема: координує діяльність з передання прав на об'єкти інтелектуальної власності, у тому числі створені цілком або частково за рахунок державного бюджету; організовує розгляд заяв і скарг щодо видачі охоронних документів на об'єкти інтелектуальної власності, а також інших звернень фізичних і юридичних осіб з питань інтелектуальної власності; координує роботу з інформаційного забезпечення діяльності у сфері інтелектуальної власності, здійснює нормативно-методичне керівництво в цій сфері, забезпечує комплектування національного фонду патентної документації; вносить у встановленому порядку до Міністерства освіти та науки пропозиції щодо участі України в роботі міжнародних організацій з інтелектуальної власності, здійснює міжнародне співробітництво і бере участь у підготовці і підписанні міжнародних угод з питань інтелектуальної власності; проводить роботу з підготовки та перепідготовки фахівців у питаннях інтелектуальної власності.

Внаслідок ліквідації Державної служби зв'язку України було утворено Адміністрацію Державної служби спеціального зв'язку та захисту

інформації України. Згідно з Указом Президента України «Про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» від 30 червня 2011 року Адміністрація Державної служби спеціального зв'язку та захисту інформації України є правонаступником Державної служби зв'язку України і Державної адміністрації зв'язку урядового органу, що діяв у складі Міністерства транспорту та зв'язку України [135].

Адміністрація Державної служби спеціального зв'язку та захисту інформації України (далі — Адміністрація) є центральним органом виконавчої влади у складі Державної служби спеціального зв'язку та захисту інформації України (далі — Держспецзв'язку України). Адміністрація є центральним органом виконавчої влади зі спеціальним статусом, головним органом у системі центральних органів виконавчої влади з формування і забезпечення реалізації державної політики у сферах організації спеціального зв'язку та захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, надання послуг поштового зв'язку. Адміністрація є центральним органом виконавчої влади в галузі зв'язку, спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

Серед **основних завдань** зазначеної вище інституції в контексті предмета дослідження такі:

- 1) забезпечення формування і реалізації державної політики у сферах захисту державних інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем (далі — інформаційно-телекомунікаційні системи), криптографічного та технічного захисту інформації, використання і захисту державних електронних інформаційних ресурсів, телекомунікацій, користування радіочастотним ресурсом України, надання послуг поштового зв'язку; участь у формуванні і реалізації державної політики у сфері електронного документообігу органів державної влади та органів місцевого самоврядування, розробленні та впровадженні електронного цифрового підпису в органах державної влади та органах місцевого самоврядування;
- 2) забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

- 3) визначення вимог і порядку створення та розвитку систем технічного та криптографічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
- 4) здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, протидії технічним розвідкам, а також за додержанням технічних вимог керівних документів у сфері надання послуг електронного цифрового підпису;
- 5) охорона об'єктів та майна Держспецзв'язку України, у тому числі приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації тощо [135].

Щодо Державної служби спеціального зв'язку та захисту інформації (Держспецзв'язку), то її створення має довгу історію. Так, у лютому 1998 року Указом Президента України «Про заходи щодо вдосконалення криптографічного захисту інформації в телекомунікаційних і інформаційних системах» на Головне управління урядового зв'язку Служби безпеки України було покладено вирішення усього комплексу завдань, пов'язаних зі створенням такої системи в Україні. У травні 1998 року на ГУУЗ СБ України Указом Президента України № 505 покладено завдання з реалізації державної політики в цій сфері. З метою концентрації зусиль у сфері захисту інформації за рішенням Президента України у серпні 1998 року на базі Головного управління урядового зв'язку СБ України із залученням фахівців Головного управління технічного захисту інформації Держкомсекретів було створено Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України (ДСТСЗІ СБ України), який став головною структурою в державі з питань криптографічного та технічного захисту інформації.

Відповідно до Указу Президента України «Про додержання прав людини під час проведення оперативно-технічних заходів» від 7 листопада 2005 року було вперше визначено необхідність створення в державі Служби спеціального зв'язку та захисту інформації України як центрального органу виконавчої влади із спеціальним статусом, визначивши її основними завданнями реалізацію державної політики у

сфері захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення функціонування Державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації [136].

Отже, **Державна служба спеціального зв'язку і захисту інформації України** була створена на основі ДСТСЗІ СБУ.

Нині вона є центральним органом виконавчої влади зі спеціальним статусом, що виконує такі завдання, як:

- участь у формуванні та реалізації державної політики у сфері захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації;
- забезпечення в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб органів державної влади, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації;
- забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;
- визначення вимог і порядку створення та розвитку систем технічного та криптографічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
- здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису;
- охорона об'єктів, приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України [137].

Таким чином, Державна служба спеціального зв'язку та захисту інформації України як суб'єкт захисту інформації з обмеженим доступом

має необхідні повноваження щодо формування та реалізації державної політики у сфері захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації.

**Служба безпеки України** є спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці. Так, СБ України вносить Президенту України пропозиції про видання актів з питань збереження державної таємниці, обов'язкових для виконання органами державного управління, підприємствами, установами, організаціями і громадянами. Зокрема, СБ України було розроблено проект Закону України «Про державні секрети» [138].

Важливість захисту персональних даних як інформації з обмеженим доступом підтверджується не лише фактом прийняття законів України «Про захист персональних даних» [139], «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» [140], «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних», що набув чинності з 1 січня 2012 року [141], але і тим, що реалізацію державної політики у сфері захисту персональних даних забезпечує спеціально створений центральний орган виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через міністра юстиції України — **Державна служба України з питань захисту персональних даних (ДСЗПД України)**.

ДСЗПД України у своїй діяльності використовує рекомендації міжнародних організацій щодо захисту персональних даних.

Указом Президента України «Про Положення про Державну службу України з питань захисту персональних даних» від 6 квітня 2011 року було визначено такі **основні завдання** цієї інституції:

- 1) внесення пропозицій щодо формування державної політики у сфері захисту персональних даних;
- 2) реалізація державної політики у сфері захисту персональних даних;
- 3) контроль за додержанням вимог законодавства про захист персональних даних;

4) здійснення міжнародно-правового співробітництва у сфері захисту персональних даних [142].

Задля реалізації покладених вище завдань, ДСЗПД України має доволі широке коло повноважень, що визначені Указом Президента України «Про Положення про Державну службу України з питань захисту персональних даних» та Законом України «Про захист персональних даних», зокрема ДСЗПД України відповідно до покладених на неї завдань:

- 1) узагальнює практику застосування законодавства з питань захисту персональних даних, розробляє пропозиції щодо вдосконалення законодавчих актів, актів Президента України, Кабінету Міністрів України, нормативно-правових актів міністерств та в установленому порядку подає їх Міністру юстиції України;
- 2) готує пропозиції щодо визначення загальної стратегії та пріоритетних напрямів діяльності у сфері захисту персональних даних;
- 3) розробляє критерії ризику незаконного використання та розголошення інформації, що міститься в базах персональних даних;
- 4) розробляє методичні матеріали і рекомендації з питань, віднесених до її компетенції;
- 5) розробляє типовий порядок обробки персональних даних у базах персональних даних;
- 6) розробляє критерії і порядок оцінювання стану захищеності персональних даних у базах персональних даних підприємств, установ і організацій усіх форм власності, державних органів чи органів місцевого самоврядування, фізичних осіб — підприємців, які обробляють персональні дані відповідно до закону;
- 7) реєструє бази персональних даних та веде Державний реєстр баз персональних даних, надає витяги із нього;
- 8) забезпечує створення Державного реєстру баз персональних даних;
- 9) визначає вимоги до документів, що подаються для реєстрації баз персональних даних;
- 10) у межах компетенції розглядає пропозиції, запити, звернення, вимоги та скарги фізичних та юридичних осіб, органів;
- 11) видає документи встановленого зразка про реєстрацію баз персональних даних у Державному реєстрі баз персональних даних;
- 12) здійснює державний нагляд та контроль за додержанням законодавства про захист персональних даних;



- 13) розробляє та затверджує плани перевірок володільців та (або) розпорядників баз персональних даних щодо дотримання ними вимог законодавства у сфері захисту персональних даних;
- 14) проводить у межах своїх повноважень виїзні та безвиїзні перевірки володільців та (або) розпорядників баз персональних даних;
- 15) видає володільцям та (або) розпорядникам баз персональних даних обов'язкові до виконання приписи щодо усунення порушень законодавства про захист персональних даних та вимагає надання необхідної інформації та документів, що підтверджують усунення виявлених порушень;
- 16) складає адміністративні протоколи про виявлені порушення законодавства у сфері захисту персональних даних;
- 17) передає правоохоронним органам матеріали про виявлені порушення у сфері захисту персональних даних;
- 18) здійснює контроль за дотриманням правил передачі персональних даних іноземним суб'єктам відносин, пов'язаних із персональними даними;
- 19) бере участь у міжнародному співробітництві з питань захисту персональних даних, вивчає, узагальнює та поширює світовий досвід з цих питань;
- 20) організовує та забезпечує взаємодію з іноземними суб'єктами відносин, пов'язаними із персональними даними;
- 21) бере участь у підготовці міжнародних договорів України з питань захисту персональних даних, готує пропозиції щодо укладення, денонсації таких договорів, забезпечує їх виконання;
- 22) погоджує порядок обробки персональних даних, які належать до банківської таємниці;
- 23) організовує роботу з підвищення кваліфікації спеціалістів у галузі захисту персональних даних та впроваджує в практику досягнення науки і передового досвіду;
- 24) проводить науково-дослідні та дослідно-конструкторські роботи у галузі захисту персональних даних;
- 25) проводить дослідження, в тому числі наукові у сферах, що належать до її компетенції;
- 26) здійснює інші повноваження, визначені законами України та покладені на неї Президентом України [142].



Щодо **Державної архівної служби України** та **Державної служби інтелектуальної власності України**, то їх адміністративно-правовий статус як суб'єктів захисту інформації з обмеженим доступом нормативно закріплено указами Президента України «Про затвердження Положення про Державну архівну службу України» від 6 квітня 2011 року [143] та «Про затвердження Положення про Державну службу інтелектуальної власності України» від 8 квітня 2011 року [144] відповідно.

Дослідження ОВВ як елемента адміністративно-правового режиму захисту інформації з обмеженим доступом засвідчило, що, незважаючи на значну та розгалужену сукупність ОВВ у цій сфері, говорити про, справді, сформовану систему цих органів у сфері захисту інформації з обмеженим доступом зарано.

Ситуація ускладнюється перманентною реструктуризацією вищезазначених інституцій та зміною тих завдань, функцій, повноважень, що на них покладаються. А тому відстежити якість виконаних зобов'язань доволі важко. Тим більше, що в системі державного управління не визначено державного органу, який безпосередньо реалізує завдання у сфері захисту інформації з обмеженим доступом. Усі вищезазначені органи забезпечують лише окремі напрями (вектори) у цьому контексті.

Так, серед функцій органів державного управління відсутні функції стосовно охорони інформації з обмеженим доступом, що не становить державної таємниці, тобто розробки і впровадження на загальнодержавному рівні організаційних, нормативно-методичних заходів, координування і контролю у цій сфері діяльності [145]. Не вирішеним залишається питання щодо визначення головного органу, що має здійснювати необхідні заходи у сфері захисту державної таємниці. Оскільки аналіз світової практики засвідчує, що охорона державної таємниці та іншої інформації обмеженого доступу з точки зору організаційного, нормативно-методичного забезпечення, координації і контролю покладена на один державний орган [146, с. 116–117].

Отже, актуальним напрямом удосконалення захисту інформації з обмеженим доступом в Україні є підвищення ефективності функціонування вищезазначених органів шляхом корекції їх компетенції та повноважень, оптимізації їх організаційно-функціональної структури, а також створення спеціалізованого ЦОВВ що забезпечуватиме реаліза-

цію державної політики у цій сфері, беручи до уваги законодавчо закріплені види інформації з обмеженим доступом.

### ***Відповідальність за порушення режимних норм***

Як елемент адміністративно-правового режиму виокремлюють *відповідальність за порушення режимних норм*. Залежно від характеру та ступеня суспільної небезпеки порушень, передбачається кримінальна, адміністративна чи дисциплінарна відповідальність.

Так, у КК України виокремлено розділ 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», що містить лише 6 статей, які передбачають кримінальну відповідальність за вчинення злочинів інформаційного характеру:

- ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»;
- ст. 361–1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;
- ст. 361–2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації»;
- ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї»;
- ст. 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється»;
- ст. 363–1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку».

Водночас, можемо констатувати, що ряд статей КК України, які також передбачають кримінальну відповідальність за порушення окремих видів інформації з обмеженим доступом, розташовані в інших главах, також мають інформаційний характер, зокрема:

- ст. 328 «Розголошення державної таємниці», відповідно до якої передбачена кримінальна відповідальність за розголошення державної таємниці за відсутності ознак державної зради або шпигунства;
- ст. 329 «Втрата документів, що містять державну таємницю»;
- ст. 330 «Передача або збирання відомостей, що становлять конфіденційну інформацію, яка знаходиться у володінні держави»;
- ст. 182 «Порушення недоторканності приватного життя» передбачає відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації...»;
- ст. 176 «Порушення авторського права і суміжних прав»;
- ст. 168 «Розголошення таємниці усиновлення (удочеріння)»;
- ст. 163 «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер»;
- ст. 381 «Розголошення відомостей про заходи безпеки щодо особи, взятої під захист»;
- ст. 387 «Розголошення даних оперативно-розшукової діяльності, досудового розслідування»;
- ст. 422 «Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості» тощо.

Адміністративні делікти також не систематизовано в окремому розділі, а розпорошено по різних розділах (главах) Кодексу України про адміністративні правопорушення.

Зокрема, викликають зацікавлення роботи О. В. Стоєцького, в яких автор досліджує питання адміністративної відповідальності за правопорушення у сфері інформаційної безпеки<sup>54</sup>. Так, дослідник дійшов ви-

<sup>54</sup> Стоєцький О. В. Адміністративна відповідальність за порушення у сфері інформаційної безпеки України : автореф. дис. на здобуття наук ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право»/ О. В. Стоєцький ; Запорізький. нац. ун-т. — Запоріжжя, 2013. — 19 с.; Стоєцький О. В. Реалізація адміністра-

сновку, що Особлива частина КУпАП містить склади інформаційних проступків у таких главах:

- главі 5 «Адміністративні правопорушення в галузі охорони праці і здоров'я населення»;
- главі 6 «Адміністративні правопорушення, що посягають на власність»;
- главі 7 «Адміністративні правопорушення в галузі охорони природи, використання природних ресурсів, охорони пам'яток історії та культури»;
- главі 10 «Адміністративні правопорушення на транспорті, в галузі шляхового господарства і зв'язку»;
- главі 12 «Адміністративні правопорушення в галузі торгівлі, громадського харчування, сфері послуг, в галузі фінансів і підприємницькій діяльності»;
- главі 14 «Адміністративні правопорушення, що посягають на громадський порядок і громадську безпеку»;
- главі 15 «Адміністративні правопорушення, що посягають на встановлений порядок управління»;
- главі 15-а «Адміністративні правопорушення, що посягають на здійснення народного волевиявлення та встановлений порядок його забезпечення» тощо.

При чому кожна з глав має різну кількість складів проступків у сфері інформації, за які передбачена адміністративна відповідальність.

Проте найбільша кількість складів правопорушень містить глава 15 КУпАП, а саме: адміністративні правопорушення, які посягають на встановлений порядок управління; глава 15-а КУпАП — адміністративні правопорушення, що посягають на здійснення народного волевиявлення та встановлений порядок його забезпечення; глава 12 КУпАП — адміністративні правопорушення в галузі торгівлі, громадського харчування, сфері послуг, в галузі фінансів і підприємницькій діяльності; глава 10 КУпАП — адміністративні правопорушення на транспорті, в галузі шляхового господарства і зв'язку, а також глава 7 КУпАП — адміністративні правопорушення у галузі охорони природи, використання природних ресурсів, охорони пам'яток історії та культури.

---

тивно-правових норм у сфері забезпечення інформаційної безпеки / О. В. Стоєцький // Адвокат. — 2008. — № 12. — С. 36–39.

Щодо безпосередньо адміністративної відповідальності за порушення інформації з обмеженим доступом, то слід відмітити такі статті:

- ст. 188–39 «Порушення законодавства у сфері захисту персональних даних»;
- ст. 188–40 «Невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних»;
- ст. 212–2 «Порушення законодавства про державну таємницю»;
- ст. 212–5 «Порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави»;
- ст. 212–6 «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем» тощо.

### ***Просторово-часові межі чинності адміністративно-правового режиму інформації з обмеженим доступом***

Щодо цього елемента адміністративно-правового режиму, а саме встановлення *просторово-часових меж* його чинності, тобто визначення тієї території, на якій буде введено режим, і того терміна дії, впродовж якого він буде діяти, то на відміну від режимів надзвичайного, воєнного, екологічного станів, для адміністративно-правового режиму захисту інформації з обмеженим доступом такий елемент не має настільки важливого значення.

Територіально адміністративно-правовий режим захисту інформації з обмеженим доступом може охоплювати як всю країну, так і окремий район, область чи територію Автономної Республіки Крим.

Оскільки адміністративною наукою за терміном дії режими поділяються на постійні (митний, прикордонний, паспортний) і введені на певний термін (режим надзвичайного, воєнного, екологічного стану) [85, с. 250], тому адміністративно-правовий режим захисту інформації з обмеженим доступом постійний.

Загалом питання строків щодо окремих видів інформації з обмеженим доступом, крім державної таємниці, на законодавчому рівні не визначено.

Щодо адміністративно-правового режиму захисту державної таємниці, то відповідно до ст. 13 Закону України «Про державну таємницю» «строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. Він не може перевищувати для інформації з ступенем секретності «особливої важливості» — 30 років, для інформації «цілком таємно» — 10 років, для інформації «таємно» — 5 років» [40].

Після закінчення зазначеного строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць виносить рішення про скасування рішення про віднесення її до державної таємниці або про подовження строку дії зазначеного рішення в межах наведених вище строків. Крім того, Президент України з власної ініціативи або на підставі пропозицій державних експертів з питань таємниць, чи за зверненням державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян може встановлювати більш тривалі строки дії рішень про віднесення інформації до державної таємниці, ніж 30, 10 і 5 років.

### 3.3 УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Як ми зауважували у попередніх своїх роботах<sup>55</sup>, динамічність розвитку інформаційних відносин в Україні сприяла, насамперед, фрагментарному та ситуативному підходу при створенні інформаційного законодавства. Розгляд нормативно-правового регулювання інформації з обмеженим доступом також підтверджує цю тезу.

До найбільш суттєвих *недоліків правового регулювання інформаційних відносин в Україні* слід включити такі.

1. Наявність колізій та конкуренції НПА, що регулюють правові відносини в інформаційній сфері.
2. Фрагментарність і ситуативність правового регулювання.

<sup>55</sup> Ліпкан В. А. Систематизація інформаційного законодавства України : [монографія] / В. А. Ліпкан, В. А. Залізняк ; за заг. ред. В. А. Ліпкана. — К. : О. С. Ліпкан, 2012. — 304 с.

3. Неузгодженість понятійно-категоріального апарату (інформаційної термінології), що закріплено в НПА.
4. Численність та розгалуженість НПА, що ускладнює їх правореалізацію та контроль за виконанням.
5. Неузгодженість ряду НПА, що були ухвалені до 1996 року, з Конституцією України.
6. Домінування підзаконних НПА над законами.

Отже, удосконалення вітчизняного інформаційного законодавства є важливим та своєчасним напрямом наукової діяльності, одним із напрямів якого є вивчення зарубіжного досвіду у цій сфері та адаптація його до особливостей та специфіки українського інформаційного суспільства. Іншим, найбільш дієвим, на нашу думку, є проведення масштабної систематизаційної роботи у цій сфері.

При виборі конкретної форми систематизації необхідно враховувати не лише складний і специфічний характер інформаційних відносин та становлення інформаційного права як самостійної галузі права, а й той факт, що інформаційне право як молода галузь права не є систематизованою галуззю. А тому не можна говорити про необхідність прийняття нових кодексів або їх нових редакцій з урахуванням змін, що відбулися у суспільному житті країни.

Здебільшого стосовно нових галузей, предмет регулювання яких ще достатньо не визначений, найбільш раціональним та адекватним напрямом удосконалення є проведення систематизації нормативно-правового матеріалу за допомогою інкорпорації та консолідації. У даному випадку інкорпорація буде відігравати функцію обліку нормативно-правового матеріалу, а консолідація має започатковувати процес подальшої кодифікації. Тим більш, тривалий час можуть існувати не кодифіковані, а консолідовані нормативно-правові акти.

### *Етапи систематизації інформаційного законодавства*

Систематизація інформаційного законодавства має здійснюватись поступово. Даний процес має проходити ряд етапів, на кожному з яких потрібно дотримуватися певних правил законодавчої техніки та сформованих у теорії права засад.



*На першому етапі* доречно визначити, яке саме коло суспільних відносин буде регулюватись Інформаційним кодексом. Чи буде тотожною сфера дії Інформаційного кодексу сфері дії Закону України «Про інформацію»?

*На другому етапі* слід визначитись із обсягом нормативного матеріалу, який підлягає опрацюванню. Оскільки ще наприкінці 1990-х років за результатами досліджень у Науково-дослідному центрі правової інформатики Академії правових наук України із застосуванням комп'ютерної інформаційно-аналітичної системи «Законодавство» було визначено, що інформаційне законодавство становить значний масив нормативно-правових актів (понад 260 законів, 295 постанов Верховної Ради, 380 указів і 90 розпоряджень Президента, 1160 постанов і 210 розпоряджень Кабінету Міністрів, 1 500 актів міністерств і відомств тощо)<sup>56</sup>.

Саме на цьому етапі визначається той масив нормативного матеріалу, що не втратив чинності. Причому, слід брати до уваги той факт, що ряд нормативно-правових актів можуть де-юре бути чинними, але де-факто втратили силу у зв'язку з ухваленням нового законодавства. Отже, на другому етапі визначається спектр і чинність нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері.

*На третьому етапі* здійснюється видалення з чинних нормативних актів або їх частин тих норм, які наразі вже не мають принципового значення, як-от: преамбули, що втратили значення, статті з перерахуванням актів, які скасовані або містять тимчасові правила, статті, які мають ненормативний характер і не сприяють розумінню чинного нормативного матеріалу.

*На четвертому етапі* здійснюється безпосередньо формування структури нормативно-правового акта відповідно до опрацьованого нормативного матеріалу. Саме на цьому етапі визначається колізійність норми права чи відсутність саме тих, що потребують законодавчого урегулювання у зв'язку з появою нових суспільних відносин.

Систематизація законодавства у сфері інформації з обмеженим доступом має здійснюватись у формі інкорпорації, консолідації та подальшого виокремлення певного розділу в межах Інформаційного кодексу України.

<sup>56</sup> Цимбалюк В. С. Інформаційне право (основи теорії і практики) : [монографія] / В. С. Цимбалюк. — К. : Освіта України, 2010. — 388 с.

## Напрями інкорпорації

Інкорпорація становить собою таку форму систематизації законодавства, яка полягає у зовнішньому впорядкуванні вже наявних НПА без зміни змісту норм права.

Інкорпорація інформаційного законодавства покликана його упорядкувати за одним чи кількома критеріями без зміни змісту. Серед основних критеріїв, за якими здебільшого здійснюється інкорпорація законодавства, є дата прийняття НПА, алфавітний порядок, предметна ознака (галузі, інститути права та сфери державної діяльності), суб'єкт видання НПА, юридична чинність тощо.

Доцільно визначити **критерій інкорпорації інформаційного законодавства**, яким, на нашу думку, виступають галузі та інститути, зокрема:

- НПА, що регулюють суспільні відносини у сфері діяльності ЗМІ (в межах цієї галузі виокремити такі інститути, як друковані ЗМІ, телебачення і радіомовлення, Інтернет тощо);
- НПА, що регулюють суспільні відносини у сфері забезпечення права на інформацію (в межах цієї галузі виокремити такі інститути, як право на доступ до інформації тощо).

Незважаючи на те, що внаслідок інкорпорації не змінюється зміст нормативного матеріалу, завдяки їй виявляються ті НПА чи окремі норми, що втратили чинність, мали тимчасове значення або підлягають скасуванню. Інкорпоровані акти також не містять ненормативних частин актів, відомості про осіб, які підписали НПА, але включають офіційні зміни чи доповнення до НПА.

Систематизація інформаційного законодавства у формі **інкорпорації** полягає в підготовці й виданні державними та недержавними інституціями чи окремими фахівцями різного роду збірників, що забезпечують доступність і можливість ознайомлення широкого кола громадськості з текстами законів і підзаконних нормативно-правових актів, які регулюють правові відносини в інформаційній сфері<sup>57</sup>.

Інкорпорований збірник інформаційного законодавства охоплює НПА, що регулюють такі інформаційні відносини, як закони України,

<sup>57</sup> Череповський К. П. Щодо наукової розробленості інкорпорації інформаційного законодавства / К. П. Череповський // Національна і міжнародна безпека в сучасних трансформаційних процесах : матеріали наук.-практ. конференції. — К., 2011. — С. 69–71.

постанови Верховної Ради України, укази і розпорядження Президента України, постанови і розпорядження Кабінету Міністрів України, що мають нормативний характер, нормативні акти міністерств, інших центральних органів виконавчої влади, які підлягають реєстрації.

Після визначення критерію інкорпорації інформаційного законодавства необхідно здійснити облік усього нормативного матеріалу за цим критерієм. Причому інкорпорований збірник інформаційного законодавства має містити не першочергові тексти вищезазначених НПА, а їх останню редакцію. Самі ж норми права не зазнають жодних змін та інкорпорується у тому вигляді, в якому вони є чинними на момент систематизації, тобто зміст нормативного матеріалу незмінний.

Отже, один і той самий НПА може входити до складу різних інкорпорованих збірників, що створюються за різними критеріями (хронологічний, предметний), чи водночас існувати окремо.

Незважаючи на те, що інформаційній відносини іманентно є динамічними, а тому, відповідно, й інформаційне законодавство також, на нашу думку, його **інкорпорація є важливим напрямом наукової і правотворчої діяльності на сучасному етапі**. Оскільки значення інкорпорації як форми систематизації полягає в тому, що вона упорядковує весь чинний нормативно-правовий матеріал у певній сфері з метою полегшення правозастосовної діяльності та реалізації доступу до правової інформації громадськості.

Таким чином, процес **інкорпорації інформаційного законодавства** складається з кількох взаємопов'язаних етапів. На першому етапі інкорпоратор з'ясовує критерії систематизації, тобто здійснює вибір виду інкорпорації (повна чи часткова; офіційна чи неофіційна; предметна чи хронологічна). Ураховуючи стан інформаційного законодавства України та правові недоліки правового регулювання інформаційних відносин, найбільш доречним, на нашу думку, є проведення генеральної, предметної та офіційної інкорпорації. На другому етапі визначається обсяг нормативно-правового матеріалу, який потребує інкорпорації, тобто коло тих НПА, предметом яких є суспільні відносини у сфері інформації. На третьому етапі слід здійснити «чистку» НПА шляхом видалення з тексту окремих статей, пунктів, абзаців, що втратили силу, чи, навпаки, включення всіх подальших змін, доповнень з уточненням реквізитів ак-

тів, які внесли такі зміни чи доповнення; усунення з тексту тих частин, які не містять нормативних розпоряджень, зробивши позначку про причини відсутності таких частин; зібрання відомостей про осіб, які підписали нормативний акт, тощо. На четвертому етапі усі НПА групуються відповідно до предмета регулювання в межах інформаційної проблематики (ЗМІ, інформаційна безпека тощо) та займають відповідне місце в структурі інкорпораційного збірника.

Інкорпоратор використовує відповідні прийоми й методи систематичної обробки нормативного матеріалу залежно від поставленої мети.

Єдиною роботою в Україні, спеціально присвяченою аналізу проблем інкорпорації інформаційного законодавства, виступає дисертація К.П.Череповського «Інкорпорація інформаційного законодавства України», який є представником наукової школи В.А.Ліпкана.

### *Напрями консолідації*

У процесі інкорпорації законодавства особами, які уповноважені проводити дані роботи, широко використовуються консолідаційні прийоми як допоміжний етап при створенні інкорпорованого збірника законодавства<sup>58</sup>. Під час проведення консолідаційних робіт широко застосовуються прийоми, властиві інкорпорації. Таким чином, обидва види систематизації тісно взаємопов'язані та взаємодоповнюють одне одного. Наприклад, у процесі проведення інкорпорації та консолідації використовуються по суті одні й ті самі прийоми та правила, проте сама сутність проведених робіт, їх результати відрізняються. Це дає нам змогу стверджувати, що консолідація та інкорпорація, хоча й подібні між собою види систематизації законодавства, але водночас за своєю теоретико-юридичною сутністю є зовсім різними і виконують зовсім різні, покладені лише на них, функції<sup>59</sup>.

Здебільшого **консолідація** є уніфікацією нормативно-правових актів, оскільки усуває їх численність, позбавляє надмірного подрібнення, сприяє їх об'єднанню. Особливу актуальність ця форма систематизації набула у сфері відомчої правотворчості.

<sup>58</sup> Меленко С. Г. Консолідація як вид систематизації нормативно-правових актів : дис. ... канд. юрид. наук : 12.00.01 / Сергій Гаврилович Меленко. — Чернівці, 2002. — 206 с., С. 41.

<sup>59</sup> Меленко С. Г. Консолідація як вид систематизації нормативно-правових актів : дис. ... канд. юрид. наук : 12.00.01 / Сергій Гаврилович Меленко. — Чернівці, 2002. — 206 с., С. 46.

Доволі ґрунтовно стабільність процесу консолідації була досліджена С. Г. Меленком. Дослідник визначив, що під час проведення робіт, пов'язаних із консолідацією законодавства, систематизатор повинен послідовно виконати такі дії:

- визначити обсяг нормативно-правового матеріалу, який піддається консолідації;
- проаналізувати кожен документ як об'єкт консолідації;
- прийняти класифікаційне рішення, до якої галузі права віднести даний нормативний акт або його частину;
- ухвалити рішення про включення цілого нормативного акта до консолідованого збірника законодавства чи про доцільність розподілу акта на його складові частини та включення їх до консолідованого збірника нормативно-правових актів;
- визначити місце даного документа або його складової частини в ієрархічній будові консолідованого збірника;
- звернути увагу на частини документа і зазначити, які з них можуть бути віднесені до інших галузей права та включені до інших галузевих або міжгалузевих збірників законодавства;
- визначити, чи має місце повторення гіпотези, диспозиції та санкції у статтях цього нормативного акта та інших документів;
- вказати на той чи інший нормативний акт або його частини, які втратили свою дію, і усунути їх зі складу консолідованого збірника нормативно-правового матеріалу<sup>60</sup>.

Цікавим є дослідження М. І. Дімчогло, яка констатує, що слід зазначити новелу в законодавчому регулюванні функціонування ЗМІ в Молдові — створення такого консолідованого законодавчого акта, як *Кодекс телебачення і радіо в Молдові*, що був прийнятий 27 липня 2006 року<sup>61</sup>.

Дослідження вищезазначених дій дає змогу дійти висновку, що під час консолідації й інкорпорації використовуються спільна методика, прийоми систематизаційної діяльності щодо удосконалення нормативного матеріалу.

<sup>60</sup> Меленко С. Г. Консолідація як вид систематизації нормативно-правових актів : дис. ... канд. юрид. наук : 12.00.01 / Сергій Гаврилович Меленко. — Чернівці, 2002. — 206 с., С. 67.

<sup>61</sup> Дімчогло М. І. Консолідація інформаційного законодавства у сучасних правових системах (на прикладі законодавства окремих країн) / М. І. Дімчогло // Правові та політичні проблеми сучасності : матеріали наук.-практ. конф., (м. Луцьк, 22 квіт. 2012 р.). — К., 2012. — С. 23–27.

Отже, **всі форми систематизації є діалектично взаємопов'язаними та взаємодоповнювальними**. Тож завдяки консолідації інформаційне законодавство становитиме логічно побудовану систему.

Важливе значення для ефективної систематизаційної діяльності інформаційного законодавства в Україні має вироблення її на основі *уніфікованих принципів*.

На думку представника київської школи інформаційного права *В. Д. Гавловського*, в основі систематизації норм інформаційного права повинні бути пророблені юридичною наукою та перевірені практикою ґрунтовні принципи: об'єднання традицій та новацій правознавства; інкорпорація норм чинного інформаційного законодавства України в нову систему через агрегацію інститутів права; формування міжгалузевих інститутів права на основі зв'язків із галузевими інститутами<sup>62</sup>.

На противагу фрагментарному розв'язанню проблем правового регулювання правових відносин в інформаційній сфері, на наше переконання, **найбільш адекватним шляхом** підвищення ефективності вітчизняного інформаційного законодавства є проведення широкомасштабної, **поступової його систематизації крізь призму трьох основних форм: інкорпорації, консолідації та кодифікації**.

Єдиною роботою в Україні, спеціально присвяченою аналізу проблем консолідації інформаційного законодавства, виступає дисертація *М. І. Дімчогло* «Консолідація інформаційного законодавства України», яка є представницею наукової школи *В.А.Ліпкана*.

### **Напрями кодифікації**

За необхідність систематизації національного інформаційного законодавства у формі кодифікації висловлюються такі вітчизняні науковці, як: *І. Арістова, К. Беляков, В. Гавловський, В. Гриценко, В. Гурковський, М. Гуцалюк, Ю. Максименко, О. Марценюк, В. Цимбалюк, М. Швець* та інші.

<sup>62</sup> Гавловський В. Д. Інформаційне законодавство України : від інкорпорації до кодифікації / В. Д. Гавловський // Систематизація законодавства в Україні : проблеми теорії і практики. — К., 1999. — С. 27.



Також дані положення репрезентовані і в роботах представників наукової школи В. А. Ліпкана: В. Баскакова<sup>63</sup>, М. Дімчогло<sup>64</sup>, В. Залізняка<sup>65</sup>, Ю. Максименко<sup>66</sup>, П. Матвієнко<sup>67</sup>, К. Татарникової<sup>68</sup>, К. Череповського<sup>69</sup> (детальніше див. підрозділ «Праці наукової школи В.А.Ліпкана з інформаційної тематики» у розділі «Корисна бібліографія»).

Ю. Є. Максименко зауважує, що кодифікація інформаційного законодавства зумовлена рядом об'єктивних обставин, головними з яких є: наявність численних нормативно-правових актів із регулювання інформаційних правовідносин різної юридичної сили; динамічність інформаційних відносин; неузгодженість зі стандартами Європейського Союзу; декларативність окремих норм через брак механізму правореалізації; необхідність системного розв'язання проблеми нормативно-правового регулювання суспільних відносин у сфері забезпечення інформаційної безпеки України<sup>70</sup>.

<sup>63</sup> Баскаков В. Захист інформації з обмеженим доступом: розвиток вітчизняного законодавства / В. Баскаков // Підприємництво, господарство і право. — 2011. — № 4. — С. 126–128.; Баскаков В. Інформація з обмеженим доступом: аналіз термінологічно-понятійного апарату / В. Баскаков // Підприємництво, господарство і право. — 2011. — № 5. — С. 124–127.; Баскаков В. Захист інформації з обмеженим доступом в умовах боротьби з організованою злочинністю / В. Баскаков, В. Ліпкан // Боротьба з організованою злочинністю і корупцією (теорія і практика). — К., 2011. — № 24. — С. 263–269.

<sup>64</sup> Дімчогло М. І. Онови теорії консолідації інформаційного законодавства / М. І. Дімчогло // Підприємництво, господарство і право. — 2012. — № 5. — С. 41–46.; Дімчогло М. І. Консолідація як вид систематизації інформаційного законодавства / М. І. Дімчогло // Правова інформатика. — 2012. — № 1 (33). — С. 15–24.

<sup>65</sup> Залізник В. А. Системний підхід при дослідженні систематизації інформаційного законодавства України / В. А. Залізник // Філософські, методологічні і психологічні проблеми права : тези доп. III Всеукр. наук.-теорет. конф., (Київ, 23 квіт. 2010 р.). — К., 2010. — С. 56–57.

<sup>66</sup> Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права ; історія політичних і правових учень» / Ю. Є. Максименко. — К., 2007. — 20 с.

<sup>67</sup> Матвієнко П. Є. Аналіз сучасного етапу розвитку законодавства про комерційну таємницю в Україні / П. Є. Матвієнко // Підприємництво, господарство і право. — 2009. — № 12. — С. 85–88.

<sup>68</sup> Татарникова К. Г. Деякі аспекти методології кодифікації інформаційного законодавства / К. Г. Татарникова // Правові та політичні проблеми сучасності : матеріали наук.-практ. конф., (м. Луцьк, 22 квіт. 2012 р.). — К., 2012. — С. 38–40.

<sup>69</sup> Череповський К. П. Щодо наукової розробленості інкорпорації інформаційного законодавства / К. П. Череповський // Національна і міжнародна безпека в сучасних трансформаційних процесах : матеріали конференції. — К., 2011. — С. 69–71.

<sup>70</sup> Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : дис. ... канд. юрид. наук : 12.00.01 / Юлія Євгенівна Максименко. — К., 2007. — 188 с.



Слід акцентувати увагу, що саме цей шлях підвищення ефективності сукупності НПА, які регулюють інформаційні відносини в Україні, має значне правове підґрунтя.

Питання кодифікації інформаційного законодавства України також порушувались на численних конференціях, «круглих столах», конгресах: на міжнародній науково-практичній конференції «Систематизація законодавства в Україні: проблеми теорії і практики» (жовтень 1999 р., м. Київ); науково-технічній конференції «Правове, нормативне та методологічне забезпечення системи захисту інформації в Україні» (квітень 2000 р., м. Київ); на «круглому столі» «Інформаційна безпека» Міжнародного конгресу «Інформаційне суспільство в Україні — стан, проблеми, перспективи» (вересень 2000 р., м. Київ), «Проблеми кодифікації інформаційного законодавства України» (червень 2009 р., м. Київ), міжнародній науково-практичній конференції «Інформаційні стратегії в глобальному управлінні» (29 жовтня 2011 р., м. Київ), науково-практичній конференції «Національна і міжнародна безпека в сучасних трансформаційних процесах» (29 грудня 2011 р., м. Київ); науково-практичній конференції «Правові та політичні проблеми сучасності» (22 квітня 2012 р., м. Луцьк) тощо.

Розгляд проблем систематизації інформаційного законодавства України під час проведення наукових заходів має важливе значення, оскільки учасники висловлюють різні пропозиції до майбутнього кодексу, обмінюються фаховими думками, а результати таких заходів надсилаються компетентним органам державної влади.

Отже, майже десять років окремі науковці, групи фахівців і відповідні державні інституції займаються розробкою Інформаційного кодексу України (Кодексу законів України про інформацію, Кодексу України про інформацію тощо). Проте донині відсутній проект цього НПА, який був би винесений на публічне обговорення. Окремі спроби були зроблені під час проведення міжнародної науково-практичної конференції «Інформаційні стратегії в глобальному управлінні», влаштованої громадською організацією Глобальна Організація Союзнницького Лідерства за підтримки видавництва *ФОП О. С. Ліпкан*<sup>71</sup>. Під час заходу один із фундаторів і промоутерів інформаціологічної тематики

<sup>71</sup> Інтернет-конференції [Електронний ресурс]. — Режим доступу : <http://www.natsecurity.com.ua>

в Україні — В. С. Цимбалюк — подав для обговорення власний проект Концепції кодифікації законодавства України про інформацію<sup>72</sup>.

Створення майбутнього проекту цього НПА здійснюється у складних умовах. Так, у наукових колах точиться конфлікт між технократичним і гуманітарним підходами щодо його створення. Технократи основну увагу приділяють передачі інформації, а гуманітарії — праву на інформацію.

### ***Підходи до розроблення Інформаційного кодексу***

Окрім поодиноких пропозицій до майбутнього Інформаційного кодексу України, важливого значення набуває системне розв'язання проблем систематизації інформаційного законодавства.

Здійснений нами контент- та івент-аналіз наукових публікацій, де мультиплікандом виступав термін «Інформаційний кодекс», уможливив побачити наявність кількох наукових концепцій щодо кодифікації інформаційного законодавства:

- проект *Кодексу України про інформацію*, розробники — В. Цимбалюк, М. Швець та інші;
- проект *Інформаційного кодексу України*, розробник — Державний комітет телебачення та радіомовлення України за участю представників міністерств й інших комітетів;
- проект модельного *Інформаційного кодексу*, запропонований О. Барановим, І. Жилиєвим, М. Родіоновим та іншими. По суті, цей проект відтворює Концепцію реформування законодавства України у сфері суспільних інформаційних відносин в редакції 2000 року тільки на міждержавному рівні як модельний кодекс, але при цьому не враховано, що вітчизняна наука інформаційного права напрацювала нові теоретичні обґрунтування структуризації та кодифікації інформаційного законодавства.

Отже, на нашу думку, доречно розглянути запропоноване різними фахівцями бачення структури цього НПА.

<sup>72</sup> Цимбалюк В. С. Концепція Кодифікації законодавства України про інформацію / В. С. Цимбалюк // Інформаційні стратегії в глобальному управлінні : матеріали міжнар. наук.-практ. конференції. — К., 2011. — С. 73–91.

## *Проект М.Швеця та В. Брижка*

Цікавий є проект *Кодексу України про інформацію*, запропонований для громадського обговорення *М. Швецем та В. Брижком*.

Загальна структура Кодексу України про інформацію має такий вигляд: преамбула, загальна, спеціальна і прикінцева (заклучна) частини.

**Частина I «Загальна частина»** має таку структуру: розділ 1 «Загальні положення», розділ 2 «Суб'єкти інформаційних відносин», розділ 3 «Об'єкти інформаційних відносин», розділ 4 «Галузі, види, джерела інформації, інформаційних продуктів, інформаційних ресурсів», розділ 5 «Державна інформаційна політика», розділ 6 «Інформаційна діяльність, її види та інформаційні послуги», розділ 7 «Інформаційні послуги», розділ 8 «Інформаційне забезпечення інтелектуальної свободи», розділ 9 «Інформаційні технології та засоби їх забезпечення», розділ 10 «Підтримка інформаційної безпеки», розділ 11 «Охорона прав в інформаційних відносинах», розділ 12 «Захист прав в інформаційних відносинах», розділ 13 «Дія та застосування норм міжнародного права».

**Частина II «Особлива частина»** складається з розділу 14 «Основні інститути інформаційного права» з підрозділами: 14–1 «Засоби масової інформації», підрозділ 14–2 «Наука та освіта (науково-технічна інформація)», підрозділ 14–3 «Інформатизація та Національна програма інформатизації» та розділу 15 «Інші інститути інформаційного права», який також поділяється на підрозділи, зокрема: підрозділ 15–1 «Захист персональних даних», підрозділ 15–2 «Зв'язок та телекомунікації», підрозділ 15–3 «Електронні документи, електронний цифровий підпис та електронний документообіг», підрозділ 15–4 «Дистанційне навчання», підрозділ 15–5 «Телемедицина», підрозділ 15–6 «Електронна торгівля (комерція)», підрозділ 15–7 «Електронне урядування», підрозділ 15–8 «Бібліотечна та архівна справа», підрозділ 15–9 «Державні інформаційні стандарти», підрозділ 15–10 «Комерційна та державна таємниця».

**Частина III «Заклучна частина»** містить тільки 1 розділ «Прикінцеві положення та перехідні положення», що розкриває такі питання, як: введення в дію, внесення змін та доповнень до нормативно-правової бази.

Даний проект викликає доволі значну кількість дискусійних запитань, оскільки він не містить жодного розділу, де передбачено відповідальність за порушення інформаційного законодавства. Крім того, назва деяких розділів не є усталеною в наукових колах, наприклад: розді-

ли «Інформаційне забезпечення інтелектуальної свободи», «Підтримка інформаційної безпеки».

**Тим більше, що в «Особливій частині» вже виокремлено «Захист персональних даних», хоча, на нашу думку, це питання слід розглядати у рамках окремого розділу, присвяченого інформації з обмеженим доступом.**

У чому розбіжність розділів «Охорона прав в інформаційних відносинах» і «Захист прав в інформаційних відносинах»?

Питанням теоретичного відмежування таких понять, як захист, охорона, підтримка, забезпечення, регулювання і безпека приділено чимало наукових праць, тож авторам доцільно було б скористатися цим доробком, а не віднаходити велосипед.

### **Проект В. Цимбалюка**

Цікавим для розгляду також є **проект Інформаційного кодексу**, запропонований В. С. Цимбалюком. Так, вищезазначений НПА складається з преамбули, загальної, особливої та спеціальної частин, а також прикінцевих і перехідних положень. Ми, власно, відстоюємо позицію, відповідно до якої інформаційне законодавство має бути репрезентовано через розроблення Інформаційного кодексу, який структурно має складатися із: загальної, особливої та спеціальної частин. Тому позиція В. С. Цимбалюка резонує з нашою, і ми концептуально підтримуємо його.

У книзі I «Загальна частина» міститься 7 розділів, зокрема:

- розділ 1 «Основні положення»;
- розділ 2 «Суб'єкти інформаційних відносин»;
- розділ 3 «Об'єкти інформаційних відносин», який поділяється на декілька підрозділів: галузі, види, джерела інформації, інформаційних продуктів, інформаційних ресурсів; інформаційна діяльність та її види; інформаційні послуги; інформаційні системи, інформаційні технології і засоби їх забезпечення;
- розділ 4 «Підтримка інформаційної безпеки»;
- розділ 5 «Охорона прав в інформаційних відносинах»;
- розділ 6 «Захист прав в інформаційних відносинах»;
- розділ 7 «Дія та застосування норм міжнародного права».

**Книга II «Особлива частина»** містить 4 розділи:

- розділ 14 «Права та обов'язки людини, громадянина щодо інформації», що має підрозділ 14.1 «Інформаційне забезпечення інтелектуальної свободи»;
- розділ 15 «Права суспільства у сфері інформації»;
- розділ 16 «Права та обов'язки держави в інформаційній сфері»;
- розділ 17 «Міжнародне співробітництво у глобальному інформаційному просторі».

**Книга III «Спеціальна частина»** охоплює 3 розділи, які розподіляються на глави та підрозділи. Так, розділ 18 «Основні сфери інформаційної діяльності» складається з підрозділу 18.1 «Інформаційна діяльність у сфері масової комунікації», що поділяється на главу 1 «Засоби масової інформації та реклама» та главу 2 «Наука та освіта (науково-технічна інформація)»; підрозділу 18.2 «Зв'язок, телекомунікації», підрозділу 18.3 «Інформатизація та Національна програма інформатизації», підрозділу 18.4 «Бібліотечна справа», підрозділу 18.5 «Архівна справа», підрозділу 18.6 «Кінематографія», підрозділу 18.7 «Музейна справа»; розділу 19 «Інформаційна безпека», розділу 20 «Інші види інформаційної діяльності», що охоплює главу 1 «Електронні документи, електронний цифровий підпис та електронний документообіг», главу 2 «Захист інформації та персональних даних», главу 3 «Дистанційне навчання», главу 4 «Телемедицина», главу 5 «Електронна торгівля (комерція)», главу 6 «Електронне урядування», главу 7 «Культура та мистецтво», главу 13 «Державні стандарти в інформаційній сфері», главу 14 «Комерційна таємниця».

**Отже, знову ж таки спостерігається відсутність окремого розділу, присвяченого інформації з обмеженим доступом, внаслідок чого ряд її видів (комерційна таємниця, персональні дані) належать до різних розділів.**

Крім відмінностей у баченні структури даного НПА, відсутня єдність серед прихильників кодифікації інформаційного законодавства навіть щодо назви майбутнього Кодексу, зокрема пропонують таке:

1. Кодекс про інформацію та інформатизацію України.
2. Кодекс України про суспільні інформаційні відносини та інформаційну безпеку.
3. Кодекс України про інформацію.
4. Кодекс законів України про інформацію.
5. Кодекс про інформаційний суверенітет України.

6. Кодекс про захист інформації в Україні.
7. Кодекс про інформацію та інтелектуальну власність.
8. Інформаційний кодекс України тощо.

Варіативність назв майбутнього Кодексу обумовлена браком єдності в наукових колах щодо визначення обсягу нормативного матеріалу, який підлягає кодифікації. Тобто виникає питання: які саме нормативно-правові акти становлять інформаційне законодавство, а отже, потребують систематизації?

Будь-яка діяльність має інформаційний характер, тим більше в умовах розвитку інформаційного суспільства, актуалізації необхідності теоретичного вивчення та осмислення змісту права на інформацію<sup>73</sup>, права на доступ до інформації<sup>74</sup>, правового режиму інформаційних прав і свобод людини і громадянина<sup>75</sup>, реалізації державою інформаційної функції<sup>76</sup> і на загал — необхідності докорінної концептуальної зміни вектора та інтенсивності, методології розроблення і механізмів реалізації *державної інформаційної політики України*.

Найбільш доречною, на нашу думку, є назва «Інформаційний кодекс України», оскільки саме така назва, як правило, використовується в більшості НПА, що визначають необхідність його створення, чітко розкриває об'єкт і предмет правового регулювання та відповідає назві галузі права.

<sup>73</sup> Чуприна О. В. Право на інформацію: сутність та зміст / О. В. Чуприна // Правові та політичні проблеми сучасності : матеріали наук.-практ. конф., (м. Луцьк, 22 квіт. 2012 р.). — К., 2012. — С. 44–47.; Чуприна О. В. Адміністративно-правові аспекти права на інформацію / О. В. Чуприна // Національна і міжнародна безпека в сучасних трансформаційних процесах: матеріали конференції. — К., 2011. — С. 71–73.

<sup>74</sup> Капінус Л. І. Проблеми визначення права на доступ до інформації / Л. І. Капінус // Правові та політичні проблеми сучасності : матеріали наук.-практ. конф., (м. Луцьк, 22 квіт. 2012 р.). — К., 2012. — С. 27–30.

<sup>75</sup> Максименко Ю. Є. Щодо обґрунтованості обмеження прав і свобод громадян / Ю. Є. Максименко // Правові та політичні проблеми сучасності : матеріали наук.-практ. конф., (м. Луцьк, 22 квіт. 2012 р.). — К., 2012. — С. 33–35.

<sup>76</sup> Климентьев О. П. Ознаки інформаційної функції / О. П. Климентьев // Правові та політичні проблеми сучасності : матеріали наук.-практ. конф., (м. Луцьк, 22 квіт. 2012 р.). — К., 2012. — С. 30–33.



## *Проект Держкомтелерадіо*

Таку назву має і проект НПА, розроблений Державним комітетом інформаційної політики, телебачення і радіомовлення України. Даний проект виглядає повноцінним кодифікованим актом та має доволі розгалужену та найбільш адекватну, на нашу думку, структуру.

**Загальна частина** складається з 5 розділів:

- розділ I «Предмет (об'єкт) регулювання і суб'єкти інформаційної діяльності»;
- розділ II «Державне регулювання інформаційної сфери»;
- розділ III «Використання мови»;
- розділ IV «Міжнародні відносини в інформаційній сфері», що має декілька глав, зокрема: глава I «Міжнародна інформаційна діяльність», глава 2 «Міжнародне співробітництво у видавничій справі»;
- розділ V «Відповідальність за порушення норм цього Кодексу».

**Особлива частина** також складається з кількох розділів:

- розділ VI «Інформація як предмет правового регулювання»;
- розділ VII «Правовий режим інформаційної діяльності»;
- розділ VIII «Діяльність інформаційних агентств». Він містить декілька глав, зокрема: глава 1 «Діяльність і статус інформаційних агентств», глава 2 «Порядок заснування, державна реєстрація та припинення діяльності інформаційних агентств», глава 3 «Статус суб'єктів діяльності інформаційних агентств», глава 4 «Розповсюдження продукції інформаційного агентства», глава 5 «Особливості відповідальності за порушення цього Кодексу суб'єктами діяльності інформаційних агентств»;
- розділ IX «Правове регулювання діяльності друкованих засобів масової інформації», який складається з трьох глав: «Організація діяльності друкованих засобів масової інформації», «Діяльність редакцій друкованих засобів масової інформації» та «Відносини редакцій зі споживачами»;
- розділ X «Правові засади функціонування телебачення і радіомовлення», який складається з восьми глав: «Основа і заснування телерадіомовних організацій України та ліцензування каналів мовлення», «Організація телерадіомовлення», «Права і обов'язки телерадіоорганізацій та їх працівників», «Права телеглядачів і ра-



- діослухачів», «Матеріально-технічна база телерадіоорганізацій», «Правовий режим організації й роботи кабельного, цифрового та супутникового телебачення», «Супутникове мовлення», «Про систему Суспільного телебачення і радіомовлення України»;
- розділ XI «Діяльність мережі Інтернет в Україні» охоплює чотири глави, а саме: глава 1 «Державна політика України щодо Інтернету», глава 2 «Застосування державної мови в українському сегменті Інтернету», глава 3 «Реєстрація мережевих засобів масової інформації», глава 4 «Збір, використання і захист інформації персонального характеру»;
  - розділ XII «Видавнича діяльність» складається з трьох глав: «Особливості видавничої справи», «Організація і здійснення видавничої справи», «Припинення діяльності у видавничій справі та особливості відповідальності суб'єктів видавничої діяльності»;
  - розділ XIII «Правове регулювання рекламної діяльності як носія інформації» охоплює три глави: «Вимоги до реклами», «Особливості рекламування деяких видів продукції», «Контроль за дотриманням норм законодавства про рекламу»;
  - розділ XIV «Правовий режим політичної реклами та політичної агітації» складається з чотирьох глав, а саме: глава 1 «Засади правового регулювання політичної реклами та агітаційної діяльності», глава 2 «Політична рекламна та агітаційна діяльність в період офіційно оголошеної виборчої (референдумної) кампанії», глава 3 «Повноваження суб'єктів політичного процесу та органів державної влади», глава 4 «Особливості контролю за політичною рекламою і політичною агітацією»;
  - розділ XV «Інформаційна безпека як складова частина Національної безпеки України» складається з чотирьох глав: «Основи державної політики щодо інформаційної безпеки України», «Організаційно-правові засади становлення та розвитку національного інформаційного простору України», «Захист національного інформаційного простору України», «Контроль за дотриманням та відповідальність за порушення законодавства про інформаційну безпеку України»;
  - розділ XVI «Організація соціального захисту журналістів та особливості трудових відносин»;

- розділ XVII «Досудовий розгляд спорів і конфліктів, що виникають в інформаційній сфері»;
- розділ XVIII «Прикінцеві положення».

У цілому дослідження вищезазначених проектів Інформаційного кодексу України дали змогу дійти висновку про неоднозначне розуміння фахівцями змісту інформаційного законодавства, хоча визначення обсягу нормативного матеріалу, який підлягає кодифікації, є одним із найважливіших етапів процесу кодифікації. На наше переконання, дана проблема лежить в методологічній площині: науковій і теоретичній потребі з'ясування змісту інформаційних правовідносин і правових відносин в інформаційній сфері<sup>77</sup>. До того ж правова база у сфері інформації з обмеженим доступом чомусь на викликає зацікавленості серед науковців як окремий напрям кодифікаційної роботи.

### *Проект В. Ліпкана та В. Залізняка*

Структурно Інформаційний кодекс України має складатися з преамбули, трьох частин : загальної, особливої та спеціальної та прикінцевих положень.

**Загальна частина** охоплює 6 розділів, що розподіляються на відповідні глави.

*Перший розділ* «Основні положення» має розкривати зміст основних понять (інформація, інформаційне законодавство, інформаційні ресурси, інформаційна безпека, інформаційні відносини, документ, інформаційна інфраструктура, інформаційні технології, інформаційно-комунікаційні технології, доступ до інформації, режими доступу до інформації, інформація з обмеженим доступом, конфіденційна інформація, державна таємниця, банківська таємниця, персональна інформація (інформація про особу), інформаційні права і свободи, право на інформацію тощо).

*Другий розділ* «Основи інформаційного законодавства» має бути присвячений визначенню особливостей інформаційного законодав-

<sup>77</sup> Перов Д. О. Ознаки правових відносин в інформаційній сфері / Д. О. Перов // Правові та політичні проблеми сучасності : матеріали наук.-практ. конф., (м. Луцьк, 22 квіт. 2012 р.). — К., 2012. — С. 35–37.; Дімчогло М. І. Окремі принципи інформаційних правовідносин / М. І. Дімчогло // Національна і міжнародна безпека в сучасних трансформаційних процесах : матеріали конференції. — К., 2011. — С. 59–61.

ства, місця Інформаційного кодексу України в інформаційному законодавстві, структури, завдань і принципів інформаційного законодавства, сфери дії.

*Третій розділ* «Об'єкти інформаційних відносин» характеризуватиме специфіку та багатоаспектність об'єктів інформаційних відносин і складатиметься з декількох підрозділів:

- підрозділ 3.1 «Галузі та види інформації»;
- підрозділ 3.2 «Джерела інформації»;
- підрозділ 3.3 «Правовий режим інформації»;
- підрозділ 3.4 «Кругообіг інформації», який поділяється на глави:
  - глава 3.4.1 «Створення інформації»;
  - глава 3.4.2 «Поширення інформації»;
  - глава 3.4.3 «Зберігання інформації»;
  - глава 3.4.4 «Знищення інформації».

*Четвертий розділ* під назвою «Суб'єкти інформаційних відносин та їх права і обов'язки» також складатиметься з підрозділів:

- 4.1 «Суб'єкти інформаційних відносин»;
- 4.2 «Права і обов'язки людини та громадянина в інформаційній сфері»;
- 4.3 «Напрями державної політики в інформаційній сфері»;
- 4.4 «Повноваження органів державної влади в інформаційній сфері»;
- 4.5 «Повноваження органів місцевого самоврядування у інформаційній сфері»;
- 4.6 «Права та обов'язки приватних юридичних осіб у інформаційній сфері»;
- 4.7 «Гарантії реалізації інформаційних прав і свобод людини та громадянина».

*П'ятий розділ* «Міжнародне співробітництво в інформаційній сфері» присвячено міжнародно-правовим засадам співробітництва України з іншими державами та міжнародними організаціями в інформаційній сфері. Він має кілька підрозділів:

- 5.1 «Міжнародна інформаційна діяльність»;
- 5.2 «Правові та організаційні засади співробітництва з іншими державами в інформаційній сфері»;
- 5.3 «Взаємодія України з міжнародними організаціями в інформаційній сфері».

*Шостий розділ* «Відповідальність за порушення інформаційного законодавства України» складається з декількох підрозділів:

- 6.1 «Відповідальність за порушення інформаційного законодавства»;
- 6.2 «Звільнення від відповідальності за порушення інформаційного законодавства»;
- 6.3 «Вирішення спорів і конфліктів, що виникають в інформаційній сфері»;
- 6.4 «Контроль за дотриманням інформаційного законодавства».

**Особлива частина Інформаційного кодексу України** відповідає основним галузям інформаційного права України. Таким чином, Особлива частина складається з декількох розділів:

- *розділ сьомий* «Правове регулювання діяльності засобів масової інформації» охоплює такі підрозділи:
  - 7.1 «Діяльність друкованих засобів масової інформації»;
  - 7.2 «Правові засади функціонування телебачення і радіомовлення»;
  - 7.3 «Діяльність мережі Інтернет в Україні»;
  - 7.4 «Діяльність інформаційних агентств»;
  - 7.5 «Телекомунікаційна діяльність»;
- розділ 8 «Правове регулювання бібліотечної діяльності»;
- розділ 9 «Правове регулювання архівної діяльності»;
- розділ 10 «Правове регулювання рекламної діяльності»;
- розділ 11 «Правове регулювання телемедицини»;
- розділ 12 «Правове регулювання електронної торгівлі»;
- розділ 13 «Правове регулювання дистанційного навчання»;
- розділ 14 «Правове регулювання кінематографії»;
- розділ 15 «Правове регулювання інтелектуальної власності»;
- розділ 16 «Інформаційна безпека України», який складається з таких підрозділів:
  - 16.1 «Основні засади інформаційної безпеки України»;
  - 16.2 «Національні інтереси в інформаційній сфері»;
  - 16.3 «Загрози інформаційній безпеці України»;
  - 16.4 «Система забезпечення інформаційної безпеки України»;
  - 16.5 «Напрями державної політики у сфері інформаційної безпеки України»;
- розділ 17 «Прикінцеві положення».

Саме тому, зважаючи на динаміку інформаційних відносин, в **Спеціальній частині** мають міститися розділи, присвячені формуванню новітніх інститутів інформаційного права (правовідносини в соціальних мережах, Інтернет-телебачення, інформаційні операції, маніпулювання свідомістю, цифрометрія, інформація з обмеженим доступом тощо). Дана частина має фактично виступати дзеркалом майбутнього розвитку інформаційного суспільства. Оскільки тема є складною і потребує окремих наукових досліджень, то в рамках даного дослідження було надано наше концептуальне бачення без конкретизації Спеціальної частини, натомість у наших подальших наукових розвідках ці положення знаходитимуть своє наукове віддзеркалення.

Таким чином, тривалий час необхідність кодифікації інформаційного законодавства мала лише теоретичний характер. Однак, оскільки кодифікаційні акти мають високу юридичну цінність, внутрішню узгодженість та можливість регулювати широке коло правових відносин, то на сучасному етапі правотворення у наукових вітчизняних і зарубіжних колах спостерігається єдність позицій щодо необхідності створення Інформаційного кодексу України. Маємо надію, що врахування авторських пропозицій і теоретичного доробку щодо структури майбутнього кодифікаційного акта сприятиме підвищенню ефективності правового регулювання інформаційних відносин в Україні.

# **ОСОБЛИВОСТІ АДМІНІСТРАТИВНО-ПРАВОВИХ РЕЖИМІВ ОКРЕМИХ ВИДІВ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ**

---

---

- 4.1 АДМІНІСТРАТИВНО-ПРАВОВИЙ РЕЖИМ ДЕРЖАВНОЇ ТАЄМНИЦІ
- 4.2 АДМІНІСТРАТИВНО-ПРАВОВИЙ РЕЖИМ ПЕРСОНАЛЬНИХ ДАНИХ (ІНФОРМАЦІЯ ПРО ФІЗИЧНУ ОСОБУ)
- 4.3 АДМІНІСТРАТИВНО-ПРАВОВИЙ РЕЖИМ СЛУЖБОВОЇ ІНФОРМАЦІЇ







Окреслення стану адміністративно-правових режимів інформації з обмеженим доступом буде здійснюватись через дослідження чинного українського законодавства, зокрема шляхом висвітлення адміністративно-деліктного законодавства у цій сфері та визначення адміністративного статусу відповідних суб'єктів.

Як зазначалось у попередніх розділах, інформація з обмеженим доступом згідно з Законом України «Про доступ до публічної інформації» поділяється на:

- 1) конфіденційну інформацію;
- 2) таємну інформацію;
- 3) службову інформацію.

Кожен із цих видів інформації з обмеженим доступом має певну специфіку в сенсі адміністративно-правового регулювання, а тому потребує більш детального розгляду. У зв'язку з тим, що вищезазначені види інформації з обмеженим доступом, своєю чергою, також можуть бути класифіковані на певну кількість підвидів, вважаємо за необхідне у рамках цієї роботи розглянути найбільш важливі підвиди конфіденційної та таємної інформації, зокрема стан та перспективи розвитку адміністративно-правового регулювання персональних даних (інформації про фізичну особу), державної таємниці та службової інформації відповідно.

## 4.1 АДМІНІСТРАТИВНО-ПРАВОВИЙ РЕЖИМ ДЕРЖАВНОЇ ТАЄМНИЦІ

### *Нормативно-правове регулювання суспільних відносин у сфері державної таємниці*

Державна таємниця як вид інформації з обмеженим доступом є найбільш урегульованою чинним законодавством. Більш того, саме цей вид таємниці першим знайшов відповідне правове закріплення у вітчизняному законодавстві.

Так, Закон України «Про державну таємницю» був прийнятий ще 21 січня 1994 року [40].

Щодо інших видів таємниць, то в науковій літературі дискусійними залишаються навіть назви деяких видів таємниць та загалом відсутнє адекватне закріплення їх правового режиму.

Насамперед це пов'язано з тим, що захист державної таємниці має для будь-якої незалежної держави надзвичайно вагомe значення, оскільки відомості, що складають її зміст, завжди є стратегічно важливими в магістральних сферах життєдіяльності суспільства.

Витік, розголошення чи втрата такої інформації загрожує інтересам держави. Тому захист державної таємниці був й залишається складовою частиною системи національної безпеки будь-якої країни, про що свідчить наявність чинних нормативно-правових актів та створення відповідної спеціалізованої системи інституцій.

Саме тому в Законі України «Про основи національної безпеки України» визначається, що «на сучасному етапі основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві в інформаційній сфері є: розголошення інформації, яка становить державну ...таємницю...» [51]. Оскільки серед основних напрямів державної політики з питань національної безпеки, які закріплені цим же нормативно-правовим актом, відсутній захист державної таємниці, що, на нашу думку, є абсолютно неправильним, усунення цієї прогалини на законодавчому рівні є невідкладним завданням.

Державна таємниця існує у всіх країнах світу і є невід'ємною складовою суверенітету і системи управління, однак права, обов'язки і відповідальність кожного суб'єкта інформаційних відносин мають бути визначені як національним законодавством, так і міжнародними пра-

вовими нормами, а також мають бути розв'язані організаційні питання використання інформаційних ресурсів для потреб безпеки держави [191, с. 51].

Більшість розвинених країн мають відповідні правові акти у цій сфері [148–159] та впроваджують необхідні заходи для захисту державної таємниці. Здебільшого в країнах колишнього радянського табору такі акти мають назву «Про державну таємницю», хоча ряд держав ухвалили закони «Про державні секрети» чи «Про захист державних секретів».

Щодо країн-членів НАТО, то «Польща, Чехія, Болгарія, Румунія, Словенія розробили на підставі нових принципів акти щодо захисту класифікованої інформації, Словаччина — акт щодо захисту класифікованих матеріалів, а Угорщина, Латвія, Литва та Естонія адаптували раніше існуючі у них закони про захист державних та офіційних секретів або державної таємниці» [7, с. 86–87].

Важливість захисту державної таємниці підтверджується також тим, що даному питанню приділена відповідна увага і міжнародних інституцій: НАТО, ОБСЄ, ООН, які визначають загальні засади захисту державної таємниці, хоча і зазначають, що така діяльність є суто внутрішньою справою кожної держави.

Практично кожний факт порушення встановлених правил поведіння з державною таємницею становить джерело небезпеки, про що свідчить і міжнародний досвід захисту секретної інформації [160, с. 7; 161, с. 7].

Нині між Україною та багатьма іноземними державами існують ратифіковані угоди щодо спільної діяльності з охорони таємниць [162, с. 4]. Зокрема такі угоди про взаємну охорону секретної інформації протягом 2001–2011 рр. були підписані між Кабінетом Міністрів України та урядами Демократичної Соціалістичної Республіки Шрі-Ланка, Великої Соціалістичної Народної Лівійської Арабської Джамагірією, Республіки Екваторіальна Гвінея, Естонської Республіки, Соціалістичної Республіки В'єтнам, Ісламської Республіки Пакистан, Республіки Албанія, Республіки Хорватія, Азербайджанської Республіки, Латвійської Республіки, Чеської Республіки, Республіки Таджикистан, Республіки Індія, Киргизької Республіки, Республіки Македонія, Республіки Казахстан, Республіки Вірменія, Грузії, Грецької Республіки, Республіки Польща, Туркменистану, Італійської Республіки, Держави Ізраїль,

Російської Федерації, Китайської Народної Республіки, Французької Республіки.

Інколи українська сторона говорить про необхідність перегляду певних засад цих угод задля вдосконалення механізму захисту державної таємниці [162, с. 4].

Як зауважує А. М. Благодарний, нерідко в законах, якими ратифікують міжнародні угоди, в систему законодавства включаються норми, що виражені в підзаконних нормативних актах [163, с. 21]. Це створює в практиці правозастосування колізію норм, ігнорування норм закону на користь норм підзаконного акта [164, с. 35].

Отже, концептуальним нормативно-правовим актом, що регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України, з численними змінами та доповненнями (внесеними згідно із законами України від 21 вересня 1999 року [165], від 19 червня 2003 року [166], від 19 лютого 2004 року [167], від 21 травня 2008 року [168], від 6 липня 2010 року [169], від 7 жовтня 2010 року [170], від 3 лютого 2011 року [171]) нині є **Закон України «Про державну таємницю»**.

Крім вищезазначеного Закону, суспільні відносини у сфері охорони державної таємниці урегульовано на рівні значного кола підзаконних нормативно-правових актів, а саме:

- Постанови Кабінету Міністрів України «Про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці» від 15 червня 1994 року [172];
- Постанови Кабінету Міністрів України «Питання Державного комітету з питань державних секретів» від 16 червня 1993 року [173];
- Наказу Міністерства охорони здоров'я України і Служби безпеки України «Про затвердження Переліку психічних захворювань (розладів), які можуть завдати шкоди охороні державної таємниці і за наявності яких допуск до державної таємниці громадянинові не надається» від 13 травня 2002 року [174] тощо.

## Поняття «державна таємниця»

Відповідно до ст. 1 Закону України «Про державну таємницю» **державна таємниця (секретна інформація)** визначається як вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [40].

Навіть поверховий аналіз цієї дефініції викликає ряд запитань. *За яким критерієм виділено законодавцем саме ці сфери? Чому лише розголошення може завдати шкоди? Як, наприклад, щодо втрати матеріальних носіїв під час пожежі, на яких розташована інформація, що має характер державної таємниці? Що становить собою шкода національній безпеці? Охоплює вона матеріальний чи моральний аспекти? Шкода завдається національній безпеці чи національним інтересам?*

Водночас, у визначенні поняття державної таємниці законодавець вказує на наявність декількох ознак.

1. Таємність інформації, тобто обмеженість доступу до неї.
2. Значущість, важливість такого роду відомостей у певний проміжок часу для інтересів держави, тобто в разі розголошення державної таємниці національній безпеці України може бути завдана шкода матеріального чи іншого характеру.
3. Чітке визначення сфер, у яких може існувати державна таємниця, а саме: оборона, економіка, наука і техніка, зовнішні відносини, державна безпека й охорона правопорядку.
4. Узаконення відомостей, що становлять державну таємницю, тобто визначення переліку таких відомостей у спеціальному правовому акті — Зводі, на підставі та в межах якого створюються розгорнуті переліки відомостей, що становлять державну таємницю.
5. Охорона такої інформації здійснюється винятково державою, тобто встановлення на підставі чинного законодавства єдиного порядку забезпечення охорони зазначеної інформації державно-правовими засобами.

На думку М. М. Іванова, **державну таємницю** становлять «передбачені в спеціальних переліках, особливо охоронювані в даний час і

такі, що мають важливе значення для оборонних та інших державних інтересів, конкретні відомості різного характеру, перехід яких у розпорядження іноземної держави може завдати шкоди цим інтересам» [175, с. 101].

Виникає питання, що означає особливо (Підкреслено нами. — Авт.) охоронювані? Чому ці відомості мають важливе значення винятково для оборонних та інших державних (Підкреслено нами. — Авт.) інтересів? Як щодо суспільних? Чому лише перехід (Підкреслено нами. — Авт.) цих відомостей у розпорядження іноземної держави може завдати шкоди? Чи не завдається шкода національним інтересам у разі втрати таких відомостей, якщо при цьому ними не заволоділа іноземна держава? Та наостанок, чи не буде заподіяння шкоди переходом відомостей, що становлять державну таємницю, не до іноземної держави, а до криміналітету?

Аналіз емпіричної бази у цій сфері надає можливість з впевненістю зазначити, що головним порушником законодавства про державну таємницю є насамперед не іноземні держави, а саме «звичайні» особи (хакери) чи то для власного задоволення чи з метою отримання прибутку. Наприклад, оприлюднення наприкінці 2010 року офіційних документів Державного департаменту США у мережі «WikiLeaks», засновники якого за попередніми даними заробили близько одного мільярда євро.

Ці документи-депеші були надіслані американськими дипломатичними службами вищого рангу з 274 посольств і представництв США зі всього світу в Держдепартамент, а також з канцелярії держсекретаря в американські представництва, включаючи представництва в НАТО й ООН. У них містилася інформація про країни, в яких вони працюють, відгуки про політичну еліту та вищих державних осіб цих країн тощо.

Загалом було розсекречено 15652 документи під грифом «таємно», 101748 — під грифом «конфіденційно», 133887 — під грифом «для службового користування».

Розсекречення цих даних викликало різні оцінки. З боку громадськості, як правило, позитивні. Так, український політик Олег Ляшко навіть ініціював проект «Україна у WikiLeaks: політика без грифу», де українською мовою надаються для ознайомлення широкого загалу автентичні документи-відгуки про нашу державу, вітчизняних політичних лідерів дипломатичних служб, які працюють в Україні.

«Прочитавши документи з «WikiLeaks», усвідомлюєш, що подвійні стандарти вже не можуть залишатися одним із успішних методів сучасної зовнішньої і внутрішньої політики. Реальні мотиви неодмінно стануть надбанням громадськості. До того ж з цифровою швидкістю» [176, с. 1].

Більш обґрунтованим вважається визначення поняття «державна таємниця» І. М. Даньшина, який визначає державну таємницю як відомості військового, економічного та іншого важливого значення, що в їх збереженні особливо зацікавлена наша держава, перелік яких затверджується вищими органами держави [177, с. 51].

З одного боку, це визначення дещо збігається з нормативно закріпленою Законом України «Про державну таємницю» дефініцією. З іншого — не враховано важливого моменту, що у збереженні відомостей, які становлять державну таємницю, зацікавлена не лише держава, а й суспільство загалом. Крім того, перелік відомостей, що становлять державну таємницю, має бути не лише затвердженим вищими органами держави, тобто включення цієї інформації до Зводу відомостей, що становлять державну таємницю, а й з обов'язкове опублікування цього Зводу, змін до нього.

### ***Система органів, що покликані забезпечити захист державної таємниці***

Крім легальної дефініції державної таємниці, Закон України «Про державну таємницю» закріпив також інші важливі засади правового режиму державної таємниці в Україні, а саме: компетенцію державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці; порядок віднесення інформації до державної таємниці; процедуру засекречування та розсекречування матеріальних носіїв інформації; основні заходи організаційного, правового характеру щодо охорони державної таємниці тощо.

Серед державних інституцій, що мають необхідні повноваження у сфері захисту державної таємниці, слід виділити *Верховну Раду України, Президента України, Раду національної безпеки та оборони України, Кабінет Міністрів України, центральні та місцеві органи виконавчої влади, Раду міністрів Автономної Республіки Крим, а також органи місцевого самоврядування.*



Так, державну політику щодо державної таємниці як складову за-сад внутрішньої та зовнішньої політики визначає Верховна Рада України; Президент України — видає укази та розпорядження з питань охорони державної таємниці; Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці; Кабінет Міністрів України спрямовує та координує роботу міністерств, інших органів виконавчої влади щодо забезпечення здійснення державної політики у сфері охорони державної таємниці тощо.

Спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці є Служба безпеки України (СБУ). Задля цього СБУ має необхідні повноваження, зокрема: брати участь у розробці та здійсненні відповідно до Закону України «Про державну таємницю» та інших актів законодавства заходів щодо забезпечення охорони державної таємниці та конфіденційної інформації, що є власністю держави, сприяти у порядку, передбаченому законодавством, підприємствам, установам, організаціям та підприємцям у збереженні комерційної таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України [178].

### ***Етапи віднесення інформації до державної таємниці***

Процедура визнання інформації державною таємницею є довготривалою та доволі складною. Можна виділити три основні етапи віднесення інформації до державної таємниці.

На *першому етапі* вона розпочинається з діяльності державного експерта з питань таємниць, виконання функцій якого покладено на конкретних посадових осіб, зокрема у Верховній Раді України на Голову Верховної Ради України; в інших державних органах, Національній академії наук України, на підприємствах, в установах і організаціях — Президентом України за поданням Служби безпеки України на підставі пропозицій керівників відповідних державних органів, Національної академії наук України, підприємств, установ і організацій.

Віднесення інформації до державної таємниці здійснюється мотивованим рішенням державного експерта з питань таємниць за його власною ініціативою, за зверненням керівників відповідних держав-

них органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян [40].

На *другому етапі* Служба безпеки України на підставі рішень державних експертів з питань таємниць формує Звід відомостей, що становлять державну таємницю.

На *третьому етапі* здійснюється опублікування Зводу відомостей, що становлять державну таємницю, в офіційних виданнях України. Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи змін до нього.

### ***Звід відомостей, що становлять державну таємницю***

**Звід відомостей, що становлять державну таємницю, — акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених сферах.**

Чинним нині є ЗВДТ, затверджений Наказом СБ України ще 12 серпня 2005 року № 440 [179]. Хоча до цього Наказу протягом 2006 — 2010 рр. було внесено ряд змін та доповнень, зокрема наказами Служби Безпеки від 24 січня 2006 року, 25 квітня 2006 року, від 12 жовтня 2006 року, від 15 лютого 2007 року, від 28 грудня 2007 року, від 17 червня 2008 року, від 5 листопада 2008 року, від 16 березня 2009 року, від 25 листопада 2009 року, від 24 лютого 2010 року, від 23 липня 2010 року [180–190].

Вагомі нормативно-правові акти у сфері інформації з обмеженим доступом були прийняті в 2011 році, що змінили змістовне наповнення інституту таємниць, а тому дивно, що нині відсутні будь-які зміни чи доповнення до Зводу відомостей, що становлять державну таємницю.

На підставі та в межах ЗВДТ органи державної влади України створюють галузеві, відомчі, міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю. Основною метою таких переліків є конкретизація та систематизація даних про інформацію, що віднесена до державної таємниці. Зазначені розгорнуті переліки мають не суперечити ЗВДТ.

Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов'язану із державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з держав-

ною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю. Але виникає необхідність погодження їх зі Службою безпеки України та затвердження державними експертами з питань таємниць, а також реєстрації у Службі безпеки України.

Практика використання подібних розгорнутих переліків вже успішно апробована і деякими іноземними державами, наприклад, Російською Федерацією [191, с. 7].

### ***Строки, протягом яких діє рішення про віднесення інформації до державної таємниці***

Відповідно до ч. 1 ст. 13 Закону України «Про державну таємницю» строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. Він не може перевищувати для інформації із ступенем секретності «особливої важливості» — 30 років, для інформації «цілком таємно» — 10 років, для інформації «таємно» — 5 років [40].

Встановити триваліші строки дії рішень про віднесення інформації до державної таємниці, може винятково Президент України або з власної ініціативи, або на підставі пропозицій державних експертів з питань таємниць, або за зверненням державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян. Хоча порядок подовження строків дії рішень про віднесення інформації до державної таємниці Президентом України за зверненням державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян на законодавчому рівні не закріплено.

Після закінчення строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць має скасувати рішення про віднесення її до державної таємниці або прийняти рішення про продовження строку дії зазначеного рішення.

## *Перелік інформації, що не може бути віднесена до державної таємниці*

До державної таємниці може бути віднесено значний спектр інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку.

Водночас забороняється відносити до державної таємниці будь-які відомості, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

У ст. 8 Закону України «Про державну таємницю» законодавцем чітко визначено, яка інформація не може належати до державної таємниці:

- про стан довкілля, про якість харчових продуктів і предметів побуту;
- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;
- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;
- про факти порушень прав і свобод людини і громадянина;
- про незаконні дії державних органів, органів місцевого самоврядування та їх посадових осіб;
- інша інформація, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена [40].

Наявність у зазначеній статті бланкетної норми та, як наслідок, відсутність чіткого переліку інформації, що не може бути віднесена до державної таємниці, на нашу думку, може сприяти зловживанню в цій сфері, коли окремі відомості необґрунтовано відносять чи навпаки не відносять до державної таємниці, аргументуючи це неможливістю звуження змісту й обсягу конституційних прав та свобод людини і громадянина чи можливістю завдання шкоди здоров'ю та безпеці населення.

Крім того, ряд норм дещо не відповідають нормам Закону України «Про інформацію». Так, у ст. 21 цього Закону визначено які відомості не

можуть бути віднесені до інформації з обмеженим доступом. Але у п. 5 цієї самої статті вже зазначається про незаконні дії органів державної влади (Підкреслено нами. — Авт.), органів місцевого самоврядування, їх посадових та службових осіб (Підкреслено нами. — Авт.), а також у п. 6 вже говориться про інші відомості (Підкреслено нами. — Авт.), доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Таким чином, перелік інформації, що не може бути обмежено є дещо не уніфікованим, а тому може сприяти зловживанням у цій сфері з боку органів державної влади, посилаючись на колізійні норми.

### ***Відповідальність за порушення законодавства у сфері державної таємниці***

Розділ VI Закону України «Про державну таємницю» присвячений питанню відповідальності за порушення законодавства про державну таємницю.

Визначено перелік правопорушень у цій сфері:

- розголошення державної таємниці;
- втрата документів та інших матеріальних носіїв секретної інформації;
- недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;
- засекречування інформації чи навмисне невіднесення до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України;
- необґрунтоване заниження ступеня секретності або необґрунтоване розсекречування секретної інформації;
- безпідставне засекречування інформації; надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці;
- ненадання грифа секретності матеріальним носіям інформації, що становить державну таємницю;
- безпідставне скасування чи зниження грифа секретності матеріальних носіїв секретної інформації;
- порушення встановленого законодавством порядку надання допуску та доступу до державної таємниці;

- порушення встановленого законодавством режиму секретності та невиконання обов'язків щодо збереження державної таємниці;
- невжиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці;
- провадження діяльності, пов'язаної з державною таємницею, без одержання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщення державних замовлень на виконання робіт, доведення мобілізаційних завдань, пов'язаних з державною таємницею, в державних органах, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;
- недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними; невиконання норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або просочення її технічними каналами тощо.

Залежно від суспільної небезпечності цих правопорушень передбачаються такі види юридичної відповідальності, як дисциплінарна, адміністративна та кримінальна.

На думку Ю. Мірошника, «найбільшу суспільну небезпеку в сфері державної таємниці представляють наступні загрози: втрата таємної інформації; викривлення останньої; несанкціоноване користування таємною інформацією; використання таємних інформаційних ресурсів зі злочинною метою. Вони мають серйозні наслідки, які вимагають оцінки з позиції забезпечення національних інтересів. Завжди існує загроза, що система захисту таємної інформації не дасть бажаних результатів, її буде використано у злочинних цілях» [192, с. 33].

Хоча державна таємниця як вид інформації з обмеженим доступом є законодавчо врегульованою, тобто у вітчизняному праві наявні відповідні норми, що регулюють суспільні відносини в цій сфері, а також створені відповідні спеціалізовані інституції, що покликані забезпечувати її захист, говорити про високий рівень її забезпечення неможли-

во. Даний факт підтверджується статистичними даними, відповідно до яких кількість осіб, щорічно притягнутих до адміністративної відповідальності за вчинення порушення законодавства про державну таємницю, постійно збільшується.

### **Основні причини вчинення адміністративних порушень законодавства про державну таємницю**

Серед основних проблем, що негативно впливають на стан адміністративно-правового захисту державної таємниці, слід виділити соціально-економічні, кадрові, організаційні тощо.

Так, витік інтелектуального потенціалу з метою розв'язання своїх соціально-економічних проблем, є доволі серйозною загрозою захисту державної таємниці. Як зауважує Ю. Телюга, «саме з емігрантами Україна втрачає більшість власних секретів».

Не менш впливовим фактором незадовільного стану забезпечення державної таємниці є плінність кадрів, що працювали в режимно-секретних органах. За деякими статистичними даними, протягом останніх 5 років близько 80 % спеціалістів режимно-секретних органів звільнилися.

Тим більше, розвиток інформаційно-телекомунікаційних технологій вимагає від осіб, що здійснюють діяльність у сфері захисту державної таємниці, не лише мати відповідні знання, вміння та навички у правовій сфері, а й необхідний рівень спеціальних знань, вмінь та навичок у сфері інформаційних технологій, а також обізнаності зі специфікою діяльності правоохоронних органів та змістом завдань, на вирішення яких спрямована діяльність таких органів.

Нині спеціалісти, що навчалися за фахом «правознавство» не мають належної підготовки для роботи з новітніми інформаційними технологіями і навпаки, спеціалісти з ІТ поверхово знайомі із законодавством.

Результати аналізу судових рішень по справах про адміністративні порушення законодавства про державну таємницю, наданих А. М. Благодарним, свідчать, що *основними причинами вчинення адміністративних порушень законодавства про державну таємницю є:*

- недостатнє знання деякими особами, що мають допуск і доступ до державної таємниці, норм чинного законодавства про державну таємницю;



- нехтування деякими особами, що мають допуск і доступ до державної таємниці, нормами чинного законодавства. Так, деякі керівники підприємств, установ та організацій, які провадять діяльність, пов'язану з державною таємницею, вважають, що вони не володіють інформацією, розголошення якої може завдати шкоди національній безпеці України [163, с. 159].

А тому, справді, актуальною є пропозиція авторів передбачити у Законі України «Про державну таємницю» обов'язкове проведення перевірки знання норм законодавства про державну таємницю та правил секретного діловодства особами, яким надається допуск до державної таємниці [163, с. 159].

З цього приводу додамо, що доречно передбачити проведення перевірки знання норм законодавства про державну таємницю та правил секретного діловодства особами, яким надається не лише допуск до державної таємниці, а й доступ. Також механізм перевірки знань норм законодавства про державну таємницю можна передбачити на рівні певної Інструкції чи Правил, які розробила б СБ України як основний орган, що здійснює захист державної таємниці, та закріпила на рівні Наказу СБ України.

Тим більше, що це прямо передбачено в п. 7 ч. 1 ст. 24 Закону України «Про Службу безпеки України», згідно з яким Служба безпеки України відповідно до своїх основних завдань зобов'язана брати участь у розробці і здійсненні відповідно до Закону України «Про державну таємницю» та інших актів законодавства заходів щодо забезпечення охорони державної таємниці [178] (Підкреслено нами. — Авт.)

І, нарешті, незадовільне фінансування режимно-секретних установ, організацій та підприємств призводить до неналежного обладнання приміщень РСО чи істотної застарілості форм і методів її захисту. Особливо це стосується того факту, що ряд державних таємниць набувають цифрової форми, а тому для фахівців з ІТ, які мають злочинні наміри та необхідні знання чи навички, не надто складно знайти доступ до них. Щодо державних інституцій, то у зв'язку з недостатнім фінансуванням, в РСО та інших установах, що мають забезпечувати захист державної таємниці, бракує не лише новітніх технологій чи засобів для її захисту, а немає навіть натяку на їх розроблення.

Більше того, практика провадження в справах про порушення законодавства про державну таємницю свідчить, що іноді на підприєм-

ствах, установах, організаціях, що провадять діяльність, пов'язану з державною таємницею, РСО не має ізольованого приміщення [193]; не працюють інженерно-технічні засоби охорони РСО; таємна інформація обробляється на неатестованих ПЕОМ [193].

### ***Перспективи розвитку адміністративно-деліктного законодавства у сфері захисту державної таємниці***

Загалом удосконалення інституту адміністративної відповідальності є одним із актуальних напрямів реформування вітчизняного адміністративного права, оскільки ряд норм КУпАП втратили свою актуальність чи навпаки існує нагальна потреба прийняття нових статей.

Тривалий час за порушення законодавства про державну таємницю була встановлена винятково кримінальна відповідальність. Нині Кримінальний кодекс України (КК України) містить ряд статей в контексті порушеної проблематики, а саме: розголошення державної таємниці (ст. 328 КК України), втрата документів, що містять державну таємницю (ст. 329 КК України), державна зрада (ст. 111 КК України), шпигунство (ст. 114 КК України) тощо.

Адміністративна відповідальність за порушення законодавства про державну таємницю була встановлена Законом України «Про внесення змін до Кодексу України про адміністративні правопорушення щодо встановлення відповідальності за порушення законодавства про державну таємницю», який був прийнятий Верховною Радою України 21 вересня 1999 року [194].

За цей час до даної статті було внесено незначні зміни та доповнено законами України «Про внесення змін до деяких законодавчих актів України» від 11 травня 2004 року [195] та «Про внесення змін до деяких законодавчих актів України щодо діяльності Державної служби спеціального зв'язку та захисту інформації України» від 19 березня 2009 року [196].

Отже, ст. 212–2 КУпАП передбачає такі склади правопорушень у сфері державної таємниці:

- 1) недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;
- 2) засекречування інформації:
  - про стан довкілля, про якість харчових продуктів і предметів побуту;

- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися та загрожують безпеці громадян;
  - про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти та культури населення;
  - про факти порушень прав і свобод людини і громадянина;
  - про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових осіб;
  - іншої інформації, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена;
- 3) безпідставне засекречування інформації;
  - 4) надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненадання грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставне скасування чи зниження грифа секретності матеріальних носіїв секретної інформації;
  - 5) порушення встановленого законодавством порядку надання допуску та доступу до державної таємниці;
  - 6) невжиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці;
  - 7) провадження діяльності, пов'язаної з державною таємницею, без отримання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщення державних замовлень на виконання робіт, доведення мобілізаційних завдань, пов'язаних з державною таємницею, в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;
  - 8) недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства та проведення роботи з ними;

9) невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності [197].

Розгляд всіх складових (об'єкта, суб'єкта, об'єктивної та суб'єктивної сторін) кожного із адміністративних правопорушень, відповідальність за вчинення яких встановлено у ст. 212–2 КУпАП, було детально розглянуто в дисертаційному дослідженні А. М. Благодарного «Адміністративна відповідальність за порушення законодавства про державну таємницю», а тому не будемо зупинятися на характеристиці цих складів адміністративних правопорушень.

Лише зауважимо, що ми погоджуємось із автором вищезазначеного дослідження, що «для створення логічно завершеного, ефективного правового регламентування адміністративної відповідальності за порушення законодавства про державну таємницю необхідно закріпити у чинному КУпАП (або у новому Кодексі України про адміністративні проступки) норму, яка б передбачала адміністративну відповідальність юридичних осіб за порушення законодавства про державну таємницю. Пропонується вважати дії юридичної особи винними, якщо вони є наслідком усвідомлюваних дій (бездіяльності) її посадових осіб, працівників, а також осіб, які не знаходяться з нею в трудових відносинах, але виконують певні дії в інтересах юридичної особи за договором» [163, с. 95].

Крім того, заслуговує на особливу увагу позиція дослідника щодо підвищення суми санкції як попередження адміністративних правопорушень, відповідальність за вчинення яких встановлено у ст. 212–2 КУпАП. Так, було обґрунтовано доцільність збільшення суми штрафу, що підлягає стягненню з порушників законодавства про державну таємницю, а саме за вчинення порушення законодавства про державну таємницю вперше пропонується накладення штрафу на фізичних осіб від трьох до п'яти неоподатковуваних мінімумів доходів громадян, а на посадових осіб — від семи до п'ятнадцяти неоподатковуваних мінімумів доходів громадян; за повторне протягом року вчинення порушення законодавства про державну таємницю пропонується накладення штрафу на фізичних осіб від чотирьох до десяти неоподатковуваних мінімумів доходів громадян, а на посадових осіб — від десяти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян або по-

збавлення права займатися діяльністю, що передбачає надання доступу до державної таємниці, на строк до одного року [163, с. 172].

Проте вважаємо також, беручи до уваги важливість правопорушень, передбачених ст. 212–2 КУпАП, розширити спектр адміністративних стягнень. Так, поряд зі штрафом за доцільне буде передбачення і таких стягнень, як: громадські роботи, виправні роботи, адміністративний арешт.

Не менш конструктивним вбачається необхідність посилення санкції за вчинення правопорушення, передбаченого ст. 212–2 КУпАП, у воєнний час або у військовій обстановці.

Необхідним напрямом удосконалення адміністративно-деліктного законодавства у цій сфері є внесення змін до ст. 212–2 КУпАП, зокрема об'єднати п. 1, відповідно до якого передбачено відповідальність за недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації та п. 8, згідно з яким передбачено відповідальність за недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства та проведення роботи з ними.

На нашу думку, п. 8 охоплює п. 1. Так, порушення порядку передачі державної таємниці іншій державі чи міжнародній організації і є одним із порушень вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства та проведення роботи з ними.

По-друге, дана стаття містить ряд оціночних понять, що потребують законодавчого визначення, серед яких «реальна загроза», «порушення цілісності», «безпідставне засекречування інформації» тощо.

Так, щодо «безпідставного засекречування інформації», то нині в чинному законодавстві відсутній перелік підстав засекречування інформації.

Чи можна вважати підставами засекречування інформації перелік інформації, що може бути віднесена до державної таємниці та перелік інформації, що не відноситься до державної таємниці, що визначено в ст. 8 Закону України «Про державну таємницю»? На нашу думку, ні. Саме тому слід чітко визначити на законодавчому рівні перелік підстав

засекречування інформації, щоб не було можливості уповноваженим особам довільно трактувати дану норму.

Тим більше не зрозуміло, чому надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці (п. 4 ч.1 ст. 212–2 КУпАП), є окремим складом проступку, хоча у п. 3. ч. 1. ст. 212–2 КУпАП передбачено адміністративну відповідальність за безпідставне засекречування інформації.

#### **4.2 АДМІНІСТРАТИВНО-ПРАВОВИЙ РЕЖИМ ПЕРСОНАЛЬНИХ ДАНИХ (ІНФОРМАЦІЯ ПРО ФІЗИЧНУ ОСОБУ)**

Серед наступного виду інформації з обмеженим доступом слід значити конфіденційну інформацію, яка згідно зі ст. 7 Закону України «Про доступ до публічної інформації» визначається як інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [59].

Як ми зазначали раніше, конфіденційна інформація також може бути класифікована за різними критеріями на кілька підвидів, а тому неможливо всебічно та об'єктивно розглянути в межах одного дослідження їх усі.

Зважаючи на те, що останнім часом набуло широкого наукового, громадського резонансу проблема захисту персональних даних, вважаємо за необхідне окреслити саме специфіку адміністративно-правового режиму захисту персональних даних (інформації про особу) як виду конфіденційної інформації.

Тим більше, що задекларований зовнішньополітичний курс України на інтеграцію з Європейським Союзом та ратифіковані Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року [198], а також Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 8 листопада 2001 року [199], що набрали чинності з 1 січня 2011 року, вимагають уніфікації правових засад захисту пер-



сональних даних, тобто є одним із магістральних напрямів співпраці України з вагомими міжнародними інституціями.

Європейське право охоплює більше двох десятків загальноєвропейських конвенцій, директив та рекомендацій з питань захисту персональних даних. Майже кожна розвинена країна світу, яка ратифікувала Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року та Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 8 листопада 2001 року, на їх основі ухвалила свої базові нормативно-правові акти задля захисту персональних даних у різноманітних сферах життєдіяльності суспільства як-от: медичній, статистичній, державній, журналістській, поліцейській тощо.

Не лише країни—члени ЄС прийняли такі акти, а аналогічні закони прийнято в багатьох країнах світу, у тому числі — в країнах СНД, зокрема в Росії. Тому прийняття Закону України «Про захист персональних даних» було б актуальним завданням для вітчизняної наукової еліти та законодавця.

Поряд із суспільними відносинами у сфері державної таємниці, суспільні відносини, пов'язані із захистом персональних даних під час їх обробки, також урегульовані на рівні окремого спеціалізованого нормативно-правового акта — **Закону України «Про захист персональних даних»** від 1 червня 2010 року, який набрав чинності 1 січня 2011 року [59].

Тривалий час суспільні відносини, пов'язані зі збиранням, зберіганням, використанням та поширенням інформації про особу (персональних даних) були урегульовані більш як двома десятками нормативно-правових актів України. Однак ці акти не відповідали міжнародному та європейському законодавству, зокрема щодо розуміння змісту персональних даних, а також вимог їх захисту. Крім того, в Інтернеті чи на спеціалізованих ринках України можна було без проблем придбати різні бази даних (ДАІ, податкової, телефонну базу 09 і т. ін.), що містили персональну інформацію.

Яскравим прикладом недостатньо ефективної діяльності нашої держави у сфері захисту персональних даних стала поява російського сайту Radarix, завдячуючи якому можна було отримати інформацію про народження, місце проживання, ідентифікаційний код особи, ви-



падки порушення вітчизняного законодавства та санкції, що були застосовані до правопорушників тощо. І це, беручи до уваги наявність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», у ст. 8 якого закріплено, що інформацію з обмеженим доступом, вимогу щодо захисту якої встановлено законом, слід обробляти в системі із застосуванням комплексного захисту інформації з підтвердженою відповідністю [200], а також передбачення кримінальної, цивільної тощо відповідальності у відповідних нормативно-правових актах (ст. 132 КК України «Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби», ст. 157 КК України «Перешкоджання здійсненню виборчого права або права брати участь у референдумі, роботі виборчої комісії або комісії з референдуму чи діяльності офіційного спостерігача (в частині умисного внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціоновані дії з інформацією, що міститься в базі даних Державного реєстру виборців, чи інше несанкціоноване втручання в роботу Державного реєстру виборців, вчинене службовою особою, яка має право доступу до цієї інформації, або іншою особою шляхом несанкціонованого доступу до бази даних Державного реєстру виборців)», ст. 163 КК України «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер», ст. 182 КК України «Порушення недоторканності приватного життя (незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди або поширення цієї інформації у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації)», ст. 232 КК України «Розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю», ст. 232–1 КК України «Незаконне використання інсайдерської інформації», ст. 328 КК України «Розголошення державної таємниці», ст. 329 КК України «Втрата документів, що містять державну таємницю», ст. 330 КК України «Передача або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави», ст. 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку,

що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації», ст. 361–2 КК України «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації», ст. 362 КК України «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї», ст. 363 КК України «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється», ст. 28 ЦК України «Ім'я фізичної особи», ст. 277 ЦК України «Спростування недостовірної інформації», ст. 296 ЦК України «Право на використання імені», ст. 301 ЦК України «Право на особисте життя та його таємницю», ст. 302 ЦК України «Право на інформацію», ст. 306 ЦК України «Право на таємницю кореспонденції», ст. 307 ЦК України «Захист інтересів фізичної особи при проведенні фото-, кіно-, теле- та відеозйомок», ст. 308 ЦК України «Охорона інтересів фізичної особи, зображеної на фотографіях та в інших художніх творах», ст. 226 Сімейного кодексу України (СК України) «Право на таємницю усиновлення», ст. 227 СК України «Право на приховання факту усиновлення від дитини, яка усиновлена», ст. 228 СК України «Забезпечення таємниці усиновлення» тощо).

### ***Історія ухвалення Закону України***

#### ***«Про захист персональних даних»***

Необхідність прийняття Закону України «Про захист персональних даних» було ініційовано ще в 2005 році. Більше того, було розроблено декілька законопроектів. 16 березня 2006 року депутати 287-ма голосами ухвалили Закон України «Про захист персональних даних» (законопроект М. Родіонова, С. Ніколаєнко І. Юхновського та ін. № 2618). Але Закон так і не був прийнятий, оскільки Президент України наклав на нього вето, аргументуючи тим, що концептуальні засади

Закону не узгоджуються з нормами Конституції України і з вимогами міжнародно-правових актів, а також наявна низка внутрішніх колізій в цьому Законі, що уможлиблює в майбутньому порушення конституційних прав людини, невиконання міжнародних зобов'язань України.

Після процедури вето закону проект повернувся до парламенту і на черговому розгляді новообраним складом Верховної Ради України Закон було ухвалено в цілому і знову направлено Президенту України, який 30 січня 2007 року також скористався правом вето. Після декількох спроб подолати право вето Президента України 18 травня 2007 року Закон було відхилено.

У новому авторському складі (О. А. Баранов, В. М. Брижко, І. Б. Жиляев, Г. В. Карпов, Т. А. Качка, О. Б. Шевчук, В. М. Литвин, В. І. Полохало, К. С. Самойлик) проект Закону України «Про захист персональних даних» було зареєстровано 25 березня 2008 року. 25 червня 2009 року цей законопроект було ухвалено в першому читанні, а 1 червня 2010 року — в цілому. 24 червня 2010 року він був підписаний Президентом України, а законної сили Закон набув 7 липня 2010 року, з застереженням, що чинності набуває з 1 січня 2011 року, оскільки Кабінету Міністрів України протягом шести місяців з дня набрання чинності цим Законом слід забезпечити прийняття нормативно-правових актів, передбачених цим Законом та забезпечити приведення своїх нормативно-правових актів у відповідність із цим Законом.

## **Основні засади Закону України**

### **«Про захист персональних даних»**

Даний правовий документ закріплює основоположні засади захисту персональних даних, зокрема *права і обов'язки суб'єктів відносин*, пов'язаних із персональними даними, серед яких виділяють суб'єкта персональних даних (фізичну особу, стосовно якої відповідно до закону здійснюється обробка її персональних даних); володільця бази персональних даних (фізичну або юридичну особу, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом); розпорядника бази персональних даних (фізичної чи юридичної особи, якій володільцем бази персональних даних

або законом надано право обробляти ці дані); третьої особи (будь-якої особи, за винятком суб'єкта персональних даних, володільця чи розпорядника бази персональних даних та уповноваженого державного органу з питань захисту персональних даних, якій володільцем чи розпорядником бази персональних даних здійснюється передача персональних даних відповідно до закону); уповноваженого державного органу з питань захисту персональних даних (центрального орган виконавчої влади, до повноважень якого належить захист персональних даних, що утворюється відповідно до законодавства), інших органів державної влади та органів місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних.

Згідно зі ст. 5 цього акта «персональні дані, крім знеособлених персональних даних, за режимом доступу є інформацією з обмеженим доступом» [139]. Виняток складають персональні дані певних категорій громадян. Так, персональні дані фізичної особи, яка претендує зайняти чи займає виборну посаду (у представницьких органах) або посаду державного службовця першої категорії, не належать до інформації з обмеженим доступом.

Згідно зі ст. 25 Закону України «Про державну службу» від 16 грудня 1993 року [201] перша категорія — посади перших заступників міністрів, керівників центральних органів виконавчої влади, які не є членами Уряду України, їх перших заступників, Постійного Представника Президента України в Автономній Республіці Крим, голів обласних, Київської та Севастопольської міських державних адміністрацій, керівників Адміністрації Президента України, Апарату Верховної Ради України, заступників керівників Адміністрації Президента України, Апарату Верховної Ради України, інші прирівняні до них посади).

У поширенні персональних даних цих категорій осіб не може бути відмовлено, якщо підстави для відмови не передбачено іншим, наприклад, профільним законом — Законом України «Про Президента України», Законом України «Про місцеві державні адміністрації», Законом України «Про Кабінет Міністрів України» тощо.

Крім того, винятком з правила, згідно з яким «не допускається обробка даних про фізичну особу без її згоди» є лише «в інтересах національної безпеки, економічного добробуту та прав людини» [139].

Ми в попередніх розділах вже зауважували про строкатість, неоднозначність, неуніфікованість, легальну невизначеність вищезаз-

начених категорій і внаслідок чого потенційну небезпеку порушення норм цього Закону. Наприклад, у ст. 7 Закону України «Про персональні дані» зазначено: «якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів (Підкреслено нами. — Авт.) суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим». Тобто поряд з категорією «інтереси» вже використовується категорія «життєво важливі інтереси», тим більше, в жодному нормативно-правовому акті неможливо знайти, що саме є життєво важливими інтересами суб'єкта персональних даних, які критерії їх визначення тощо.

Слід також зазначити, що журналісти мають легальні підстави для порушення права суб'єкта на персональні дані, оскільки в ст. 24 Закону України «Про інформацію» закріплено, що «забороняються втручання у професійну діяльність журналістів, контроль за змістом поширюваної інформації, зокрема з метою поширення чи непоширення певної інформації, замовчування суспільно необхідної інформації (Підкреслено нами. — Авт.), накладення заборони на висвітлення окремих тем, показ окремих осіб або поширення інформації про них, заборони критикувати суб'єкти владних повноважень...».

Тобто журналісти, посилаючись на суспільну необхідність, можуть поширювати інформацію про певних осіб, в тому числі персональні дані, наприклад прізвище, ім'я, по-батькові тощо.

Навіть наявність ст. 296 ЦК, згідно з якою «використання імені фізичної особи в літературних та інших творах, крім творів документального характеру, як персонажа (дійової особи) допускається лише за її згодою, а після її смерті — за згодою її дітей, вдови (вдівця), а якщо їх немає, — батьків, братів та сестер», або «ім'я фізичної особи, яка затримана, підозрюється чи обвинувачується у вчиненні злочину, або особи, яка вчинила адміністративне правопорушення, може бути використане (обнародуване) лише в разі набрання законної сили обвинувальним вироком суду щодо неї або винесення постанови у справі про адміністративне правопорушення та в інших випадках, передбачених законом», або «ім'я потерпілого від правопорушення може бути обнародуване лише за його згодою», або «ім'я учасника цивільного спору, який стосується особистого життя сторін, може бути використане іншими особами лише за його згодою» надавало можливості журналістам в силу їх особливого статусу та фактора, що будь-яке правопору-

шення має суспільну значимість не нести відповідальності за порушення права суб'єкта на персональні дані, а навпаки без зайвих перепон та умов вільно поширювати персональну інформацію.

Даний факт підтверджується значною кількістю висвітлених майже в режимі он-лайн з усіма деталями, включаючи фото- і відеоряд, судових справ. Таким чином, «звичайні» правила щодо захисту приватного життя мають багато винятків, коли йдеться про діяльність ЗМІ. Виключення журналістів зі сфери дії Закону України «Про захист персональних даних» не може позитивно впливати на захист персональної інформації, а тому потребує чіткого законодавчого визначення правовий статус і ЗМІ в контексті пошуку балансу захисту права на персональну інформацію, недоторканність приватного життя та права суспільства на інформацію, свободу інформації тощо.

*Саме тому визначення чітких критеріїв віднесення інформації до суспільно необхідної чи суспільно значимої є важливим напрямом наукової діяльності та потребує законодавчого врегулювання.*

Крім того, неврегульованість правового режиму персональних даних, що містяться в базах даних після смерті особи, а також неоднозначне розуміння положень щодо порушення права фізичної особи на конфіденційність її персональних даних та заборону обробки її даних без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини сприяє незадовільному стану захисту персональних даних в Україні, а тому потребує негайного вирішення.

Прийняття Закону України «Про захист персональних даних» було однією із вимог співробітництва ЄС та України у напрямі наближення правової системи нашої держави до європейських стандартів. Заради справедливості слід зауважити, що прийняття цього нормативно-правового акта набуло широкої дискусії серед громадськості, наукових кіл, практичних підрозділів, у медіа-середовищі тощо від повного його схвалення та підтримки до несприйняття та визнання шкідливим і небезпечним для демократії в Україні.

Так, деякі дослідники зауважують, що цей Закон занадто обмежує професійні права журналістів, вимагаючи, наприклад, попереднього узгодження із особою поширення будь-якої інформації, що неї стосується, що, своєю чергою, негативно впливає на об'єктивність поширеної інформації.



Проте сфера його застосування чітко обмежена, зокрема в ст. 1 визначено, що «дія цього Закону не поширюється на діяльність зі створення баз персональних даних та обробки персональних даних у цих базах:

- журналістом — у зв'язку з виконанням ним службових чи професійних обов'язків;
- професійним творчим працівником — для здійснення творчої діяльності» [139].

З іншого боку, враховуючи недосконалість юридичної мови, ряд юридичних осіб можуть «обходити» норми цього закону, зафіксувавши, наприклад, у локальних нормативно-правових актах, що комп'ютери, на яких зберігається інформація, використовуються тільки журналістами під час виконання ними своїх творчих обов'язків.

Відповідно ж до ст. 25 Закону України «Про друковані засоби масової інформації (пресу) в Україні» журналіст редакції друкованого засобу масової інформації визначається як творчий працівник, який професійно збирає, одержує, створює і займається підготовкою інформації для друкованого засобу масової інформації та діє на підставі трудових чи інших договірних відносин з його редакцією або займається такою діяльністю за її уповноваженням [202].

Втім, у Законі України «Про професійних творчих працівників та творчі спілки» від 7 жовтня 1997 року [203] та Законі України «Про культуру» від 14 грудня 2010 року [204] професійний творчий працівник визначається як особа, яка провадить творчу діяльність на професійній основі, результатом якої є створення або інтерпретація творів у сфері культури та мистецтва, публічно представляє такі твори на виставках шляхом публікації, сценічного виконання, кіно-, теле-, відеопоказу тощо та/або є членом творчої спілки, та/або має державні нагороди за діяльність у сфері культури та мистецтва.

Отже, де-факто є два види творчих працівників, а тому не зрозуміло на кого саме розповсюджуються норми Закону України «Про захист персональних даних». Зважаючи на реалії сьогодення, а саме розвиток Інтернет-видань, вважаємо, що зазначений перелік є неповним, оскільки не охоплює журналістів Інтернет-ЗМІ, якщо таке ЗМІ не має статусу інформаційного агентства або журналіст не перебуває в професійному об'єднанні журналістів.

Крім того, практична реалізація закріплених норм в цьому Законі та, як наслідок, притягнення до відповідальності осіб, що їх порушу-



ють, ускладнюються тим, що ряд статей містить бланкетні та відсылні норми, які тривалий час не були прийняті. Наприклад, відповідно до п. 1 ст. 9 Закону України «Про захист персональних даних» «база персональних даних підлягає державній реєстрації шляхом внесення відповідного запису уповноваженим державним органом з питань захисту персональних даних до Державного реєстру баз персональних даних» [139]. Згідно ж з п. 2 цієї статті «Положення ж про Державний реєстр баз персональних даних та порядок його ведення затверджуються Кабінетом Міністрів України». Слід зауважити, що згадане вище Положення було затверджено Постановою Кабінету Міністрів України лише 25 травня 2011 року [205], тобто через півроку після набуття чинності цим актом. А тому медіа-компанії як потенційні «володільці баз даних» мали змогу «обминати» норми цього Закону.

Загалом, право на захист персональних даних згідно зі ст. 12 Загальної декларації прав людини та ст. 8 Європейської конвенції про захист прав людини і основоположних свобод визнається невід'ємною частиною права людини на захист особистого життя.

У міжнародно-правових документах наявне також і юридичне визначення поняття персональних даних. Згідно зі ст. 2 Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» персональні дані означають будь-яку інформацію, яка стосується до конкретно визначеної особи або особи, яка може бути конкретно визначеною [198]. Відповідно до ст. 2 Директиви 95/46/ЄС Європейського парламенту та Ради Європейського Союзу «Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних» від 24 жовтня 1995 року «особисті дані — будь-яка інформація про фізичну особу — ідентифіковану або таку, що може бути ідентифікована» [206].

Водночас кожна країна має власне бачення щодо розуміння сутності та змісту персональних даних. Закони про захист персональних даних в європейських країнах почали приймати у 1970-х роках.

Як зауважують деякі дослідники, історично відомими є два принципи при укладанні національних правових систем захисту персональних даних, які передбачають:

- створення всеохоплюючого закону про захист приватного життя, який спрямований на упорядкування суспільних інформаційних відносин, пов'язаних з визначеними даними. Цей підхід

веде до необхідності корегування положень всього закону при появі нових загроз;

- створення спеціальних законів для кожного типу зазіхань на приватне життя або для кожної сфери, яка є потенційним джерелом загрози та порушень (наприклад, для засобів масової інформації, банків, телекомунікацій та ін.). У даному випадку при виникненні нових загроз такий підхід призводить до безсистемності, дублювання та суперечливості норм права [31, с. 22].

### *Дефініція «персональних даних»*

Вітчизняний законодавець урахував стандарти міжнародної спільноти в цій сфері і надав таку дефініцію **персональним даним** у ст. 2 Закону України «Про захист персональних даних», **як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.**

Наведене визначення не досить чітко розкриває суть складових персональних даних. Як слушно зауважено ще перед другим читанням законопроекту «Про захист персональних даних» у висновку щодо законопроекту Головним юридичним управлінням: «текст законопроекту містить значну кількість оціночних понять і суб'єктивних критеріїв» [207].

### *Відомості, що відносяться до персональних даних*

У п. 2 ст. 11 Закону України «Про інформацію» закріплено, що «не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, а саме: даних про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адресу, дату і місце народження» [39].

Таким чином, до персональних даних відносяться такі відомості, як:

- *національність;*
- *освіта;*
- *сімейний стан;*
- *релігійні переконання;*
- *стан здоров'я;*
- *адреса народження;*

- дата народження;
- місце народження.

Наявність неоднозначного застосування окремих норм Закону України «Про інформацію» та Закону України «Про прокуратуру» судами загальної юрисдикції призвело до порушення конституційних прав і свобод громадянина України у контексті розуміння такої складової персональних даних, як стан здоров'я, її співвідношенням з лікарською таємницею тощо, що сприяло розгляду цього питання Конституційним Судом України.

Як зауважено в Рішенні Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка), «частина друга статті 32 Конституції України не допускає збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Але вітчизняним законодавством не повністю визначено режим збирання, зберігання, використання та поширення інформації, зокрема щодо психічного стану людини, її примусового огляду та лікування, не створено процедури захисту прав особи від протизаконного втручання в її особисте життя психіатричних служб. Закон України «Про інформацію» закріплює лише загальні принципи доступу громадян до інформації, що стосується їх особисто. Механізм реалізації зазначеного права належним чином не визначений. Відсутнє й регулювання використання конфіденційних даних у сфері психіатрії» [208]. «Правовідносини, що виникають у цій сфері, у т.ч. й інформаційного характеру, регулюються відомчими нормативними актами колишнього СРСР...» [208].

Розглянувши згадану справу, Конституційний Суд України вирішив, що до конфіденційної інформації, зокрема належать *свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані)*.

Крім того, до *медичної інформації, тобто свідчення про стан здоров'я людини, належать відомості про історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі наявність ризику для життя і здоров'я.*

Якщо Закон України «Про інформацію» має безальтернативний перелік відомостей, що складають персональні дані, то в Рішенні Конституційного Суду України з цього питання такий перелік є менш одностороннім. Тлумачення ст. 12 Закону України «Про інформацію» має здійснюватись у розширювальний спосіб. Оскільки, використовуючи буквальный спосіб тлумачення цієї статті, можна дійти висновку, що прізвище, ім'я, по-батькові не є персональними даними, хоча саме вони, насамперед, допомагають ідентифікувати особу. Однак зазначимо, що прізвище, ім'я, по-батькові особи чи її дата народження взяті окремо не можуть вважатись персональними даними, оскільки це не надає можливості ідентифікувати особу (адже таке саме прізвище, ім'я, по-батькові може мати багато інших осіб в країні; і дата народження без зазначення прізвища, ім'я, по батькові не персональними даними). Проте в сукупності ці відомості є персональні дані, оскільки за допомогою них може чітко бути встановлено, якій саме особі вони належать.

Хоча Закон України «Про захист персональних даних» не містить чіткого переліку відомостей, які можна віднести до персональних даних, ряд статей цього нормативно-правового акта дещо розширюють коло таких відомостей.

Відповідно до ч. 1 ст. 7 цього Закону забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також даних, що стосуються здоров'я чи статевого життя [139]. Таким чином, крім вищезазначених відомостей, що закріплені в Законі України «Про інформацію» і в Рішенні Конституційного Суду України, до персональних даних слід також віднести:

- *расове або етнічне походження;*
- *політичні, релігійні або світоглядні переконання;*
- *членство в політичних партіях та професійних спілках;*
- *дані, що стосуються здоров'я чи статевого життя.*

Отже, ураховуючи норми Закону України «Про інформацію» та Закону України «Про захист персональних даних», а також Рішення Конституційного Суду України від 30 жовтня 1997 року, **до персональних даних належать такі відомості:**

- 1) *прізвище, ім'я та по-батькові;*
- 2) *національність;*
- 3) *освіта;*

- 4) сімейний стан;
- 5) релігійні переконання;
- 6) стан здоров'я:
  - історія хвороби;
  - мета запропонованих досліджень і лікувальних заходів;
  - прогноз можливого розвитку захворювання, в тому числі наявність ризику для життя і здоров'я;
- 7) адреса народження;
- 8) дата народження;
- 9) місце народження;
- 10) майновий стан;
- 11) расове або етнічне походження;
- 12) політичні, релігійні або світоглядні переконання;
- 13) членство в політичних партіях та професійних спілках;
- 14) дані, що стосуються здоров'я чи статевого життя тощо.

Хоча, ухвалюючи Закон України «Про захист персональних даних», український законодавець використовував міжнародні та європейські стандарти, слід зауважити про значне розходження у розумінні сутності персональних даних.

Так, відповідно до європейських стандартів персональні дані поділяються на дані загального характеру (прізвище, ім'я та по-батькові, дата і місце народження, громадянство, місце проживання) та вразливі персональні дані (дані про стан здоров'я — історія хвороби, діагнози тощо; етнічна належність; ставлення до релігії; ідентифікаційні коди чи номери; персональні символи; підпис; відбитки пальців, записи голосу, фотографії; дані про розмір зарплати або інші законні доходи, про вклади і рахунки в банках, нерухомість, податковий статус; кредитна історія; дані про судимість та інші форми притягнення особи до кримінальної, адміністративної чи дисциплінарної відповідальності; результати іспитів професійного та іншого тестування тощо). За європейськими традиціями забороняється збирання, зберігання, використання та поширення без згоди суб'єкта саме вразливих персональних даних, а не усіх персональних даних взагалі.

## Суб'єкти захисту персональних даних

Персональні дані є інформацією з обмеженим доступом, тому особа, яка здійснює обробку (в тому числі збирання, зберігання, використання, поширення тощо) баз персональних даних має забезпечити захист таких баз від несанкціонованого доступу третіх осіб.

Згідно зі ст. 24 Закону України «Про захист персональних даних» *забезпечення захисту персональних даних у базі персональних даних покладається на володільця цієї бази. В органах державної влади та органах місцевого самоврядування, організаціях, установах і на підприємствах усіх форм власності визначається структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці, відповідно до закону. Фізичні особи — підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист баз персональних даних, якими вони володіють, згідно з вимогами закону [139].*

Тривалий час у вітчизняному законодавстві був відсутній спеціалізований орган контролю за захистом персональних даних. Із прийняттям Закону України «Про захист персональних даних» у ст. 23 було визначено, що «центральною державною виконавчою владою, до повноважень якої належить захист персональних даних, є уповноважений державний орган з питань захисту персональних даних, який:

- 1) забезпечує реалізацію державної політики у сфері захисту персональних даних;
- 2) реєструє бази персональних даних;
- 3) веде Державний реєстр баз персональних даних;
- 4) здійснює в межах своїх повноважень контроль за додержанням вимог законодавства про захист персональних даних із забезпеченням відповідно до закону доступу до інформації, пов'язаної з обробкою персональних даних у базі персональних даних, та до приміщень, де здійснюється їх обробка;
- 5) видає обов'язкові для виконання законні вимоги (приписи) про усунення порушень законодавства про захист персональних даних;
- 6) розглядає пропозиції, запити, звернення, вимоги та скарги фізичних і юридичних осіб;
- 7) організовує та забезпечує взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними;

8) бере участь у роботі міжнародних організацій з питань захисту персональних даних» [139].

Слід зауважити, що таким органом стала **Державна служба України з питань захисту персональних даних (ДСЗПД)**. Указом Президента України «Про Положення про Державну службу України з питань захисту персональних даних» від 6 квітня 2011 року». ДСЗПД України є центральним органом виконавчої влади, діяльність якої спрямовується і координується Кабінетом Міністрів України через міністра юстиції України, але коло завдань дещо відрізняється від тих, які були закріплені в Законі України «Про захисту персональних даних», зокрема в згаданому вище Указі Президента вже зазначається, що **основними завданнями ДСЗПД України є:**

- 1) внесення пропозицій щодо формування державної політики у сфері захисту персональних даних;
- 2) реалізація державної політики у сфері захисту персональних даних;
- 3) контроль за додержанням вимог законодавства про захист персональних даних;
- 4) здійснення міжнародно-правового співробітництва у сфері захисту персональних даних [142].

Таким чином, Закон України «Про захист персональних даних» визначає, що контроль за додержанням вимог законодавства про захист персональних даних здійснює орган виконавчої влади, котрий за своєю суттю не може давати обов'язкові вказівки Президенту, Парламенту, суддям чи правоохоронним органам. Отже, контроль за дотримання закону щодо захисту персональних даних в органах влади практично відсутній.

З іншого боку, поява нового органу контролю, що має право надавати обов'язкові до виконання вказівки усім приватним особам, що працюють з персональними даними, надає додаткові підстави для перевірок правоохоронними органами.

Тим більше, що Законом передбачено, що представники контролюючого органу мають право доступу до всіх приміщень, де здійснюється обробка персональних даних. Більш доречним, на нашу думку, слід законодавчо визначити випадки перевірки уповноваженими органами, зокрема за фактом надходження скарги від особи про неправомірне використання її персональних даних.



За умов відсутності чіткого законодавчого визначення змісту персональних даних порушення кримінальних та адміністративних справ може бути здійснено на основі виявлення набору візитівок, що знаходиться у офісі приватних осіб. Оскільки, як відомо, ніхто не надає письмової згоди на зберігання «таємниці» візитівок, де містяться персональні дані, коли їх дарують чи ними обмінюються.

Будь-яка скарга з приводу неналежного використання персональних даних, наприклад боржників у фінансовому секторі, призведе до перевірки компаній, що працюють з фізичними особами і мають їх списки з телефонами та/або іншими ідентифікаційними даними (адреси, коди та ін), від операторів мобільного зв'язку до банків і страхових компаній.

Таким чином, вважаємо за необхідне чітко законодавчо визначити межі втручання, процедуру проведення перевірок і складання відповідних актів у разі порушення законодавства про захист персональних даних тощо Державною службою України з питань захисту персональних даних.

### ***Процедура оформлення згоди суб'єкта персональних даних на використання його даних***

Законодавець не розкриває також процедуру оформлення згоди суб'єкта персональних даних на використання його даних.

Справді, Законом чітко не визначено, що розуміється під «документальною формою» згоди на використання персональних даних, оскільки згідно з нормами цього Закону документальна форма, в тому числі може бути й письмовою. Тож як співвідносяться між собою такі поняття, як «документальна форма» та «письмова форма»?

Що слід вважати достатньою письмовою формою: чи то хрестик, проставлений власноруч носієм на бланку-анкеті навпроти пропозиції «дані про себе заповнив особисто», чи все ж таки підпис і власноручне заповнення анкети.

Тим більше, як практично перевірити правоохоронним чи контролюючим органам і бути впевненими, що письмова згода підписана особисто суб'єктом персональних даних, коли, як правило, бази даних нараховують значну кількість суб'єктів персональних даних, які інколи можуть вже і не пам'ятати, що вони надавали свої персональні дані.

Хоча з відомостями, які ми надаємо для органів державної влади чи органів самоврядування, немає проблем, оскільки є примітка, що особа надає згоду на певні дії з її персональними даними.

Набагато складніше з ідентифікацією документа в електронній формі, що особливо актуально за умов широкого використання Інтернет-магазинів, коли отримання персональних даних здійснюється у телефонному режимі при замовленні тієї чи іншої продукції.

Відповідно до ст. 6 Закону України «Про електронні документи та електронний документообіг» від 22 травня 2003 року [209] обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу, є електронний підпис.

### **Юридична відповідальність за порушення законодавства у сфері захисту персональних даних**

Тривалий час за порушення законодавства у сфері захисту персональних даних передбачалась винятково кримінальна відповідальність. Причому згідно з чинним кримінальним законодавством *кримінальна відповідальність у цій сфері може бути застосована за незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди.*

Законом України «Про внесення змін до деяких законодавчих актів України щодо порушення законодавства про захист персональних даних» від 11 листопада 2010 року, який набув чинності з 1 січня 2012 року, встановлено відповідальність, зокрема, в частині незаконного збирання, зберігання, використання або поширення конфіденційної інформації про особу; незаконного збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, знищення або поширення чи їх передачі конфіденційної інформації про особу третім особам з порушенням вимог закону; ухилення від реєстрації бази персональних даних, створення або робота з базами персональних даних до проведення державної реєстрації таких баз даних; порушення порядку доступу до персональних даних, які обробляються у базах персональних даних, що призвело до розголошення цих даних або їх втрати та інше.

За ухвалення цього законопроекту проголосувало 257 за мінімально необхідної кількості в 226 голосів народних депутатів. Зокрема, було до-

повнено КУпАП статтями 188–39 і 188–40 такого змісту: «Порушення законодавства у сфері захисту персональних даних» та «Невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних».

*Серед основних правопорушень у сфері захисту персональних даних, за які передбачено адміністративна відповідальність, було закріплено такі:*

- 1) неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку із включенням його персональних даних до бази персональних даних, мету збору цих даних та осіб, яким ці дані передаються;
- 2) неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних;
- 3) ухилення від державної реєстрації бази персональних даних;
- 4) недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них;
- 5) невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних щодо усунення порушень законодавства про захист персональних даних.

Слід зауважити, що за вчинення згаданих вище правопорушень передбачається накладання доволі серйозних штрафних санкцій: на громадян від ста до п'ятисот неоподатковуваних мінімумів доходів громадян; на посадових осіб, громадян — суб'єктів підприємницької діяльності — від двохсот до тисячі неоподатковуваних мінімумів доходів громадян.

Повторне ж протягом року вчинення порушення тягне за собою накладення штрафу на громадян від трьохсот до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян — суб'єктів підприємницької діяльності — від чотирьохсот до семисот неоподатковуваних мінімумів доходів громадян.

За недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них, — тягне за со-

бою накладення штрафу від трьохсот до тисячі неоподатковуваних мінімумів доходів громадян.

Вищезазначений закон передбачає кримінальну та адміністративну відповідальність за порушення законодавства у сфері захисту персональних даних, зокрема, вносяться зміни до Кримінального кодексу України, Кодексу України про адміністративні правопорушення, Кримінально-процесуального кодексу України та Закону України «Про інформацію». Таким чином, спостерігається тенденція до посилення відповідальності за порушення законодавства у сфері захисту персональних даних.

Водночас доповнення до КУпАП у цьому контексті викликають декілька запитань. Зокрема, як співвідносяться між собою п. 2. ст. 188–39, де йдеться про такий склад правопорушення, як «неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних» та ст. 188–40, що передбачає відповідальність за невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних, оскільки, на нашу думку, неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних, є одним із способів невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних.

Серед основних *недоліків адміністративно-правового регулювання захисту персональних даних* було виділено такі: колізійність норм нормативно-правових актів, що регулюють суспільні відносини у сфері захисту персональних даних і наявність численних прогалин; неоднозначність, неузгодженість та суперечливість закріплених дефініцій та подекуди відсутність навіть базових із них; наявність значного масиву декларативних положень за відсутності механізму їх правореалізації; наявність численних бланкетних норм права, що ускладнює їх правореалізацію; наявність абстрактних, суб'єктивних понять, що потребують офіційного тлумачення або чіткого визначення тощо.

Серед основних *шляхів удосконалення адміністративно-правового регулювання захисту персональних даних* було запропоновано такі:

- визначити поняття «суспільної необхідності» як передумови поширення персональних даних без згоди суб'єкта персональних даних;
- урегулювати правовий режим персональних даних, що містяться в базах даних після смерті особи, а випадки порушення права фізичної особи на конфіденційність її персональних даних та заборону обробки її даних без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини сприяє незадовільному стану захисту персональних даних в Україні, а тому потребує негайного вирішення;
- розширити коло осіб, на яких дія Закону не поширюється, а саме на журналістів Інтернет-ЗМІ, якщо таке ЗМІ не має статусу інформаційного агентства або журналіст не перебуває в професійному об'єднанні журналістів;
- законодавчо визначити випадки перевірки уповноваженими органами захисту персональних даних, зокрема за фактом надходження скарги від особи про неправомірне використання його персональних даних, а також межі втручання, процедуру проведення перевірок і складання відповідних актів у разі порушення законодавства про захист персональних даних тощо Державною службою України з питань захисту персональних даних.

Таким чином, прийняття Закону України «Про захист персональних даних» відіграє надзвичайно важливу роль у забезпеченні захисту персональних даних. Хоча наявність таких недоліків, як колізійність норм між окремими статтями в самому Законі та зі статтями інших нормативно-правових актів, а також значної кількості прогалин не може сприяти значному покращенню захисту персональних даних.

### 4.3 АДМІНІСТРАТИВНО-ПРАВОВИЙ РЕЖИМ СЛУЖБОВОЇ ІНФОРМАЦІЇ

#### *Історія становлення інституту службової інформації*

Тривалий час нормативно-правового регулювання суспільних відносин, пов'язаних зі службовою таємницею в Україні взагалі не було.

Як за радянських часів, так і тривалий час в незалежній Україні термін «службова інформація» на нормативному рівні не застосовувався. Якщо за радянських часів використовувався термін «службова таємниця», то в чинному українському законодавстві законодавець попервах оперував терміном «конфіденційна інформація, що є власністю держави».

Вперше, до речі, його було використано в Концепції (Основах державної політики) національної безпеки України, затвердженої Постановою Верховної Ради України від 16 січня 1997 року. Зокрема закріплювалося, що витік такої інформації одна із загроз національній безпеці в інформаційній сфері. Щодо визначення цього терміна, то його в указаному акті не було.

У подальшому цей термін був застосований в Кримінальному кодексі України, ухваленому 5 квітня 2001 року. Так, у ст. 330 КК України встановлювалася кримінальна відповідальність за передачу іноземній стороні конфіденційної інформації, що є власністю держави, особою, якій ці відомості були довірені у зв'язку з виконанням службових обов'язків. Слід зауважити, що ця норма була майже ідентична нормі, що містила попередня редакція Кримінального кодексу України від 1960 року, де замість терміна «конфіденційна інформація, що є власністю держави», був закріплений термін «службова таємниця».

Наступною віхою становлення цього виду інформації з обмеженим доступом став 2004 рік, коли до Закону України «Про інформацію» було внесено зміни та доповнення, а саме:

- визначено, що інформація, яка є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ — надано статус конфіденційної;



- порядок обліку, зберігання і використання документів та інших носіїв, що містять зазначену інформацію, визначається Кабінетом Міністрів України;
- визначено категорії інформації, які не можуть бути віднесені до конфіденційної;
- встановлено відповідальність за «порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави».

До того ж доповнення були внесені і до Кодексу України про адміністративні правопорушення, а саме включено ст. 212–5 «Порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави», яка передбачала адміністративну відповідальність за «порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, яке призвело до розголошення такої інформації».

Перша редакція Закону України «Про інформацію» класифікувала інформацію за режимом доступу на відкриту інформацію та інформацію з обмеженим доступом, остання з яких за правовим режимом поділялась на конфіденційну та таємну.

Конфіденційна інформація як відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. До таємної інформації законодавець відніс інформацію, що містить відомості, які становлять державну та іншу, передбачену законом, таємницю, розголошення якої завдає шкоди особі, суспільству і державі (Підкреслено нами. — Авт.)

Спробу класифікації конфіденційної інформації було зроблено в Російській Федерації Указом Президента від 6 березня 1997 року, яким затверджено перелік відомостей конфіденційного характеру, в якому зазначались такі види інформації: персональні дані, таємниця слідства і судочинства, службова таємниця, професійна таємниця, комерційна таємниця, відомості про сутність винаходу корисної моделі або промислового зразка до офіційної публікації інформації про них<sup>78</sup>.

<sup>78</sup> Об утверждении сведений конфиденциального характера [Электронный ресурс] : указ Президента Российской Федерации от 6 марта 1997 г. в ред. от 23 сент. 2005 г. № 111. — Режим доступа : <http://www.internet-law.ru/law/inflaw/ukaz-97.htm>.



Хоча здебільшого в юридичній літературі висловлюється думка про те, що перелік відомостей, які мають обмежений доступ, настільки великий, що надати єдине визначення неможливо.

Вітчизняні юристи висловлюють різні підходи щодо класифікації конфіденційної інформації. Одні до неї відносять таємницю приватного життя, професійну таємницю, службову таємницю, таємницю слідства і судочинства, комерційну таємницю<sup>79</sup>. Інші — інформацію, що є власністю держави, (службова інформація) та персональні дані<sup>80</sup>.

Цікаво, що в законодавстві України до таємної інформації відносять такі види таємної інформації: банківська, військова, комерційна, лікарська, професійна, нотаріальних дій, адвокатська, службова, усиновлення, страхування, листування, телефонних розмов, телеграфної та іншої кореспонденції. Одночасно з цим деякі з перерахованих видів інформації зараховуються і до конфіденційної інформації. Щодо службової інформації (таємниці), то вона взагалі займає окреме місце в системі інформації з обмеженим доступом.

Зважаючи на те, що законодавець не чітко закріпив розуміння інституту таємниць, їх видів ряд державних органів і недержавних інституцій зловживали цією прогалиною. До того ж сам закон містить відомі норми та не визначає поняття, як «таємниця»<sup>81</sup>.

Щодо «іншої інформації, яка захищається державою», то вона також не була конкретизована в законодавстві, а також не були визначені критерії віднесення відомостей до такої інформації, її класифікація та правовий режим.

Тому державні органи надавали різним нормативним актам (указам і розпорядженням Президента України, постановам, інструкціям, наказам органів виконавчої влади тощо) грифи як-от: «опублікуванню не підлягає» та «не для друку».

Хоча на яких підставах це робилось — не зрозуміло. І чому саме такі грифи таємності надавалися теж.

<sup>79</sup> Кормич Б. А. Інформаційна безпека : організаційно-правові основи : [навч. посіб.] / Б. А. Кормич. — К. : Кондор, 2004. — 384 с.

<sup>80</sup> Марущак А. І. Правові основи захисту інформації з обмеженим доступом : [курс лекцій] / А. І. Марущак. — К. : КНТ, 2007. — 208 с.

<sup>81</sup> Шлома Г. О. Право на інформацію з обмеженим доступом / Г. О. Шлома // Науковий вісник Юрид. акад. МВС. — Дніпропетровськ, 2005. — № 2. — С. 310–315, с. 313.

Цікаво, що ще у 2006 році співголова Харківської правозахисної групи зазначав, що Президент України Л. Д. Кучма видав близько 900 актів під такими грифами: Прем'єр-міністр В. Ф. Янукович — близько 100, Президент В. А. Ющенко — 44, Прем'єр-міністр Ю. В. Тимошенко — 15 (також 2 розпорядження з грифом ДСК), Прем'єр-міністр Ю. І. Єхануров — жодного (одна постанова з грифом ДСК)<sup>82</sup>.

До того ж, ознайомившись із переліком цих документів, зазначений юрист зауважив, що до більшості з них було необґрунтовано обмежено доступ грифами, не передбаченими чинним законодавством. Тому він як представник Харківської правозахисної групи вимагав: зняти всі незаконні обмежувальні грифи з усіх нормативних актів, виданих усіма державними органами України. Ті з них, що насправді містять державні секрети, повинні бути віднесені до державної таємниці відповідно до Закону України «Про державну таємницю» або до відомостей з грифом «Для службового користування», а інші — без винятку і в повному обсязі повинні бути відкриті для суспільства<sup>83</sup>.

Таким чином, законними можна визнати тільки такі грифи обмеження доступу, як: «особливої таємності», «цілком таємно», «таємно», які відповідають встановленому ступеню секретності згідно із Законом України «Про державну таємницю» та «для службового користування», який передбачений відповідною Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, що затверджена Постановою КМУ від 27 листопада 1998 року.

Лише зауважимо, що нині у зв'язку з ухваленням Закону України «Про доступ до публічної інформації», цей нормативно-правовий акт має ряд змін та доповнень, зокрема у тексті Постанови слова «конфіденційна інформація, що є власністю держави», у всіх відмінках замінено словами «службова інформація».

<sup>82</sup> Секретні матеріали: що ховала влада під грифами «не для друку» та «опублікуванню не підлягає» [Електронний ресурс] / Інформаційний портал Харківської правозахисної групи. — Режим доступу до журн. : <http://www.maidan.org.ua>.

<sup>83</sup> Секретні матеріали: що ховала влада під грифами «не для друку» та «опублікуванню не підлягає» [Електронний ресурс] / Інформаційний портал Харківської правозахисної групи. — Режим доступу до журн. : <http://www.maidan.org.ua>.

Проте наразі, як зазначає Г. О. Шлома, органи влади фактично безпідставно відмовляють у наданні інформації, відносячи її до інформації з обмеженим доступом; неправомірно застосовуючи грифи обмеження доступу до інформації «опублікуванню не підлягає», «не для друку», «для службового користування», причому масштаби застосування цих обмежувальних грифів досить великі та застосовуються переважно Президентом України і Кабінетом Міністрів України<sup>84</sup>.

Слід зауважити, що інститут службової таємниці безпосередньо пов'язаний з інститутом державної таємниці. У ст. 10 Закону України «Про державну таємницю» передбачено можливість органів державної влади на підставі та в межах закону та з метою конкретизації та систематизації даних про інформацію, що віднесена до державної таємниці, створювати *розгорнуті переліки відомостей, що становлять державну таємницю*.

Цікаво, що оприлюднення розгорнутих переліків не передбачено. Хоча закріплено право зацікавлених осіб оскаржити Президенту України чи Верховній Раді України внесення до розгорнутих переліків такої інформації, яка за змістом не може визнаватись державною таємницею. Як це можна зробити, не знаючи об'єкта оскарження, перепрошуємо за каламбур — таємниця.

### ***Сучасний стан нормативно-правового регулювання суспільних відносин у сфері службової інформації***

Нормативно-правове закріплення службової інформації знайшло свій вираз у нормах Закону України «Про доступ до публічної інформації», згідно з якими **до службової інформації може належати така інформація:**

- 1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробленням напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

<sup>84</sup> Шлома Г. О. Місце інституту службової таємниці в діяльності державних органів України / Г. О. Шлома // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична : [зб. наук. праць / гол. ред. В. Л. Ординський]. — Львів, 2006. — Вип. 3. — С. 157–168.

- 2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Оскільки згадана вище інформація є інформацією з обмеженим доступом, то доступ до неї здійснюється згідно із Законом України «Про доступ до публічної інформації» при дотриманні таких вимог:

- 1) винятково в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;
- 2) розголошення інформації може завдати істотної шкоди цим інтересам;
- 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

### ***Перелік відомостей, що становить службову інформацію***

Органи державної влади, органи місцевого самоврядування, інші суб'єкти владних повноважень зобов'язані створювати переліки відомостей, що становлять службову інформацію.

Слід виділити такі *основні засади створення цих переліків*:

1. Рішення про надання (зняття) грифа «для службового користування» (далі — ДСК) інформації приймаються безпосередніми виконавцями документів згідно з даним Переліком та за висновками експертних комісій.
2. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф ДСК.
3. Відомості з грифом ДСК є власністю держави і такими, що містять відомості обмеженого поширення.
4. Відповідальність за правильне присвоєння грифу ДСК виробам та інформації несуть посадові особи, які надали гриф, підписали або затвердили ці документи.
5. У разі скасування рішення віднесення інформації до службової, про зняття грифа обмеження доступу повідомляються всі організації, яким надсилався цей документ.

6. Копіювання сторонніми організаціями документів з грифом ДСК повинно здійснюватись за погодженням з організацією — автором цих документів.
7. Використання інформаційної, телекомунікаційної або інформаційно — телекомунікаційної системи для друкування документів з грифом ДСК здійснювати тільки після створення в ній комплексної системи захисту інформації та отримання відповідного атестату.
8. Передача інформації ДСК з однієї системи до іншої здійснюється захищеними каналами зв'язку або у зашифрованому вигляді. Використання Інтернету або незахищених каналів для передачі інформації ДСК заборонено.
9. За розголошення відомостей ДСК винні особи притягаються до адміністративної відповідальності згідно з чинним законодавством.

Серед знакових вітчизняних нормативно-правових актів є також *Постанова Кабінету Міністрів України «Про внесення змін до Постанови Кабінету Міністрів України від 27 листопада 1998 року N 1893» від 17 листопада 2004 року.*

Згідно з цією Постановою було визначено *перелік орієнтовних критеріїв віднесення до службової інформації:*

- 1) повинні створюватися за кошти державного бюджету або перебувати у володінні, користуванні чи розпорядженні організації;
- 2) використовуватися з метою забезпечення національних інтересів держави;
- 3) не належати до державної таємниці;
- 4) унаслідок розголошення такої інформації можливе:
  - 4.1) порушення конституційних прав і свобод людини та громадянина;
  - 4.2) настання негативних наслідків у внутрішньополітичній, зовнішньополітичній, економічній, військовій, соціальній, гуманітарній, науково-технологічній, екологічній, інформаційній сферах та у сферах державної безпеки і безпеки державного кордону;
  - 4.3) створення перешкод у роботі державних органів<sup>85</sup>.

<sup>85</sup> Про внесення змін до постанови Кабінету Міністрів України від 27 лист. 1998 р. № 1893 : постанов. Кабінету Міністрів України від 17 лист. 2004 р. //Офіційний вісник України. — 2004. — № 46. — Ст. 3033.

Аналіз зазначених критеріїв дозволяє констатувати, що вони мають занадто узагальнений характер. А тому не є достатніми для розмежування конфіденційної і таємної інформації та потребують деталізації.

Тому актуальними є Рекомендації віднесення публічної інформації до службової згідно із Законом «Про доступ до публічної інформації», підготовлені Представником Уповноваженого Верховної Ради України з прав людини з питань доступу до публічної інформації та захисту персональних даних<sup>86</sup>:

- 1) до службової інформації відповідно до статті 9 Закону України «Про доступ до публічної інформації» можуть бути віднесені лише такі категорії публічної інформації:
  - внутрівідомча службова кореспонденція, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;
  - інформація, що зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.
- 2) інша інформація, у тому числі конфіденційна інформація про особу, не може відноситися до службової, якщо тільки вона не відповідає зазначеним вище категоріям;
- 3) якщо публічна інформація підпадає під одну із названих у п. 1 категорій, ця інформація може бути віднесена до службової при дотриманні сукупності таких вимог («трискладовий тест» відповідно до частини другої статті 6 Закону «Про доступ до публічної інформації»): 1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; 2) розголошення інформації може завдати істотної шкоди цим ін-

<sup>86</sup> Уповноважений Верховної Ради з прав людини [Електронний ресурс]. — Режим доступу : <http://www.ombudsman.gov.ua>.



- тересам; 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.
- 4) публічна інформація не може мати статусу службової, якщо завершився процес прийняття рішення з відповідного питання (що підтверджується правовим актом чи фактичними діями) або проект рішення винесено на обговорення;
  - 5) публічна інформація, що міститься у правовому акті відповідного суб'єкта владних повноважень, у тому числі акті індивідуальної дії (указ, наказ, рішення, розпорядження тощо), може бути віднесена до службової, лише якщо вона була зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни та пройшла «трискладовий тест»;
  - 6) не можуть бути обмежені в доступі, у тому числі шляхом віднесення до службової, зокрема, така інформація: яка була правомірно оприлюднена раніше розпорядником; про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно; відомості, зазначені у декларації про майно, доходи, витрати і зобов'язання фінансового характеру, оформленої за формою і в порядку, що встановлені Законом «Про засади запобігання і протидії корупції»;
  - 7) у кожному конкретному випадку при вирішенні питання щодо віднесення публічної інформації до службової, а також у кожному наступному випадку запитання інформації, яка була віднесена до службової, розпорядник обов'язково повинен обґрунтувати таке: 1) якому саме з інтересів загрожує розголошення інформації (наприклад, національній безпеці, територіальній цілісності); 2) у чому саме буде полягати шкода в разі розголошення цієї інформації; 3) яким чином істотна шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.
  - 8) після визначення того, що документ містить службову інформацію, на ньому проставляється гриф «Для службового користування», при цьому повинно бути визначено, яка саме інформація в документі є службовою — вся чи лише її частина. Якщо



лише частина інформації, що міститься в цьому документі, є службовою, то при запитуванні такого документа — незважаючи на гриф «ДСК», що стоїть на документі, — він надається в тій частині, яка не є обмеженою в доступі;

- 9) **той факт, що документ має гриф «ДСК» є недостатнім для відмови в доступі до нього.** У доступі до службової інформації може бути відмовлено лише в разі проходження «трискладового тесту» з урахуванням конкретної ситуації та обставин справи. Письмова відмова в задоволенні запиту з посиланням на віднесення інформації до службової повинна містити обґрунтування відповідно до застосованого «трискладового тесту» — у разі відсутності такого обґрунтування таку відмову слід вважати неправомірною;
- 10) перелік відомостей, що можуть становити службову інформацію, може складатися лише щодо інформації, згаданої в п. 2 ч. 1 ст. 9 Закону («зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці»). Натомість, не може бути складений вичерпний перелік інформації, про яку йдеться у п. 1 ч. 1 цієї статті («інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень»). Це пов'язано із неможливістю визначити коло усіх питань, які можуть бути підняті у службовій кореспонденції.

«Згідно з положеннями Конституції України доступ до інформації так само, як і будь-які обмеження права на інформацію, мають регламентуватися виключно законами. В них, на нашу думку, повинні бути встановлені принципи доступу до інформації, коло осіб, що мають право допуску, форми допуску, процедури оскарження і захисту порушеного права на інформацію, відповідальність осіб, винних у порушенні цього права»<sup>87</sup>.

<sup>87</sup> Шлома Г. О. Адміністративно-правове забезпечення службової таємниці в органах внутрішніх справ України : дис. ... канд. юрид. наук : 12.00.07 / Ганна Олександрівна Шлома. — Дніпропетровськ, 2008. — 286 с., с. 28.

Нині більшість державних інституцій має такі переліки, які ще було розроблено у зв'язку з виконанням доручення Служби безпеки України «Щодо відомчих переліків конфіденційної інформації» від 23 лютого 2008 року та необхідністю уточнення Переліку конфіденційної інформації, що є власністю держави у межах повноважень конкретної інституції.

Аналіз нормативно-правової бази, що закріплює діяльність основних міністерств України, надав можливість дійти висновку, що нині кожне з них має відповідний правовий фундамент, що дозволяє громадянам України мати доступ до інформації. Водночас до інформації, що є інформацією з обмеженим доступом, а саме службовою інформацією доступ обмежено на основі Переліків відомостей, що становлять службову інформацію, чи Переліку конфіденційної інформації, що є власністю держави:

- 1) *Міністерство аграрної політики та продовольства України* — Наказ Міністерства аграрної політики та продовольства України від 12 вересня 2012 року «Про затвердження Переліку відомостей, що становлять службову інформацію в Міністерстві аграрної політики та продовольства України»<sup>88</sup>;
- 2) *Міністерство освіти і науки України* — Наказ Міністерства освіти і науки України «Про затвердження Переліку конфіденційної інформації, що є власністю держави у галузі освіти і науки України, затверджено Наказом Міністра освіти і науки України від 28 березня 2008 року;
- 3) *Міністерство внутрішніх справ України* — Наказ МВС України «Про Перелік відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України» від 14 травня 2012 року;
- 4) *Міністерство екології та природних ресурсів* — Наказ Міністерства екології та природних ресурсів «Про затвердження переліку службової інформації, якій надається гриф «Для службового користування» від 28 листопада 2012 року;

<sup>88</sup> Про затвердження Переліку відомостей, що становлять службову інформацію в Міністерстві аграрної політики та продовольства України [Електронний ресурс] : наказ Міністерства аграрної політики та продовольства України від 12 верес. 2012 р. № 564. — Режим доступу : <http://minagro.gov.ua/dostup-do-publichnoi-informacii?nid=1512>.

- 5) *Міністерство економічного розвитку і торгівлі України* — Наказ Міністерства економічного розвитку і торгівлі України «Перелік відомостей, що становлять службову інформацію в Міністерстві економічного розвитку і торгівлі України» від 13 липня 2012 року;
- 6) *Міністерство енергетики та вугільної промисловості України* — Наказ Міністерства енергетики та вугільної промисловості України «Про затвердження Переліку відомостей, що становлять службову інформацію і якій присвоюється гриф обмеження доступу «Для службового користування» у Міненерговугілля України» від 19 жовтня 2011 року;
- 7) *Міністерство закордонних справ України* — Наказ Міністерства закордонних справ України «Про затвердження Переліку службової інформації, що є власністю держави» від 29 червня 2011 року;
- 8) *Міністерство культури України* — накази Міністерства культури України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів та інших матеріальних носіїв, які містять відомості, що становлять службову інформацію» від 9 червня 2011 року та «Про затвердження Переліку відомостей, що становлять службову інформацію» від 9 червня 2011 р.;
- 9) *Міністерство оборони України* — Наказ Міністерства оборони України «Про затвердження Переліку відомостей Міністерства оборони України, які містять службову інформацію (ПСІ — 2012)» від 26 червня 2012 р.;
- 10) *Міністерство охорони здоров'я України* — накази Міністерства охорони здоров'я України «Перелік відомостей, що містять службову інформацію в МОЗ України» від 16 серпня 2011 року та «Перелік відомостей, що містять конфіденційну інформацію в МОЗ України» від 16 серпня 2011 р.;
- 11) *Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України* — Наказ Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України «Перелік відомостей, що становлять службову інформацію у Міністерстві регіонального розвитку, будівництва та житлово-комунального господарства України» від 11 травня 2012 року;

- 12) *Міністерство фінансів України* — Наказ Міністерства фінансів України «Перелік відомостей Міністерства фінансів України, що становлять службову інформацію» від 15 серпня 2011 року;
- 13) *Міністерство юстиції України* — накази Міністерства юстиції України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів та інших матеріальних носіїв, які містять відомості, що становлять службову інформацію у Міністерстві юстиції України» від 8 червня 2011 року та «Про затвердження Переліку відомостей, що становлять службову інформацію у Міністерстві юстиції України» від 8 червня 2011 року;
- 14) *Міністерство соціальної політики України* — Наказ Міністерства соціальної політики України «Про затвердження Переліку службової інформації Міністерства соціальної політики України, якій надається гриф обмеження доступу «Для службового користування»» від 26 грудня 2011 року.

Зауважимо, що ряд інших міністерств не мають переліків службової інформації. Це, насамперед, пов'язано з тим, що вони були утворені недавно, а саме: Міністерство молоді та спорту України, Міністерство інфраструктури України, Міністерство промислової політики України, Міністерство доходів і зборів України.

Так, Указом Президента України від 24 грудня 2012 року утворено Міністерство доходів і зборів України шляхом реорганізації Державної митної служби України та Державної податкової служби України. Нині ця установа не має такого Переліку, хоча кожна попередня з них мала, наприклад, Державна митна служба України затвердила «Перелік відомостей, які містять конфіденційну інформацію митних органів, спеціалізованих митних установ і організацій, що є власністю держави, і документів та інших матеріальних носіїв такої інформації, яким надається гриф обмеження доступу «Для службового користування»» Наказом Держмитслужби від 22 квітня 2009 року.

Отже, незважаючи на ухвалення Закону України «Про доступ до публічної інформації», де визначено поняття «службова інформація», у відомчому законодавстві спостерігається термінологічна плутанина, неуніфікованість понять. Поряд з поняттям «службова інформація» застосовується поняття «конфіденційна інформація, що є власністю держави», «службова інформація, що є власністю держави» тощо.

Майже в кожному такому Переліку є розділ, присвячений безпосередньо охороні інформації з обмеженим доступом. Так, у Наказі МВС України «Про Перелік відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України» від 14 травня 2012 року закріплено, що у сфері охорони інформації з обмеженим доступом службовою є інформація, що розкриває:

- 1) організацію та фактичний стан забезпечення охорони державної таємниці, за винятком відомостей, які віднесені до державної таємниці;
- 2) систему охорони, перепускний, внутрішньо об'єктовий режим, технічне обладнання режимних об'єктів, зон, приміщень, де здійснюються роботи, пов'язані з державною таємницею, за умови мирного часу якщо при цьому не розкриваються відомості, які віднесені до державної таємниці;
- 3) зміст інформації, яка вноситься до форм облікової документації матеріальних носіїв інформації з обмеженим доступом, актів їх звірки наявності, знищення, у тому числі з питань мобілізаційної підготовки, територіальної оборони та цивільного захисту на особливий період, які не містять відомостей, що становлять державну таємницю;
- 4) зміст, організацію, результати службових розслідувань за фактами: розголошення державної таємниці, втрат матеріальних носіїв секретної інформації, інших порушень режиму секретності, норм і вимог технічного захисту інформації першої та другої категорій за винятком відомостей, які віднесені до державної таємниці;
- 5) зміст номенклатури посад працівників органу (підрозділу) внутрішніх справ, зайняття яких потребує оформлення допуску до державної таємниці;
- 6) порядок доступу працівників органів внутрішніх справ до окремих службових приміщень, де виконуються роботи, пов'язані з державною таємницею;
- 7) засоби та заходи захисту інформації на режимній території, в інформаційно-телекомунікаційних та комп'ютерних мережах, у режимних приміщеннях органів і підрозділів внутрішніх справ, військових частинах, за винятком відомостей, які віднесені до державної таємниці;

- 8) заходи щодо захисту інформації з обмеженим доступом під час прийому іноземних делегацій, груп та окремих іноземців, за винятком відомостей, які віднесені до державної таємниці;
- 9) дані про особу, якій надано допуск до державної таємниці (прізвище, ім'я, по батькові, дата та місце народження, місце проживання, посада, найменування органу, підрозділу, номер і дата наказу про надання доступу за винятком відомостей, які віднесені до державної таємниці;
- 10) переліки режимних, атестованих приміщень структурних підрозділів апарату МВС України, ГУМВС, УМВС, міськрайлінорганів, вищих навчальних закладів, військових частинах, науково-дослідних установ та підприємств;
- 11) заходи безпеки інформації на об'єктах, де циркулює конфіденційна інформація, за винятком відомостей, які віднесені до державної таємниці;
- 12) перелік технічних засобів, що використовуються для проведення вимірювань захищеності об'єктів інформаційної діяльності від витоку інформації технічними каналами;
- 13) відомості, що зберігаються на ідентифікаторах комплексів засобів захисту інформації від несанкціонованого доступу, за винятком відомостей, які віднесені до державної таємниці;
- 14) акти перевірок про результати комплексних спеціальних перевірок, за винятком відомостей, що становлять державну таємницю;
- 15) відомості про планування, впровадження заходів, фактичний стан, наявність недоліків в організації технічного захисту інформації в органах, підрозділах внутрішніх справ, за винятком відомостей, що становлять державну таємницю;
- 16) відомості про результати експертних випробувань комплексних систем захисту інформації в автоматизованих системах на відповідність вимогам нормативно-правових актів з питань технічного захисту інформації.



## Поняття «службова інформація» у доктринальних джерелах

У юридичній енциклопедії за редакцією Ю.С. Шемшушенка **службова таємниця** визначається як узагальнена назва відомостей, розголошення яких забороняється чинним законодавством або зумовлюється службовою необхідністю, які стали відомими і якими користуються у процесі та при виконанні своїх службових обов'язків службові особи. Службова таємниця є конфіденційною інформацією, різновидом професійної таємниці, що містить відомості з обмеженим доступом про діяльність державних органів, органів місцевого самоврядування, підприємств, установ, організацій незалежно від форми власності й про особу<sup>89</sup>.

На думку В. О. Мазурова, **службова таємниця** — це охоронювані законом конфіденційні відомості про діяльність державних органів, доступ до яких обмежений законом у силу службової необхідності, а також які стали відомими державним органам і органам місцевого самоврядування тільки на законній підставі й у силу виконання їхніми представниками службових обов'язків, що мають дійсну чи потенційну цінність у силу невідомості їх третім особам, до них немає вільного доступу на законній підставі, власник відомостей вживає заходів до їхньої конфіденційності, незаконне одержання чи розголошення яких створює загрозу заподіяння шкоди власнику цих відомостей і надає йому право на захист відповідно до законодавства<sup>90</sup>. Такої самої позиції дотримується Г. А. Шлома<sup>91</sup>.

М. С. Демкова та М. В. Фігеля вважають, що **службовою таємницею** є: 1) положення плану контрольно-ревізійної роботи на термін до часу повідомлення об'єкта контролю про початок проведення ревізії (перевірки); 2) факти виявлених під час проведення ревізій і перевірок порушень, зловживань до їх повного документального підтверджен-

<sup>89</sup> Юридична енциклопедія : в 6 т. / [редкол. : Ю.С. Шемшушенко (гол. редкол.) та ін.]. — К. : Укр. енциклопедія, 1998. — Т. 5 : П-С. — 733 с. ; Юридичний словник-довідник / за ред. Ю. С. Шемшученка. — К. : Феміна, 1996. — 696 с.

<sup>90</sup> Мазуров В. А. Тайна : государственная, коммерческая, банковская, частной жизни. Уголовно-правовая защита : [учеб. пособие] / В. А. Мазуров ; под науч. рук. д-ра юрид. наук, проф. С. В. Землюкова. — М. : Дашков и К, 2003. — 156 с., С. 23.

<sup>91</sup> Шлома Г. О. Адміністративно-правове забезпечення службової таємниці в органах внутрішніх справ України : дис. ... канд. юрид. наук : 12.00.07 / Ганна Олександрівна Шлома. — Дніпропетровськ, 2008. — 286 с., С. 34.



ня й закріплення в актах, а також заплановані з цією метою зустрічні перевірки, раптові інвентаризації готівки й майна, контрольні обміри та інші ревізійні дії; 3) надані правоохоронними органами оперативні та інші відомості щодо діяльності підприємств, установ і організацій (вчинених порушень, зловживань посадових осіб, дані посадовими особами письмові пояснення, протоколи допиту з конкретних питань тощо); 4) інформація про оперативну й слідчу роботу органів прокуратури, МВС, СБУ, їх органів дізнання в тих випадках, коли її розголошення може зашкодити слідству, порушити право людини на справедливий та об'єктивний розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи; 5) конкретні пояснення посадових осіб щодо виявлених фактів зловживань, крадіжок тощо; 6) відомості, які містяться у зверненнях громадян щодо їхнього (чи інших громадян) особистого життя, та інша інформація, що зачіпає (порушує) їхні права та законні інтереси; 7) документи, що становлять внутрішньовідомчу службу кореспонденцію (доповідні записки, листування між підрозділами, матеріали колегій тощо), якщо вони пов'язані з процесом прийняття рішень і передують їх прийняттю; 8) інформація банківських і фінансових установ, підготовлена на запити органів державної контрольно-ревізійної служби; 9) чернетки матеріалів ревізій і перевірок<sup>92</sup>.

Запропоноване М. С. Демковою та М. В. Фігель визначення службової таємниці охоплює особливості діяльності лише окремих правоохоронних органів, без врахування наявності службової таємниці в інших державних органах та органах місцевого самоврядування у зв'язку з виконанням покладених на них функцій держави.

На думку О. В. Ботвінкіна та В. П. Ворожка, службова таємниця — це склад і обсяг відомостей, що є в розпорядженні конкретних державних органів, служб або їх посадових осіб стосовно підконтрольних об'єктів, контролюючих, правоохоронних та інших державних органів, їх працівників, способів досягнення визначених законодавством завдань і які з цієї причини на певний період не підлягають зовнішньому чи внутрішньому розголошенню<sup>93</sup>.

<sup>92</sup> Демкова М. С. Доступ до інформації та електронне урядування / М. С. Демкова, М. В. Фігель. — К. : Факт, 2004. — 336 с., С. 73.

<sup>93</sup> Ботвінкін О. В. Інформація з обмеженим доступом, що не є державною таємницею, в законодавстві України : аналіт. огляд / О. В. Ботвінкін, В. П. Ворожок. — К. : НА СБ України, 2006. — 96 с., С. 38.

Дане визначення відповідає дефініції службової інформації, що міститься в окремих нормативно-правових актах.

До того ж, названі дослідники на основі аналізу відомчої нормативної бази зазначили, що до категорії службових таємниць відносяться:

- положення планів контрольно-ревізійної роботи на термін до часу повідомлення об'єкта контролю про початок проведених ревізій (перевірок);
- факти виявлених під час проведення ревізій і перевірок порушень, зловживань до їх повного документального підтвердження й закріплення в актах;
- надані правоохоронними органами оперативні та інші відомості щодо діяльності підприємств, установ і організацій (вчинених порушень, зловживань посадових осіб, дані посадовими особами письмові пояснення, протоколи допиту з конкретних питань тощо);
- інформація про оперативну й слідчу роботу органів прокуратури, МВС, СБУ, їхніх органів дізнання в тих випадках, коли її розголошення може зашкодити слідству, порушити право людини на справедливий та об'єктивний розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;
- конкретні пояснення посадових осіб щодо виявлення фактів зловживань, крадіжок тощо;
- відомості, які містяться у зверненнях громадян щодо їхнього (чи інших громадян) особистого життя, та інша інформація, що зачіпає (порушує) їхні права та законні інтереси;
- документи, що становлять внутрішньовідомчу службову кореспонденцію (доповідні записки, листування між підрозділами, матеріали колегій тощо);
- інформація банківських і фінансових установ та інших організацій, де вказані відомості, проходять як службова таємниця;
- чернетки матеріалів ревізій і перевірок<sup>94</sup>.

<sup>94</sup> Ботвінкін О. В. Інформація з обмеженим доступом, що не є державною таємницею, в законодавстві України : аналіт. огляд / О. В. Ботвінкін, В. П. Ворожко. — К. : НА СБ України, 2006. — 96 с., С. 38–39.

## **Поняття «службова інформація» у нормативно-правових актах**

Як ми зазначали раніше, поняття «службова таємниця» (службова інформація) не знайшло свого адекватного відображення у вітчизняному законодавстві, хоча ряд проектів вітчизняних нормативно-правових актів його закріплюють. Так, ще у проекті концепції Закону України «Про доступ до інформації» Центру політико-правових реформ **службова таємниця** визначається як склад і обсяг відомостей, що є в розпорядженні конкретного органу державної контрольно-ревізійної служби або її посадової особи стосовно об'єктів контролю, контрольних, правоохоронних та інших державних органів, їх працівників, способів досягнення визначених законодавством завдань, що необхідні для якісного проведення контрольно-ревізійних дій, забезпечення відповідної їх раптовості та ефективності і які з цієї причини на певний період не підлягають зовнішньому чи внутрішньому розголошенню.

Відповідно до проекту Закону України «Про державні секрети» **службова таємниця** — це вид інформації, що охоплює відомості у сфері внутрішньої та зовнішньої політики держави, оборони, державної безпеки та охорони правопорядку, державного управління, економіки, фінансів, банківської діяльності, науки і техніки, яка не становить державної таємниці, але розголошення якої може призвести до негативних наслідків та перешкод у зазначених сферах і має характер окремих даних, що можуть бути складовою відомостей, що становлять державну таємницю. Відомості, що віднесені до службової таємниці, мають ступінь обмеження доступу «Для службового користування».

Прогресивніше визначення службової таємниці міститься у законопроекті РФ «О служебной тайне», де вона розуміється як відомості, що створюються або накопичуються в органах державної влади, органах місцевого самоврядування і створюваних ними організаціях, і які включають як власне відомості про діяльність конкретного органу або організації, так і отримані від інших суб'єктів відомості конфіденційного характеру.

Загалом у законодавстві інших країн (Латвійська Республіка, Азербайджанська Республіка, Російська Федерація та ін.) немає поділу інформації з обмеженим доступом на конфіденційну й таємну. Так,

згідно із Законом Латвійської Республіки «Про свободу інформації» від 20 жовтня 1998 року під інформацією з обмеженим доступом розуміється інформація: 1) якій було надано такий статус відповідно до Закону; 2) призначена для внутрішнього користування органом; 3) що є комерційною таємницею; 4) яка стосується приватного життя фізичної особи; 5) яка має відношення до сертифікації, експертизи, поданих проєктів, запрошення на проведення тендера або оцінювання інших процесів подібного характеру<sup>95</sup>.

У Законі Азербайджанської Республіки «Про свободу інформації» від 19 липня 1998 року до інформації з обмеженим доступом належать: відомості, які стосуються державної, професійної (адвокатська, нотаріальна, лікарська), службової, банківської, комерційної, слідчої та судової таємниці, відомості про особисте й сімейне життя, терористичні акції<sup>96</sup>.

Законом Російської Федерації «Про інформацію, інформаційні технології та про захист інформації» від 29 липня 2006 року передбачено такі види інформації з обмеженим доступом: державна таємниця, комерційна таємниця, службова таємниця, професійна таємниця та інші таємниці. Перелік не є вичерпним. Установлено також, що охорона персональних даних здійснюється окремим Законом<sup>97</sup>. У згаданому Законі Російської Федерації термін «конфіденційна інформація» не використовується. Передбачається тільки термін «конфіденційність», що означає обов'язкове виконання особою, яка отримала доступ до певної інформації, вимоги не передавати таку інформацію третім особам без згоди її власника.

Щодо чинних нормативно-правових актів, то це поняття міститься в окремих підзаконних актах. Зокрема у Постанові правління фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань України від 17 жовтня 2003 року визначено, що **службова таємниця** — склад і обсяг відомостей, що є в розпорядженні працівників робочих органів виконавчої дирекції Фонду стосовно страхувальника, що необхідні для якісного проведення переві-

<sup>95</sup> О свободе информации [Электронный ресурс] : Закон Латвийской Республики от 20 дек. 1998 р. — Режим доступа : <http://arhivi.lv/>.

<sup>96</sup> О свободе информации [Электронный ресурс] : Закон Азербайджанской Республики от 19 июня 1998 г. — Режим доступа : <http://medialaw.ru>.

<sup>97</sup> Об информации, информационных технологиях и о защите информации [Электронный ресурс] : Федеральный Закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ. — Режим доступа : <http://rg.ru/2006/07/09/>.

ки і які з цієї причини на певний період не підлягають зовнішньому чи внутрішньому розголошенню.

В акті Головного контрольно-ревізійного управління України, до речі, зареєстрованому в Міністерстві Юстиції України, дане поняття є ідентичним дефініції, запропонованої в проекті Закону України «Про державні секрети»<sup>98</sup>.

Зважаючи на вище визначене, під **службовою таємницею** слід розуміти відомості, що охороняються державою, в будь-якій галузі науки, техніки, виробництва та управління, розголошення (передача, виток тощо) яких може завдати шкоди інтересам держави.

### **Ознаки службової інформації**

До ознак інформації, яка становить службову таємницю, Ю. С. Шемшушенко на підставі чинного законодавства відносить, зокрема, такі: 1) це конфіденційна інформація, що є власністю держави; 2) одержання, використання, поширення і зберігання службової таємниці здійснюється посадовими особами, які є державними і муніципальними службовцями у зв'язку з виконанням ними службових обов'язків відповідно до закону; 3) режим інформації, що становить службову таємницю, яким визначаються порядок віднесення інформації до службової таємниці та її розсекречення, порядок захисту, зберігання, передачі та доступу до такої інформації встановлюється спеціальними нормативно-правовими актами<sup>99</sup>.

В. О. Мазуров виділяє такі ознаки службової таємниці:

- 1) віднесена законом до службової інформації про діяльність державних органів, доступ до якої обмежений за законом чи в силу службової необхідності;
- 2) є конфіденційною інформацією іншої особи (комерційна таємниця, банківська таємниця, таємниця приватного життя);
- 3) не є державною таємницею і не підпадає під перелік відомостей, доступ до яких не може бути обмежений;

<sup>98</sup> Про затвердження Інструкції про порядок проведення ревізій і перевірок Державною контрольно-ревізійною службою в Україні [Електронний ресурс] : наказ Головного контрольно-ревізійного управління України. — Режим доступу : <http://zakon2.rada.gov.ua>.

<sup>99</sup> Великий енциклопедичний юридичний словник / за ред. акад. НАН України Ю. С. Шемшушенка. — К. : Юридична думка, 2007. — 992 с.

- 4) отримана представником державного органу, органу місцевого самоврядування тільки в силу виконання обов'язків по службі у випадках і в порядку, установлених законом;
- 5) має дійсну чи потенційну цінність у силу невідомості її третім особам<sup>100</sup>.

### **Співвідношення понять «службова таємниця» та «державна таємниця»**

Співвідношення понять «державна таємниця» та «службова таємниця» має здійснюватися з урахуванням ретроспективного аналізу.

У радянському законодавстві використовували словосполучення — «державні секрети», під яким розумілись усі відомості, які підлягають охороні державою та розголошення яких може завдати шкоди державним інтересам. Державні секрети охоплювали державна, військова та службова (виробнича) таємниці.

Як слушно зауважують В. В. Макаренко, С. В. Суслін, С. М. Сидоренко, А. К. Гринь, «загальнодержавна система забезпечення охорони державних секретів СРСР являла собою комплексний правовий інститут, що характеризувався наступними загальними ознаками:

- наявністю комплексної системи норм законодавства (конституційного, адміністративного, кримінального тощо), регулюючих суспільні відносини у даній сфері охоронної діяльності держави (норми права, що визначають посадову поведінку по відношенню до предмета охорони; норми, що визначають сам предмет охорони; повноваження, форми і методи охоронної діяльності державних органів для забезпечення збереження об'єкта охорони; відповідальність посадових осіб і громадян за незабезпечення збереження або за посягання на об'єкт охорони та ін.);
- наявністю кола державних органів та посадових осіб, до офіційної компетенції яких входить обов'язок забезпечувати збереження об'єкта їх охоронної діяльності;
- наявністю кола державних органів, здійснюючих контроль за забезпеченням збереження відповідних об'єктів, тобто за дотри-

<sup>100</sup> Мазуров В.А. Тайна: государственная, коммерческая, банковская, частной жизни. Уголовно-правовая защита : [учеб. пособ.] / В. А. Мазуров ; под науч. рук. д-ра юрид. наук, проф. С. В. Землюкова. — М. : Дашков и К, 2003. — 156 с., С. 22.



манням порядку діяльності державних установ, підприємств та організацій, які здійснюють цю охоронну діяльність;

- наявністю встановленого державою порядку і об'єму відповідальності (кримінальної, адміністративної, дисциплінарної) за порушення режиму забезпечення збереження відповідного об'єкта і за посягання на об'єкт охорони (державну таємницю)<sup>101</sup>.

Відсутність законодавчого визначення цього терміна компенсувалась тим, що їх правовий режим знаходив своє закріплення в різноманітних інструкціях, положеннях, переліках відомостей, де зазначалось, що:

- державну таємницю складають відомості, розголошення (передача, витік тощо) яких може негативно вплинути на якісний стан військово-економічного потенціалу країни чи спричинити інші тяжкі наслідки для обороноздатності, державної безпеки, економічних і політичних інтересів СРСР;
- службову таємницю складають відомості, що охороняються державою в будь-якій галузі науки, техніки, виробництва та управління, розголошення (передача, витік тощо) яких може завдати шкоди інтересам держави<sup>102</sup>.

Відомості, що складала державну таємницю, залежно від ступеня секретності мали гриф «особливої важливості» і «цілком таємно», а відомості, що складала службову таємницю — гриф «таємно».

Зауважимо, що поряд з вищезазначеними відомостями існувала також інформація, яка була заборонена до опублікування у засобах масової інформації і мала гриф «для службового користування». Останню називали несекретними відомостями обмеженого розповсюдження. У зв'язку з цим деякі науковці вважали, що службова таємниця містить відомості, які мали гриф «таємно» та «ДСК».

Різниця між ними полягала в їх важливості для забезпечення державних інтересів, формі і ступеню відповідальності за їх розголошення та відповідної шкоди, яка нанесена чи могла бути нанесеною внаслідок розголошення таких відомостей. До державних секретів належала лише

<sup>101</sup> Організаційно-правові основи охорони конфіденційної інформації, що є власністю держави : [навч. посіб.] / В. В. Макаренко, С. В. Суслін, С. М. Сидоренко, А. К. Гринь. — К. : НА СБ України, 2008. — 73 с., С. 6.

<sup>102</sup> Макаренко В. Проблема визначення місця державних секретів в системі інформації з обмеженим доступом [Електронний ресурс] / В. Макаренко. — Режим доступу : <http://www.bezpeka.com/ru>.



та частина відомостей, що складали службову таємницю, розголошення яких наносило чи могло нанести шкоди державним інтересам.

У правовому відношенні питання захисту службової таємниці як складової державної таємниці вирішувалися у двох аспектах:

- встановлення спеціального режиму поводження із відомостями, що охороняються в установах, організаціях і на підприємствах, діяльність яких безпосередньо пов'язана зі створенням та використанням цих відомостей;
- розробка заходів по недопущенню витоку державної таємниці та її розголошенню посадовими чи іншими особами при здійсненні наданих їм державою прав і обов'язків у відповідній сфері діяльності<sup>103</sup>.

### **Співвідношення понять «службова таємниця» і «професійна таємниця»**

У сучасному українському законодавстві визначення поняття «професійна таємниця» міститься лише у двох нормативно-правових актах, а саме: в Законі України «Про рахункову палату»<sup>104</sup> та в Законі України «Про фінансові послуги та державне регулювання ринків фінансових послуг»<sup>105</sup>.

Під професійною таємницею в Законі України «Про рахункову палату» розуміється стан збереження матеріалів, документів, інших відомостей, якими користуються посадові особи Рахункової палати та особи, які залучаються до здійснення функцій Рахункової палати під час проведення перевірок, ревізій, обслідувань, і про які забороняється розголошувати у будь-якій формі до моменту прийняття рішення Рахункової палати<sup>106</sup>.

<sup>103</sup> Організаційно-правові основи охорони конфіденційної інформації, що є власністю держави : [навч. посіб.] / В. В. Макаренко, С. В. Суслін, С. М. Сидоренко, А. К. Гринь. — К. : НА СБ України, 2008. — 73 с., С. 7.

<sup>104</sup> Про Рахункову палату : Закон України від 11 лип. 1996 р. // Відомості Верховної Ради України. — 1996. — № 43. — Ст. 212.

<sup>105</sup> Про фінансові послуги та державне регулювання ринків фінансових послуг : Закон України від 12 лип. 2001 р. // Відомості Верховної Ради України. — 2002. — № 1. — Ст. 1.

<sup>106</sup> Про Рахункову палату : Закон України від 11 лип. 1996 р. // Відомості Верховної Ради України. — 1996. — № 43. — Ст. 212.

У Законі України «Про фінансові послуги та державне регулювання ринків фінансових послуг» під професійною таємницею розуміються матеріали, документи, інші відомості, якими користуються в процесі та у зв'язку з виконанням своїх посадових обов'язків посадові особи державних органів, що здійснюють регулювання ринків фінансових послуг, та особи, які залучаються до здійснення цих функцій, і які забороняється розголошувати у будь-якій формі до моменту прийняття рішення відповідним уповноваженим державним органом<sup>107</sup>.

Отже, у законодавстві України немає загального поняття професійної таємниці та службової таємниці. Не закріплюється належним чином і перелік відомостей, які належать до таких видів інформації. Поняття професійної таємниці дається щодо діяльності Рахункової палати та державних органів, які регулюють ринки фінансових послуг. Поняття службової таємниці надано стосовно органів контролюно-ревізійної служби та інших органів.

Положення законодавства щодо службової інформації (поняття, перелік відомостей) не узгоджені між собою.

В юридичній літературі до професійної таємниці зараховують такі види інформації з обмеженим доступом: лікарська таємниця, професійна таємниця суддів, адвокатська таємниця, таємниця вчинення нотаріальних дій, таємниця усиновлення.

Здебільшого в наукових колах професійну таємницю визначають як окремий вид інформації з обмеженим доступом, що об'єднує відомості, одержувані суб'єктом-професіоналом про фізичних і юридичних осіб при виконанні ним професійних обов'язків. Отже, професійна таємниця містить досить широке коло різного роду інформації і заснована на специфіці діяльності представників багатьох професій.

Особливість даного виду інформації з обмеженим доступом в тому, що конфіденційні відомості, що належать фізичним і юридичним особам, отримуються і використовуються іншою особою — представником певної професії при виконанні професійних обов'язків з метою забезпечення реалізації і захисту прав і законних інтересів фізичних і юридичних осіб. Зазначена особливість, своєю чергою, визначає специфіку як суб'єктного складу і змісту, так і специфіку підстав виник-

<sup>107</sup> Про фінансові послуги та державне регулювання ринків фінансових послуг : Закон України від 12 лип. 2001 р. // Відомості Верховної Ради України. — 2002. — № 1. — Ст. 1.

нення правового режиму професійної таємниці щодо конкретних відомостей.

Професійна таємниця визначається не змістом конкретних відомостей, а їх наявністю у віданні визначених законом державних органів внаслідок виконання ними своїх функцій. Виконання зазначеної діяльності обумовлює строковий характер професійної таємниці — обмеження доступу скасовуються після закінчення такої діяльності органами державної влади. Для інформації, що становить професійну таємницю, може бути характерним перехід до категорії таємної з категорії конфіденційної (якщо до моменту передачі у відання відповідних органів власник визнав зазначену інформацію конфіденційною). В такому випадку скасування обмеження доступу до неї як до таємної інформації не скасовує її належності до категорії конфіденційної. Такий перехід може відбуватися й щодо інших видів таємної інформації.

Таким чином, питання загального визначення і систематизації професійної та службової таємниці потребують додаткового дослідження й адекватного закріплення на законодавчому рівні.

### ***Охорона документів, що мають гриф «Для службового користування»***

Такі документи повинні зберігатися у службових приміщеннях і бібліотеках у шафах (сховищах), які надійно замикаються та опечатуються. Забороняється зберігати такі документи у підсобних фондах бібліотек.

Справи з грифом «Для службового користування», видані для роботи, підлягають поверненню у канцелярію або архівний підрозділ у той же день.

Окремі справи з грифом «Для службового користування» з дозволу керівника канцелярії або архівного підрозділу організації можуть перебувати у виконавця протягом терміну, необхідного для виконання завдання, за умови повного забезпечення їх схоронності та додержання правил зберігання.

Про факти втрати документів з грифом «Для службового користування» або розголошення відомостей, що містяться в них, терміново доводиться до відома керівника організації, керівників режимно-секретного підрозділу та канцелярії, а також письмово повідомляються

органи СБУ із зазначенням обставин втрати документів чи розголошення відомостей та вжитих заходів.

Для розслідування факту втрати документів з грифом «Для службового користування» або встановлення факту розголошення відомостей, що містяться в них, наказом керівника організації призначається комісія, висновок якої затверджується керівником організації.

Відповідні записи про втрачені документи вносяться в облікові форми на підставі акта комісії, затвердженого керівником організації.

За порушення, що призвели до розголошення інформації «Для службового користування», втрати або незаконного знищення документів з грифом «Для службового користування», особи несуть кримінальну, адміністративну та дисциплінарну відповідальність згідно із законодавством.

## ВИСНОВКИ

Сучасний стан адміністративно-правового регулювання суспільних відносин у сфері інформації з обмеженим доступом в Україні потребує поліпшення та узгодження з міжнародними стандартами. Йдеться, передусім, про удосконалення адміністративно-правового статусу суб'єктів забезпечення захисту інформації з обмеженим доступом, а також внесення відповідних змін та доповнень до чинного Кодексу України про адміністративні правопорушення. Однак, якщо в адміністративно-правових розвідках і приділяється достатня увага окремим видам інформації з обмеженим доступом, проте цілісного, системного розгляду проблема адміністративно-правового режиму інформації з обмеженим доступом в Україні не знайшла адекватного відображення.

За результатами проведеного дослідження вважаємо за необхідне сформулювати такі найбільш важливі та практично значущі, науково обґрунтовані висновки.

1. Окреслено історіографію дослідження інформації з обмеженим доступом у вітчизняній адміністративній доктрині. Інформація з обмеженим доступом як правовий феномен у вітчизняній адміністративній доктрині є доволі новим та майже не розробленим. Було виділено три основні етапи становлення наукової думки, що присвячена інформації з обмеженим доступом, у вітчизняній адміністративній доктрині. Перший етап (1991 — 2005 рр.) характеризується поверховим розглядом інформації з обмеженим доступом у контексті дослідження різних аспектів інформаційної безпеки та інформаційного права, де захист і охорона інформації з обмеженим доступом визначається як важливий напрям інформаційної безпеки чи інститут інформаційного права, а також актуальний напрям наукової діяльності. Для другого етапу (2006 — 2007 рр.) властива поява досліджень монографічного рівня, предметом яких є безпосередньо інформація

з обмеженим доступом, особливості доступу до зазначеної вище інформації та виділення основних видів таємниць. Третій етап (2008 — донині) характеризується інтенсивним проведенням наукових досліджень та опублікуванням робіт різної спеціалізації, предметом яких є конкретні види таємниць (банківська, комерційна, персональна таємниця тощо).

2. Надано авторське бачення поняття «інформація з обмеженим доступом» та виділено її конститутивні ознаки в адміністративно-правовому контексті. Інформація з обмеженим доступом визначається як відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, доступ до яких обмежено відповідно до законодавства України її власником чи добросовісним користувачем (суб'єктом владних повноважень, фізичною або юридичною особою) у зв'язку з її особливою цінністю для них на законних підставах. Серед конститутивних ознак інформації з обмеженим доступом в адміністративно-правовому контексті є такі: 1) інформація з обмеженим доступом — це, насамперед, відомості, дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді; 2) інформацією, до якої може буде застосований обмежений режим доступу, є така, що не суперечить чинному законодавству України; 3) певне коло користувачів отримали доступ до неї винятково на законних підставах (добросовісні користувачі); 4) інформація з обмеженим доступом має особливу цінність для вищезазначеної категорії суб'єктів (моральну, матеріальну, особисту тощо) в силу невідомості її іншим суб'єктам; 5) власники та добросовісні користувачі інформації з обмеженим доступом здійснюють адекватні законні заходи з метою унеможливлення доступу сторонніх суб'єктів; 6) за порушення вищезазначених заходів встановлена юридична відповідальність.

3. Визначено поняття «адміністративно-правовий режим інформації з обмеженим доступом» та виокремлено основні його ознаки. Адміністративно-правовий режим інформації з обмеженим доступом — це урегульований у вітчизняному законодавстві порядок діяльності уповноважених суб'єктів права шляхом імперативного методу правового впливу та системи спеціальних засобів з метою захисту й охорони суспільних відносин у сфері інформації з обмеженим доступом. Ознаки адміністративно-правового режиму

інформації з обмеженим доступом: це порядок діяльності уповноважених органів державної влади, інших уповноважених державою інституцій, органів місцевого самоврядування, окремих громадян щодо інформації з обмеженим доступом; ця діяльність є урегульованою у вітчизняному законодавстві шляхом визначення режимних правил, відповідно до яких зазначено права, обов'язки людини і громадянина, повноваження відповідних інституцій, адміністративна відповідальність за їх порушення тощо у сфері інформації з обмеженим доступом; наявність імперативного методу правового впливу між учасниками відносин у сфері інформації з обмеженим доступом; здійснюється за допомогою відповідної системи різноманітних спеціальних засобів; метою такої діяльності є забезпечення захисту й охорони суспільних відносин у сфері інформації з обмеженим доступом, тобто відповідних прав і свобод людини та громадянина, інтересів держави та суспільства.

4. Класифіковано інформацію з обмеженим доступом на види. На законодавчому рівні не визначено критерії, за допомогою яких можна однозначно кваліфікувати ті чи інші відомості (дані) як інформацію з обмеженим доступом чи виділити основні її види. Закон України «Про доступ до публічної інформації» лише містить норму, згідно з якою інформацією з обмеженим доступом є: 1) конфіденційна інформація; 2) таємна інформація; 3) службова інформація. В окремих статтях вищезазначеного Закону надається легальна дефініція конфіденційної та таємної інформації, а також деталізується розуміння службової інформації. Було класифіковано інформацію на таку, яка є взагалі забороненою для розповсюдження в конкретній країні, та таку, розповсюдження якої має обмеження в силу певних обставин, наприклад нанесення шкоди певним категоріям осіб. Своєю чергою, конфіденційною інформацією, на нашу думку, слід визнавати будь-яку інформацію з обмеженим доступом, що не має ознак державної таємниці, а таємною — будь-яку інформацію з обмеженим доступом, що має ознаки державної таємниці.

4. Охарактеризовано елементи адміністративно-правового режиму інформації з обмеженим доступом, зокрема мету встановлення правового режиму, правові принципи, об'єкт адміністративно-правового регулювання, метод правового регулювання, «режимні правила», спеціальні державні органи, відповідальність за порушення «ре-



жимних норм», визначення просторово-часових меж дії цього адміністративно-правового режиму.

5. Визначено недоліки та надано пропозиції щодо удосконалення адміністративно-правового режиму державної таємниці. Основними чинниками, що негативно впливають на стан адміністративно-правового режиму державної таємниці, є: соціально-економічні, кадрові, організаційні тощо, а саме: плинність кадрів у режимно-секретних органах; відсутність необхідних спеціальних знань у сфері інформаційних технологій та правовій сфері, а також недостатньої обізнаності зі специфікою діяльності правоохоронних органів та змістом завдань, на вирішення яких спрямована діяльність таких органів; недостатнє знання деякими особами, які мають допуск і доступ до державної таємниці, норм чинного законодавства про державну таємницю; неналежне обладнання приміщень режимно-секретних органів та істотна застарілість форм і методів захисту державної таємниці тощо. Задля удосконалення адміністративно-правового режиму державної таємниці було запропоновано передбачити проведення перевірки знання норм законодавства про державну таємницю та правил секретного діловодства особами, яким надається не лише допуск до державної таємниці, а й доступ. Механізм перевірки знань норм законодавства про державну таємницю пропонується передбачити на рівні певної Інструкції чи Правил, які розробила б Служба безпеки України як основний орган, що здійснює захист державної таємниці, та закріпила на рівні Наказу Служби безпеки України. Серед шляхів удосконалення адміністративно-деліктного законодавства у цій сфері було підтримано позицію окремих авторів про необхідність доповнення чинного КУпАП (або закріпити це у новому Кодексі України про адміністративні проступки) нормою, що передбачала б адміністративну відповідальності юридичних осіб за порушення законодавства про державну таємницю, а також підвищення суми санкції як попередження адміністративних правопорушень, відповідальність за вчинення яких встановлено у ст. 212–2 КУпАП. Було також запропоновано розширити спектр адміністративних стягнень, зокрема поряд зі штрафом передбачити такі стягнення, як: громадські роботи, виправні роботи, адміністративний арешт. На думку авторів, є необхідність посилення санкції за вчення правопорушення, передбаченого ст. 212–2 КУпАП, у воєнний час. Необхідним напрямом удо-

сконалення адміністративно-деліктного законодавства у цій сфері є, по-перше, внесення змін до ст. 212–2 КУпАП, зокрема об'єднати п. 1, відповідно до якого передбачено відповідальність за недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації, та п. 8, згідно з яким передбачено відповідальність за недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними. На думку авторів, п. 8 охоплює п. 1. Так, порушення порядку передачі державної таємниці іншій державі чи міжнародній організації і є одним із порушень вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними. По-друге, дана стаття містить ряд оціночних понять, що потребують законодавчого визначення, серед яких: «реальна загроза», «порушення цілісності», «безпідставне засекречування інформації» тощо. Було запропоновано чітко визначити на законодавчому рівні перелік підстав засекречування інформації.

6. Розкрито стан та перспективи розвитку адміністративно-правового режиму персональних даних. Серед основних недоліків адміністративно-правового режиму персональних даних було виділено такі: колізійність норм нормативно-правових актів, що регулюють суспільні відносини у сфері захисту персональних даних і наявність численних прогалин; неоднозначність, неузгодженість та суперечливість закріплених дефініцій та подекуди відсутність навіть базових із них; наявність значного масиву декларативних положень за відсутності механізму їх правореалізації; наявність численних бланкетних норм права, що ускладнює їх правореалізацію; наявність абстрактних, суб'єктивних понять, що потребують офіційного тлумачення або чіткого визначення тощо. Серед основних шляхів удосконалення адміністративно-правового режиму персональних даних було запропоновано такі: визначити поняття «суспільної необхідності» як передумови поширення персональних даних без згоди суб'єкта персональних даних; урегулювати правовий режим персональних даних, що містяться в базах даних після смерті особи, а також порушення

права фізичної особи на конфіденційність її персональних даних та заборону обробки її даних без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини; розширити коло осіб, на яких дія Закону України «Про захист персональних даних» не поширюється, а саме: на журналістів Інтернет-ЗМІ, якщо такий засіб масової інформації не має статусу інформаційного агентства або журналіст не перебуває в професійному об'єднанні журналістів; законодавчо визначити випадки перевірки уповноваженими органами захисту персональних даних, зокрема за фактом надходження скарги від особи про неправомірне використання її персональних даних, а також межі втручання, процедуру проведення перевірок і складання відповідних актів у разі порушення законодавства про захист персональних даних тощо Державною службою України з питань захисту персональних даних.

7. Охарактеризовано адміністративно-правовий режим службової інформації. Інститут службової таємниці безпосередньо пов'язаний з інститутом державної таємниці. У ст. 10 Закону України «Про державну таємницю» передбачено можливість органів державної влади на підставі та в межах закону і з метою конкретизації та систематизації даних про інформацію, що віднесена до державної таємниці, створювати розгорнуті переліки відомостей, що становлять державну таємницю. Оприлюднення розгорнутих переліків не передбачено. Проте закріплено право зацікавлених осіб оскаржити Президенту України чи Верховній Раді України внесення до розгорнутих переліків такої інформації, яка за змістом не може визнаватись державною таємницею. Ретроспективний аналіз питання співвідношення понять «державна таємниця» та «службова таємниця» дозволяє дійти висновку, що тривалий час у законодавстві було використане інше поняття — «державні секрети», під яким розумілись всі відомості, які підлягають охороні з боку держави та розголошення яких може завдати шкоди державним інтересам. Державні секрети охоплювали державну, військову та службову (виробничу) таємницю. Відсутність законодавчого визначення цих термінів компенсувалася тим, що їх правовий режим знаходив своє закріплення в різноманітних інструкціях, положеннях, переліках відомостей, де визначалось, що: державну таємницю складають відомості, розголошення (передача, виток тощо) яких може негативно вплинути на якісний стан

військово-економічного потенціалу країни чи спричинити інші тяжкі наслідки для обороноздатності, державної безпеки, економічних і політичних інтересів СРСР; службову таємницю складають відомості, що охороняються державою в будь-якій галузі науки, техніки, виробництва та управління, розголошення (передача, виток тощо) яких може завдати шкоди інтересам держави. Відомості, що складала державну таємницю, в залежності від ступеня секретності мали гриф «особливої важливості» і «цілком таємно», а відомості, що складала службову таємницю, гриф «таємно». Необхідно зазначити, що поряд з вищезазначеними відомостями існувала також інформація, яка була заборонена до опублікування у засобах масової інформації і мала гриф «для службового користування». Останню називали не-секретними відомостями обмеженого розповсюдження. У зв'язку з цим деякі науковці вважали, що службова таємниця включала відомості, які мали гриф «таємно» та «ДСК». Різниця між ними полягала в їх важливості для забезпечення державних інтересів, формі і ступеню відповідальності за їх розголошення та відповідної шкоди, яка нанесена чи могла бути нанесеною внаслідок розголошення таких відомостей. До державних секретів відносилась лише та частина відомостей, що складала службову таємницю, розголошення яких наносило чи могло нанести шкоди державним інтересам. Відповідно до Закону України «Про доступ до публічної інформації» **до службової інформації може належати така інформація:** 1) що міститься в документах суб'єктів владних повноважень, які становлять внутрішню службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; 2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці. Ця інформація є інформацією з обмеженим доступом, тому доступ до неї є обмеженим при дотриманні сукупності таких вимог: 1) винятково в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно,

або для підтримання авторитету і неупередженості правосуддя; 2) розголошення інформації може завдати істотної шкоди цим інтересам; 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні. Органи державної влади, органи місцевого самоврядування, інші суб'єкти владних повноважень зобов'язані створювати переліки відомостей, що становлять службу інформацію. Слід виділити такі основні засади створення цих переліків: 1) рішення про надання (зняття) грифу ДСК інформації приймаються безпосередніми виконавцями документів згідно з даним Переліком та за висновками експертних комісій; 2) документам, що містять інформацію, яка становить службу інформацію, присвоюється гриф «для службового користування» (далі ДСК); 3) відомості з грифом ДСК є власністю держави і такими, що містять відомості обмеженого поширення; 4) відповідальність за правильне присвоєння грифу ДСК виробам та інформації несуть посадові особи, які надали гриф, підписали або затвердили ці документи; 5) у разі скасування рішення віднесення інформації до службової про зняття грифа обмеження доступу повідомляються всі організації, яким надсилався цей документ; 6) копіювання сторонніми організаціями документів з грифом «Для службового користування» повинно здійснюватись за погодженням з організацією — автором цих документів; 7) використання інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи для друкування документів з грифом ДСК здійснювати тільки після створення в ній комплексної системи захисту інформації та отримання відповідного атестату; 8) передача інформації ДСК з однієї системи до іншої здійснюється захищеними каналами зв'язку або у зашифрованому вигляді. Використання Інтернету або незахищених каналів для передачі інформації ДСК заборонено; 9) за розголошення відомостей ДСК винні особи притягаються до адміністративної відповідальності згідно з чинним законодавством. Визначено перелік орієнтовних критеріїв віднесення службової інформації: 1) повинні створюватися за кошти державного бюджету або перебувати у володінні, користуванні чи розпорядженні організації; 2) використовуватися з метою забезпечення національних інтересів держави; 3) не належати до державної таємниці; 4) унаслідок розголошення такої інформації можливе: 4.1 порушення конституційних прав і свобод людини та громадянина; 4.2 настання негатив-

них наслідків у внутрішньополітичній, зовнішньополітичній, економічній, військовій, соціальній, гуманітарній, науково-технологічній, екологічній, інформаційній сферах та у сферах державної безпеки і безпеки державного кордону; 4.3 створення перешкод у роботі державних органів<sup>108</sup>.

---

<sup>108</sup> Про внесення змін до постанови Кабінету Міністрів України від 27 лист. 1998 р. № 1893: постанов. Кабінету Міністрів України від 17 лист. 2004 р. // Офіційний вісник України. — 2004. — № 46. — Ст. 3033.

## CONCLUSIONS

The current state of administrative and legal regulation of social relations in the field of information with limited access in Ukraine needs improvement and harmonization with international standards. It is primarily about improving the administrative and legal status of entities ensuring the protection of information with limited access and making relevant changes and amendments to the current Code of Ukraine on Administrative Offences. However, a holistic, systematic consideration of the problem of administrative and legal regime of information with limited access does not exist in Ukraine, despite the presence of sufficient attention to certain types of information with limited access in the administrative and legal researches.

By the results of the research we consider necessary to formulate the most important, practically meaningful and scientifically valid conclusions.

1. The historiography of research information with limited access in national administrative doctrine has been outlined. Information with limited access is quite new and barely developed legal phenomenon in the national administrative doctrine. Have been identified three main stages of development scientific thought, which is devoted to information with limited access in national administrative doctrine. The first phase (1991 — 2005 years) is characterized by superficial consideration information with limited access in the context of the study of various aspects of information security and information law, the protection and preservation of where information with limited access is defined as the important area of information security or institute of information law and topical direction of research activities also. The second phase (2006 — 2007 years) characterized by the appearance of monographic researches, subject of which is directly information with limited access, features access to the above information and allocation of the main kinds of secrets. The third phase



(2008 — till present) is characterized by intense conducting scientific researches and publication of papers with different specializations, squarely focused on the specific kinds of secrets (banking, commercial, personal secret, etc.).

2. A new solution of concept of «information with limited access» and allocated its constitutive features of the administrative and legal context has been provides. Information with limited access is defined as information and/or data, that may be stored on material carriers or displayed electronically, access to which is limited by the laws of Ukraine by its owner or bona fide user (the entity of authority, person etc.) due to its special value for them on a legal basis. Among the constitutive features information with limited access in the administrative and legal context are the following: 1) the information with limited access — is primarily information, data that can be stored on physical media or displayed electronically, and 2) information, which can be applied to a limited access mode is such that complies with the legislation of Ukraine, 3) a certain number of Members gained access to it solely on legal grounds (bona fide users) 4) information with limited access is of particular value for the above categories of subjects (moral, financial, personal, etc.) because of uncertainty of other entities, 5) bona fide owners and users of information with limited access realize adequate legal measures to prevent access by unauthorized entities, 6) for violation of the above measures established legal responsibility.

3. The concept of «administrative and legal regime of information with limited access» and singled out its main features has been determined. Administrative and legal regime of information with limited access — is regulated by the national legislation operational procedure of the authorized entities by imperative method of legal enforcement and system of special facilities for the protection and conservation of public relations in the information with limited access field. Features of administrative and legal regime of information with limited access: it is the order of the authorized state bodies and other competent state institutions, local governments, and individuals regarding to information with limited access, this activity is regulated in the national legislation by determining the operational rules under which indicated rights and duties of man and citizen, authority of suitable institutions, administrative liability for violations, etc. in the field of information with limited access, the presence of imperative meth-

od of legal impact between the participants of relations in the field of information with limited access, is carried out by an appropriate system of various special facilities, the purpose of this activity is to provide protection and conservation of public relations in the area of information with limited access, i.e. the respective rights and freedoms of man and citizen interests of the state and society.

4. Information with limited access on the kinds has been classified. The criteria, by which to unambiguously classify certain information (data) as information with limited access or identify its main kinds in the legislation does not identified. The Law of Ukraine «An Access to Public Information» contains only the norm, according to which the information with limited access is: 1) confidential information, 2) secret information, and 3) service information. In some articles of the above Law is given legal definition of confidential and secret information, and detailed understanding of service information. Have been classified information to such, that is generally forbidden for distribution in particular country and such, spread of which is limited due to certain circumstances, such as damage to certain categories of people. In turn, confidential information, in our opinion, should be recognized any information with limited access, that has no features of state secrets and the secret information — is any information with limited access, which has features of state secrets.

5. Have been characterized the elements of administrative and legal regime of information with limited access, including the purpose of establishing the legal regime, legal principles, the object of administrative regulation, the method of regulation, «regime rules», special public bodies, responsibility for the violations of the «regime norms», definition of the spatial and temporal boundaries of this administrative and legal regime.

6. Has been determined the deficiencies and provided the suggestions for improving the administrative and legal regime of state secrets. The main factors that negatively affect the condition of administrative and legal regime of state secrets are: socio-economic, human, organizational, etc., namely employee turnover at regime-secret bodies, lack of necessary special knowledge in IT and in the legal field, and also lack of awareness with the specifics activities of law enforcement bodies and content of tasks, are aimed at addressing the activities of such bodies, lack of knowledge about the current legislation on state secrets by some persons, who have admission and access to state secrets; improper equipment of premises re-

gime-secret bodies and significant obsolescence of forms and methods of protection of state secrets etc. In order to improve administrative and legal regime of state secrets we propose to provide the audit of knowledge of the legislation on state secrets and rules of the secret case management, by persons, who not only have also admission & access to state secrets. The mechanism verification knowledges of legislative norms on state secret is proposed to predict at the level of some instruction or Rules, which has to develop Security Service of Ukraine as the main body, which protects state secrets. Among the ways of improving the administrative and delictual legislation in this field, we have supported the opinion of some authors about the need to supplement the current Administrative Code (or fix it in the new Code of Ukraine on administrative offenses) by norm, that would provide the administrative responsibility of legal persons for the violation of legislation on state secrets and also increasing amounts of penalties as a warning of administrative offenses, liability for which is set in Art. 212–2 of Administrative Code. Also we propose to extend the range of administrative penalties. For example, along with a fine collection to foresee such as: community service, correctional work, administrative arrest. According to the authors, there is need to strengthen penalties for offense under Art. 212–2 of Administrative Code, in wartime. It is necessary to improve the administrative and delictual legislation in this field in: amendments to Art. 212–2, in particular, to unite claim 1 (according to which liability for failure to comply with established by law order of convey of state secrets to another state or international organization is provided), with claim 8 (which provides the responsibility for noncompliance with legal requirements on ensuring the protection of national secrets, during the international cooperation, receiving foreign delegations, groups and individual foreigners or stateless person and carrying out the work with them). According to the authors, claim 8 covers claim 1. For example, violation of the order state secrets convey to another state or international organization just also is one of the violations of legislation concerning ensuring the protection of national secrets, during the international cooperation, receiving foreign delegations, groups and individual foreigners or stateless person and carrying out the work with them. Additionally, this article contains a number of evaluating notions that require legislative determination, among which «real danger», «destroying the integrity», «unreasonable information security classification» and so on. Therefore, we proposed

to clearly define reasons for information security classification at the legislative level.

7. The state and development prospects of administrative and legal regime of personal data have described. To the main shortcomings of the administrative and legal regime of personal data we include: collision of legal acts norms that regulate public relations at personal data protection and the presence of numerous gaps, ambiguity, inconsistency and fixed definitions contradiction, either lack even a basic of them sometimes; the presence of considerable massifs of declarative provisions without the mechanism of law realization; the presence of numerous blanket law norms, that complicates its legal implementation, the presence of abstract, subjective concepts, which need an official interpretation or clear definition etc. To improve administrative and legal regime of personal data we offer the following ways: to define the concept of «public necessity» as a prerequisite for dissemination of personal data without the consent of the subject of personal data; to settle the legal regime of personal data contained in the databases after the death of the person and a violation of person rights to confidentiality of personal data and the prohibition of processing of data without its consent, except in cases determined by law and only in the interests of national security, economic prosperity and human rights; to expand the number of people who are not covered by the Law of Ukraine «On Personal Data Protection», namely: online media journalists (if the media has no status news agency or journalist is not in professional association of journalists); legally to define verification occasions by competent authorities of personal data protection, in particular if person sends a complaint about the illegal use its personal data, as well as intervention boundaries, procedure of conducting inspections and making the relevant acts for violations the legislation on protection of personal data, etc. by the State Service of Ukraine on protection of personal data.

8. Administrative and legal regime for service information has been characterized. Institute of professional secrecy is directly connected with the institution of state secrets. In Art. 10 Law of Ukraine «On State Secrets» the ability of public authorities on the basis and within the law and in order to specify and systematize data information classified as state secrets to create detailed lists of information that constitute a state secret has provided. Publication of detailed lists is not provided. However, the right of interested persons to appeal to President of Ukraine or the Verk-

hovna Rada of Ukraine, inclusion in detailed lists information that cannot be recognized as state secret in content, has been established. Retrospective analysis of the relationship between the concepts of «state secrecy» and «official secret» made possible to conclude that for a long time in legislation has been used another concept — «state secrets», which are understood all information that has to be protected by the state and its divulge could harm the public interest. State secrets covering state, military and service (industrial) secrets. Lack of legal definition of these terms was compensated by the fact that their legal regime was enshrined in the various instructions, regulations, lists of information, which identifies that: State secrets are information divulgence of which (transfer, leakage, etc.) may adversely affect the quality status of military and economic potential of the country or cause other serious consequences for national defense, national security, economic and political interests of the USSR; official secrets are information that is protected by the state in any field of science, engineering, production and administration, disclosure of which (transfer, leakage, etc.) may harm the interests of the state. The information was a state secret depending on the degree of secrecy: «special importance» and «top secret» and information that constituted official secrets, classified «secret». It should be noted that along with the above information, there is also information that was forbidden to publish in the media and was «for official use only». The latter was called unclassified information with limited dissemination. In this regard, some scholars believed that the official secret includes information that classified as «secret» and «OU». The difference between them lay in their importance for the public interest, the form and degree of responsibility for their disclosure and related harm from publicizing of such information. Only part of information which was professional secrecy, the disclosure of which could harm the public interests to state secrets belonged. The following information may belong to service information according to the Law of Ukraine «On Access to Public Information»: 1) the information, contained in the documents of government entities, that make up the interdepartmental correspondence, memorandums, recommendations, if they are related to the entity activities or realization of control & supervisory functions bodies of state power, decision-making and are preceded public discussion and/or decision-making; 2) the information, gathered during operational and investigative, counterintelligence

activities in the field of defense of the country, which is not classified as state secrets. This information is information with limited access, so access to it is limited, subject to the following set of requirements: 1) only in the interests of national security, territorial integrity or public order, the prevention of disorder or crime, for the protection of health, protection of the reputation or rights of others, for preventing the disclosure of received confidentially information or for maintaining the authority and impartiality of the judiciary; 2) disclosure of the information would cause substantial harm to those interests, and 3) the harm from disclosure of the information outweighs the public interest in getting it. The state authorities, local authorities, other government entities are obliged to create lists of data that is service information. The following basic principles of creating these lists have distinguished: 1) the decision to grant (withdrawal) for official use only information are accepted by direct implementers of documents according to the list and according to the conclusions of expert commissions, and 2) a document that contains information that is service information, is assigned a security classification «for official use only» (further — OU); 3) «OU» information is the property of the state and contains limited distribution information; 4) for correct «OU» assignment to wares and information, have responsibility the officials who have provided classification, signed or approved these documents; 5) In case of cancellation of security classification of information, about removal restricting access, all of the organizations to whom it was sent, should be reported; 6) copying of «OU» documents by outside organizations should be done by agreement with the organization — the author of these documents; 7) use of information, telecommunication and information-telecommunication systems for printing of «OU» documents, carried out only after creation therein a comprehensive system of information protection and obtain the appropriate certificate; 8) transfer of «OU» information from one system to another is carried out by secure communication channel or in encrypted form. Using the Internet or unprotected channels for the transfer «OU» information is prohibited; 9) guilty persons will be brought to administrative liability in accordance with current legislation for disclosure of «OU» information. List of approximate criteria for classification service information has been identified: 1) should be established by the state budget or be in the possession, use or disposal of the organization; 2) be used in order

to ensure the state national interests, 3) do not belong to a state secret, and 4) as a result of disclosure of such information is possible: 4.1 The violation of constitutional rights and freedoms of man and citizen; 4.2 occurrence of negative consequences in domestic political, foreign, economic, military, social, humanitarian, scientific, technological, environmental, and information spheres, also in the areas of national security and the state border security; 4.3 creation of obstacles in the activities of public authorities.<sup>109</sup>

---

<sup>109</sup> About the Amending the Resolution of the Cabinet of Ministers of Ukraine dated 27 November 1998 N 1893: Resolution of the Cabinet of Ministers of Ukraine // Official Herald of Ukraine. — 2004. — № 6. — Art. 3033.



## ТЕЗАУРУС

**Адвокатська таємниця** — це питання, з яких громадянин або юридична особа зверталися до адвоката, зміст консультацій, поради та роз'яснення з приводу вирішення правових питань, а також інші відомості, отримані адвокатом від його клієнта, його представників та/або з інших джерел при здійсненні адвокатської діяльності; вся інформація, одержана від клієнта і про клієнта, а також яка стала відомою адвокату у зв'язку з поданням правової допомоги, здійсненням захисту і представництва, щодо якої відсутня згода клієнта на її розголошення. Правила адвокатської етики зобов'язують зберігати конфіденційність будь-якої інформації, зокрема, будь-яку інформацію про клієнта, в тому числі щодо його особи або інших осіб у процесі здійснення адвокатської діяльності.

**Адміністративно-правовий режим** — це специфічний порядок діяльності суб'єктів права в різних сферах державного життя, який встановлюється в законах та підзаконних актах і спрямований на їх суворо цільову та функціональну діяльність у тій царині, де необхідні додаткові засоби для підтримки необхідного державного ладу.

**Адміністративно-правовий режим інформації з обмеженим доступом** — це урегульований у вітчизняному законодавстві порядок діяльності уповноважених суб'єктів права шляхом імперативного методу правового впливу та системи спеціальних засобів з метою захисту й охорони суспільних відносин у сфері інформації з обмеженим доступом.

**Акумуляція нормативно-правових актів** — накопичення масиву текстів нормативно-правових актів із питань регулювання суспільних відносин в інформаційній сфері та інформації про їх прийняття, зміну, припинення, що можуть здійснюватись як у паперовій, так і в електронній та цифровій формах.

**Аудіовізуальні засоби масової інформації:** радіомовлення, телебачення, кіно, звукозапис, відеозапис.

**Банківська таємниця** — інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третіми особами при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту.

**Віднесення інформації до державної таємниці** — процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня її секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього.

**Відповідальність за порушення законодавства про інформацію** — передбачена ст. 47 Закону України «Про інформацію», згідно з якою порушення законодавства про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність.

**Володілець бази персональних даних** — фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедуру їх обробки, якщо інше не визначено законом.

**Гриф секретності** — реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації.

**Державна політика національної безпеки** — передбачає утвердження засад національної єдності задля розбудови демократичної, правової, конкурентоспроможної держави, формування соціально орієнтованої ринкової економіки, зміцнення науково-технологічного потенціалу, забезпечення інноваційного розвитку, зростання рівня життя і добробуту населення, забезпечення інформаційної безпеки, екологічно-, техногеннобезпечних умов життєдіяльності суспільства. Державна політика національної безпеки України формується і реалізується за умов, коли у сучасному світі нівелюється різниця між внутрішні-

ми та зовнішніми аспектами безпеки, зростає вага несилових, передусім, інформаційних складових її забезпечення.

**Державна таємниця (секретна інформація)** — вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом України «Про державну таємницю», державною таємницею і підлягають охороні державою.

**Державний експерт з питань таємниць** — посадова особа, уповноважена здійснювати відповідно до українського законодавства віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування.

**Доктрина інформаційної безпеки** — офіційний документ методологічного (концепція — документ концептуального рівня) рівня, в якому визначені засади державної інформаційної політики, керівні принципи, цільові настанови та напрями забезпечення інформаційної безпеки, окреслений механізм функціонування системи інформаційної безпеки. Слугує основою для: формування державної політики інформаційної безпеки України; підготовки пропозицій з удосконалення правового, методичного, науково-технічного й організаційного забезпечення інформаційної безпеки України; формування напрямів систематизації (інкорпорації, консолідації, кодифікації) інформаційного законодавства; розроблення концепцій, стратегій, цільових програм і планів дій із забезпечення інформаційної безпеки України.

**Допуск до державної таємниці** — оформлення права громадянина на доступ до секретної інформації.

**Доступ до державної таємниці** — надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

**Друковані засоби масової інформації** — періодичні друковані видання (преса) — газети, журнали, бюлетені тощо і разові видання з визначеним накладом.

**Е**лементи структури права на інформацію — збирання, зберігання, використання, поширення інформації.

**Ж**иттєво важливі інтереси в інформаційній сфері: 1) особи: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних; захищеність від негативного інформаційно-психологічного впливу; 2) суспільства: збереження і примноження духовних, культурних і моральних цінностей Українського народу; забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; формування і розвиток демократичних інститутів громадянського суспільства; 3) держави: недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав і міжнародних структур; ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері; побудова та розвиток інформаційного суспільства; забезпечення економічного та науково-технологічного розвитку України; формування позитивного іміджу України; інтеграція України у світовий інформаційний простір.

**Життєво важливі національні інтереси України** — права і свободи людини і громадянина; суверенітет України, її територіальна цілісність, недоторканність державного кордону, демократичного конституційного ладу, верховенство права; соборність держави на основі консолідації усіх територіальних громад, суспільних верств, етнічних груп навколо цінностей незалежного, вільного, суверенного і демократичного розвитку єдиної України; конкурентоспроможність держави та економічний добробут населення шляхом всебічного розвитку людського, науково-технічного, інноваційного потенціалів країни; удосконалення механізмів реалізації конституційного принципу розподілу влади на законодавчу, виконавчу та судову; неухильне дотримання гарантій незалежності та об'єктивності суду; обмеження втручання держави у діяльність економічних суб'єктів, громадян, громадських організацій та політичних партій, релігійних об'єднань; безпечні умови життєдіяльності, захист навколишнього природного середовища; збереження і розвиток духовних і культурних цінностей суспільства; гармонійні відносини з іншими держава-

ми світу, сприйняття Української держави міжнародним співтовариством як повноцінного та рівноправного його члена.

**Загрози інформаційній безпеці** — прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства та держави.

**Загрози національній безпеці** — наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України.

**Закон України «Про основи національної безпеки України»** — нормативно-правовий акт, прийнятий Верховною Радою України 19 червня 2003 року, який відповідно до пункту 17 частини першої статті 92 Конституції України визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.

**Законодавство у сфері інформаційної безпеки України** — охоплює: закони України «Про Національну систему конфіденційного зв'язку» від 10 січня 2002 року, «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 червня 1994 року, «Про державну таємницю» від 21 січня 1994 року, Постанову Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» від 8 жовтня 1997 року, Указ Президента України «Про Доктрину інформаційної безпеки України» від 8 липня 2009 року тощо.

**Засекречування матеріальних носіїв інформації** — введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

**Засоби масової інформації:** 1) теле- і радіомовна організації, інформаційні агентства та друковані засоби масової інформації.

ції; 2) система організацій із відображення суспільних процесів і оточуючого середовища, які створюють, обробляють і доводять до масового споживача інформацію; 3) юридичні особи, які здійснюють соціально-комунікативну діяльність на підставі державної реєстрації з метою виробництва, зберігання і публічного поширення інформації. Поділяються на аудіовізуальні та друковані.

**Звід відомостей, що становлять державну таємницю** — акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених сферах.

**Зміст доктрини інформаційної безпеки** — понятійно-категорійний апарат, методологічне розв'язання проблем забезпечення інформаційної безпеки, широка і завершена система поглядів, що ґрунтується на категоріях, які мають базовий і парадигмальний серед фахівців характер саме у цій доктрині. Зміст доктрин має ґрунтуватися на системі логічних доказів і знаходити свій вираз у поняттях, що відображають дійсність із забезпечення інформаційної безпеки.

**Інтерес** — (лат. *interest* — має значення, важливо) — 1) об'єктивно обумовлена необхідність виконання людьми (групами людей, організаціями тощо) певних функцій для задоволення потреб. І. перебувають у причинно-наслідковому зв'язку з іншими спорідненими категоріями потреба, стимул (мотив). Інтерес виступає зв'язуючою ланкою в даному ланцюгу. Інтерес з одного боку виступає формою потреб, а з іншого — причиною виникнення стимулу; 2) реальна дій, подій, звершень, що стоять за безпосередніми мотивами, помислами, ідеями, намірами і т.д. індивідів, соціальних груп і держав, що беруть участь у цих діях.

**Інформаційна безпека:** 1) невід'ємна складова кожної зі сфер національної безпеки, водночас — важлива самостійна сфера забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки; 2) безпека інформації (вузьке розуміння), а також як система, що складається з інформаційно-технічної, інформаційно-психологічної безпеки та інформаційної безпеки у сфері прав і свобод (широке розуміння).



**Інформаційна ідеологія** (ідеології інформаційного суспільства) — становить сукупність ідей та уявлень щодо інформаційних інтересів «свого» інформаційного суспільства, і механізмів їхньої реалізації в рамках конвергенції інформаційних суспільств різних країн до глобального інформаційного суспільства.

**Інформаційне законодавство** — складна внутрішньо обумовлена єдність законів і підзаконних актів, об'єднаних одним предметом нормативно-правового регулювання (інформаційні відносини), узгодженістю імперативно-диспозитивного впливу на суміжні з ними відносини та своєрідною системністю, зумовленою ієрархією правових норм у сфері інформації.

**Інформаційне законодавство спрямовано на забезпечення:** 1) дотримання конституційного права кожного «вільно збирати, зберігати, використовувати і поширювати інформацію» будь-яким законним способом (ст. 34 Конституції України), зокрема ознайомлюватися з документами і матеріалами, що безпосередньо стосуються його прав і свобод; перетворення сучасної Української держави на інформаційну; 2) можливість контролю з боку громадян і громадських організацій діяльності органів державної влади; 3) захист авторського права і права майнової власності на інформаційні ресурси, інформаційні технології та засоби їх забезпечення; 4) формування і використання інформаційних ресурсів в умовах рівності всіх форм власності шляхом створення інформаційного ринку і конкурентного середовища, проведення державної антимонопольної політики; 5) відповідальність суб'єктів інформаційних відносин за правопорушення під час формування інформаційних ресурсів та їх використання, зокрема персональної відповідальності керівників органів державної влади за якість формування державних інформаційних ресурсів і доступу до них; 6) узгодженості рішень і активного використання єдиного інформаційного простору; тісної інформаційної взаємодії з країнами-членами СНД і активного інформаційного обміну в системі міжнародного співробітництва.

**Інформаційне суспільство:** 1) суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку; 2) суспільство нового типу, що формується внаслідок глобальної соціальної революції та породжується вибуховим розвитком і конвергенцією інформаційних і комунікаційних технологій; 3)



суспільство знань, тобто суспільство, у якому головною умовою добробуту кожної людини і кожної держави стає знання, здобуте завдяки безперешкодному доступу до інформації та вмінню працювати з нею; 4) глобальне суспільство, в якому обмін інформацією не матиме ні часових, ні просторових, ні політичних меж; яке, з одного боку, сприяє взаємопроникненню культур, а з іншого — відкриває кожному співсуспільству нові можливості для самоідентифікації.

**Інформаційні відносини** — 1) однорідна група суспільних відносин, що виникають при використанні інформації в інформаційній сфері в результаті здійснення інформаційних процесів при реалізації кожним інформаційних прав і свобод, а також при виконанні обов'язків органами державної влади і місцевого самоврядування щодо забезпечення гарантій інформаційних прав і свобод; 2) інформаційні зв'язки між суб'єктами політичної системи суспільства, держави, що виникають під час одержання, використання, зберігання та споживання інформації; 3) такі відносини, що виникають між громадянами України, іноземними громадянами, особами без громадянства, юридичними особами, державою та міжнародними організаціями в усіх сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні документованої або публічно оголошеної інформації про події та явища в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах.

**Інформаційні інтереси** — це система інформаційних потреб, задоволення яких забезпечує саме існування і можливість сталого прогресивного розвитку інформаційного суспільства ... об'єктивні потреби матеріального та духовного існування як внутрішньо цілісного та самобутнього соціального утворення ... усвідомлені інформаційним суспільством та виражені в Глобальній хартії інформаційного суспільства, Декларації про державний суверенітет, Конституції України, Стратегії національної безпеки України, Доктрині інформаційної безпеки України, Засадах внутрішньої та зовнішньої політики, Концепції державної інформаційної політики, Законі України «Про основні засади розвитку інформаційного суспільства в Україні» чи якомусь іншому документі конституційного рівня у вигляді програмних цільових настанов життєво важливі інформаційні потреби існування та сталого прогресивного та безпечного розвитку енерго-інфор-

маційного середовища, людини, соціальних систем і держав. Інформаційні інтереси — це фундаментальні, базові та висхідні цінності інформаційного суспільства.

**Кібернетика** (від грецьк. — мистецтво управляти) — наука про загальні закони отримання, збереження, передавання і розповсюдження інформації у складних управляючих системах. При цьому під управляючими системами розуміється не лише технічні, а й біологічні та соціальні системи. Прикладами складних управляючих систем є нервові системи живих організмів, особливо організм людини, а також апарат управління у суспільстві.

**Комерційна таємниця** — інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та важкодоступною для осіб, які зазвичай мають справу з тим видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

**Конфіденційна інформація** — інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов

**Масова інформація** — публічно поширювана друкована та аудіовізуальна інформація.

**Мета адміністративно-правового режиму** — це забезпечення співробітництва державної адміністрації і окремих осіб у відповідній сфері задля якнайбільшої реалізації прав і свобод, а також дієвого захисту і поновлення у разі їх порушення.

**Мета адміністративно-правового режиму інформації з обмеженим доступом** — забезпечення співробітництва державної адміністрації і окремих осіб у сфері захисту інформації з обмеженим доступом задля задоволення національних інтересів держави і суспільства, якнайбільшої реалізації громадянами інформаційних прав і свобод у цій сфері, а також дієвого захисту і поновлення у разі їх порушення.

**Мета Стратегії національної безпеки України** — забезпечити такий рівень національної безпеки, який гарантував би посту-

пальний розвиток України, її конкурентоспроможність, забезпечення прав і свобод людини і громадянина, подальше зміцнення міжнародних позицій та авторитету Української держави у сучасному світі.

**Напрями державної політики інформаційної безпеки:** 1) активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України; 2) забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері та переслідування журналістів за політичні позиції; 3) забезпечення інформаційного суверенітету України; 4) вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; 5) вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

**Напрями державної політики у сфері технічного захисту інформації:** 1) удосконалення чинних та створення нових нормативно-правових актів щодо захисту інформації, яка становить державну та іншу, передбачену законом таємницю, конфіденційної інформації, що належить державі; 2) розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави; 3) удосконалення правових механізмів організаційного забезпечення ТЗІ; 4) удосконалення нормативно-правових актів щодо умов і правил провадження діяльності у сфері ТЗІ; 5) розроблення нормативно-правових актів щодо визначення статусу головної у сфері ТЗІ, головних (базових) за напрямками ТЗІ організацій; 6) удосконалення нормативно-правових актів щодо здійснення контролю за імпортом з метою впровадження в Україні іноземних інформаційних технологій із захистом інформації та засобів забезпечення ТЗІ; 7) розроблення нормативних документів із питань формування та розвитку моделі загроз для інформа-

ції; 8) розроблення нормативних документів із питань сертифікації засобів забезпечення ТЗІ та атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту; 9) удосконалення чинних та розроблення нових нормативних документів із питань ТЗІ тощо.

**Національна безпека** — захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання та нейтралізація реальних та потенційних загроз національним інтересам.

**Національні інтереси** — життєво важливі матеріальні, інтелектуальні та духовні цінності Українського народу як носія суверенітету й єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток.

**Об'єкти інформаційних відносин** — документована або публічно оголошувана (оприлюднена) інформація про події та явища в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах.

**Об'єкт режиму інформації з обмеженим доступом** — ті відносини у сфері інформації з обмеженим доступом, які фактично потрапили під дію адміністративно-правових норм, тобто відносин у зв'язку з необхідністю реалізації права на інформацію та захистом національних інтересів між різного роду запитувачами інформації (фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи) та розпорядниками інформації.

**Обов'язки учасників інформаційних відносин:** 1) поважати інформаційні права інших суб'єктів; використовувати інформацію згідно із законом або договором (угодою); 2) забезпечувати дотримання принципів інформаційних відносин; 3) забезпечувати доступ до інформації усім споживачам на умовах, передбачених законом або угодою; 4) зберігати інформацію в належному стані протягом встановленого терміну та надавати іншим громадянам, юридичним особам або державним органам у передбаченому законом порядку; 5) компенсувати шкоду, заподіяну при порушенні законодавства про інформацію.

**Ознаки адміністративно-правових режимів:** 1) застосування у сфері діяльності публічної адміністрації у зв'язку з виконан-

ням органами державної влади, місцевого самоврядування своїх обов'язків, заходів щодо забезпечення безпеки, охорони, захисту об'єктів правового регулювання; 2) наявність у розпорядженнях, що утворюють режимні правила, адміністративно-правових норм, які забороняють та зобов'язують, а також обмежують загальну правосуб'єктність фізичних та юридичних осіб; 3) обов'язкова участь у якості основних суб'єктів органів виконавчої влади або місцевого самоврядування, які реалізують державні повноваження; 4) застосування адміністративно-правових методів впливу; 5) наявність заходів адміністративного та дисциплінарного впливу.

**Ознаки адміністративно-правового режиму інформації з обмеженим доступом:** 1) це діяльність уповноважених органів державної влади, інших уповноважених державою інституцій, органів місцевого самоврядування, окремих громадян щодо захисту інформації з обмеженим доступом; 2) ця діяльність є урегульованою у вітчизняному законодавстві шляхом визначення режимних правил, відповідно до яких вказуються права, обов'язки людини і громадянина, повноваження відповідних інституцій, адміністративна відповідальність за їх порушення тощо у сфері захисту інформації з обмеженим доступом; 3) наявність імперативного методу правового впливу між учасниками відносин у сфері захисту інформації з обмеженим доступом; 4) здійснюється за допомогою відповідної системи різноманітних спеціальних засобів; 5) метою такої діяльності є забезпечення захисту суспільних відносин у сфері захисту інформації з обмеженим доступом, тобто відповідних прав і свобод людини та громадянина, інтересів держави та суспільства.

**Ознаки інформаційних правовідносин:** 1) виникають, розвиваються та припиняються у зв'язку з інформацією; 2) визначають державну політику щодо дотримання і захисту інформаційних прав людини; 3) відбивають особливості застосування публічно-правових і цивільно-правових методів правового регулювання; 4) є ідеологічними відносинами — результатом свідомої діяльності людей, спрямованої на формування необхідного суб'єкту управління інформаційного впливу; 5) виникають, припиняються або змінюються, як правило, на основі норм права; 6) мають, як правило, багатосторонній характер і є особливою формою взаємного зв'язку між невизначеним колом суб'єктів (соціальні мережі) через їхні права, обов'язки, повноваження

і відповідальність; 7) гарантуються державою через механізми реалізації державної інформаційної політики, зокрема через реалізацію державної політики інформаційної безпеки; 8) їм притаманний вольовий характер.

**Ознаки інформаційного суспільства** — компоненти, які описують інформаційне суспільство: 1) будь-який індивід, група людей, підприємство або організація в будь-якому місці країни й у будь-який час можуть одержати за відповідну плату або безоплатно на основі автоматизованого доступу та систем зв'язку певну інформацію і знання, необхідні для їхньої життєдіяльності та розв'язання як особистих, так і соціально значимих завдань; 2) виробляється, функціонує, є доступною будь-якому індивіду, групі або організації сучасна інформаційна технологія; 3) розвинені інфраструктури, що забезпечують створення національних інформаційних ресурсів в обсязі, необхідному для підтримки постійно прискореного науково-технічного прогресу; 4) прискорена автоматизація, роботизація і комп'ютеризація всіх сфер і галузей виробництва та управління; 5) радикальні зміни соціальних структур, наслідком яких стає розширення сфери інформаційної діяльності та послуг.

**Основні елементи адміністративно-правового режиму** — мета встановлення правового режиму, правові принципи, об'єкт адміністративно-правового регулювання, метод правового регулювання, «режимні правила», спеціальні державні органи, відповідальність за порушення «режимних норм», визначення просторово-часових меж дії адміністративно-правових режимів.

**Основні режимні правила адміністративно-правового режиму інформації з обмеженим доступом:** обґрунтування про необхідність віднесення інформації до інформації з обмеженим доступом шляхом окреслення можливої шкоди від її розголошення національній безпеці, інтересам окремих громадян, суспільству; визначення відомостей, які не можуть бути віднесені до інформації з обмеженим доступом; віднесення інформації до інформації з обмеженим доступом, тобто прийняття рішення про віднесення категорії відомостей або окремих відомостей до інформації з обмеженим доступом з установленням її виду; окреслення прав, свобод і обов'язків учасників правовідносин у зв'язку з доступом до інформації з обмеженим доступом; визначення правового статусу органів державної влади у сфері захисту інформації з обмеженим доступом



сфері інформації; визначення системи контролю і нагляду за виконанням режимних вимог фізичними, юридичними, посадовими особами тощо.

**Охорона державної таємниці** — комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативних заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

**Персональним дані** — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

**Правове регулювання інформаційних відносин в Україні** — здійснюване державою за допомогою права та сукупності правових засобів упорядкування відносин, які виникають між громадянами України, іноземними громадянами, особами без громадянства, юридичними особами, державою та міжнародними організаціями в усіх сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації, їх юридичне закріплення, безпека і розвиток засобів масової інформації: друківані та аудіовізуальні ЗМІ.

**Правовий моніторинг** — цілеспрямована систематична діяльність суб'єктів моніторингу щодо відстеження, обліку, оцінювання та аналізу нормативних правових актів, які регулюють суспільні відносини в інформаційній сфері, з метою їх контролю, прогнозування, планування подальшого розвитку, підвищення ефективності, якості, а також ступеня їх доступності для суб'єктів інформаційних відносин і підвищення правової обізнаності останніх на основі наданих у результаті моніторингу рекомендацій.

**Правова основа розроблення та реалізації Стратегії національної безпеки України** — Конституція України, Закон України «Про основи національної безпеки України», інші закони України та міжнародні угоди, ратифіковані Верховною Радою України, які в сукупності визначають засади політики держави у сфері національної безпеки.

**Правовий режим** — 1) особливий порядок законодавчого регулювання діяльності суб'єктів права у різноманітних сферах суспільних відносин або на певних об'єктах, який складається зі встановлення механізму забезпечення фактичної реалізації системи стимулів, нормативів, гарантій, заборон, зобов'язань, обмежень, а також їх виконання, застосування заходів приму-



су та притягнення винних до відповідальності; 2) порядок регулювання, який виражений у комплексі правових засобів, що характеризують особливе сполучення взаємодіючих між собою дозволів та заборон, а також позитивних зобов'язань, які утворюють особливу направленість регулювання.

**Принципи адміністративно-правового режиму інформації з обмеженим доступом** — це висхідні ідеї, основоположні засади, на яких ґрунтується захист інформації з обмеженим доступом в конкретній країні.

**Принципи політики національної безпеки** — пріоритет прав і свобод людини і громадянина; верховенство права; пріоритет договірних (мирних) засобів у розв'язанні конфліктів; своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам; чітке розмежування повноважень і взаємодія органів державної влади у забезпеченні національної безпеки; демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави; залучення громадянського суспільства до процесу вироблення та реалізації політики національної безпеки; використання в інтересах України механізмів міжнародної колективної безпеки.

**Принципи формування Доктрини інформаційної безпеки** — основоположні начала, на яких ґрунтується процес формування Доктрини інформаційної безпеки. Виокремлюють дві групи принципів: 1) форми ДІБ, які описують засади формування самого документа; 2) змісту, які описують засади внутрішнього наповнення даної Доктрини — текстуальної, змістовної, світоглядної, ідеологічної і концептуальної складової.

**Режим** — 1) вся система заходів, які використовуються для досягнення поставлених перед ними цілей (шир. Розум.); 2) сукупність правил поведінки (вужке розум.).

**Режимні правила адміністративно-правового режиму** — це встановлена в законодавчому порядку сукупність правил діяльності юридичних осіб або поведінки фізичних осіб, а також державних органів, їх посадових чи службових осіб та реалізація ними своїх прав, свобод та обов'язків у чітко визначених ситуаціях (умовах).

**Службова інформація** — 1) відомості, що містяться в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації,

якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; 2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

**Службова таємниця** — це відомості, що охороняються державою в будь-якій галузі науки, техніки, виробництва та управління, розголошення (передача, виток тощо) яких може завдати шкоди інтересам держави.

**Стратегія національної безпеки України** — один із основоположних документів у сфері національної безпеки, в якому визначаються принципи, пріоритетні цілі, завдання та механізми забезпечення життєво важливих інтересів особи, суспільства та держави від зовнішніх і внутрішніх загроз.

**Структура Доктрини інформаційної безпеки** — внутрішня побудова Доктрини, яка має корелювати цілям її розроблення, у ній мають знайти своє відображення: поняття інформаційної безпеки, її місце в системі національної безпеки; поняття системи інформаційної безпеки; чітке визначення національних інтересів в інформаційній сфері, визначення їх пріоритетності; мета, задачі, функції, принципи, методи та напрями функціонування системи забезпечення інформаційної безпеки; обґрунтування функцій і структури, основних характеристик, властивостей і функціональних можливостей системи безпеки в інформаційній сфері за умови забезпечення єдності форми і змісту Доктрини.

**Ступінь секретності** («особливої важливості», «цілком таємно», «таємно») — категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

**Суб'єкти захисту інформації з обмеженим доступом** — це багаторівнева система фізичних чи юридичних осіб, а також відповідних органів державної влади чи органів місцевого самоврядування, що об'єднанні спільною метою, але мають при цьому різні повноваження, можливості, засоби тощо. Суб'єктами адміністративно-правового режиму конфіденційної інформації є фізична або юридична особа, яким належить така інформація, чи за їх уповноваженням будь-хто з розпорядників.

Суб'єктами адміністративно-правового режиму таємної інформації є здебільшого державні та недержавні інституції.

**Суб'єкти інформаційних відносин** — громадяни України, іноземні громадяни та особи без громадянства, юридичні особи, держава, інші держави та їх юридичні особи, міжнародні організації тощо.

**Суспільно значима інформація** — інформація, яка виступає предметом громадського інтересу за умови, що право громадськості знати цю інформацію переважає право власника на її захист.

**Таємна інформація** — це інформація, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та, іншу передбачену законом таємницю.

**Таємниця досудового слідства** — дані досудового слідства, які можна оголосити лише з дозволу слідчого або прокурора і в тому обсязі, в якому вони визнають це можливим.

**Технічний захист секретної інформації** — вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

**Уповноважений державний орган з питань захисту персональних даних** — це центральний орган виконавчої влади, до повноважень якого належить захист персональних даних, утворених відповідно до законодавства.

**Шлях підвищення ефективності вітчизняного інформаційного законодавства** — проведення широкомасштабної, поступової його систематизації через три основні форми: інкорпорацію, консолідацію та кодифікацію, розроблення концепції розвитку інформаційного законодавства.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Литвиненко О. В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії) : автореф. дис. на здобуття наук. ступеня політ. наук : спец. 23.00.04 «Політичні проблеми міжнародних систем та глобального розвитку»/ О. В. Литвиненко. — К., 1997. — 18 с.
2. Інформаційна безпека (соціально-правові аспекти) : навч. посіб. / [В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк та ін.] ; за заг. ред. Є. Д. Скулиша. — К. : КНТ, 2010. — 776 с.
3. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : дис. ... канд. юрид. наук : 12.00.01 / Юлія Євгенівна Максименко. — К., 2007. — 188 с.
4. Василюк В. Я. Інформаційна безпека держави : [курс лекцій] / В. Я. Василюк, С. О. Климчук. — К. : КНТ, 2008. — 135 с.
5. Юдін О. К. Інформаційна безпека держави : [навч. посіб.] / О. К. Юдін, В. М. Богуш. — Х. : Консул, 2005. — 576 с.
6. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : [навч. посіб.] / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. — К. : КНТ, 2006. — 280 с.
7. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : [навч. посіб.] / В. С. Сідак, В. Ю. Артемов. — К. : КНТ, 2007. — 160 с.
8. Харченко Л. С. Інформаційна безпека України : глосарій / Л. С. Харченко, В. А. Ліпкан, О. В. Логінов ; за заг. ред. Р. А. Калюжного. — К. : Текст, 2004. — 136 с.
9. Кормич Б. А. Інформаційна безпека : організаційно-правові основи : [навч. посіб.] / Б. А. Кормич. — К. : Кондор, 2004. — 382 с.
10. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : [монографія] / Б. А. Кормич. — Одеса : Юрид. літ., 2003. — 472 с.
11. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : дис. ... доктора юрид. наук : 12.00.07 / Борис Анатолійович Кормич. — Одеса, 2004. — 427 с.
12. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки : дис. ... канд. юрид. наук : 25.00.02 / Володимир Ігорович Гурковський. — К., 2004. — 225 с.
13. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності ОВС України: організаційно-правові засади : дис. ... доктора юрид. наук : 12.00.07 / Ірина Вікторівна Арістова. — Х., 2002. — 408 с.

14. Письменицький А. А. Информационное право Украины / А. А. Письменицкий. — Х. : Бизнес Информ, 1996. — 208 с
15. Основи інформаційного права України : навч. посіб. / [В. С. Цимбалюк, В. Д. Гавловський, В. В. Гриценко та ін.]; за ред. М. Я. Швеця, Р. А. Калюжного та П. В. Мельника. — К. : Знання, 2004. — 274 с.
16. Основи інформаційного права України : навч. посіб. / [В. С. Цимбалюк, В. Д. Гавловський, В. М. Брижко та ін.]; за ред. М. Я. Швеця, Р. А. Калюжного та П. В. Мельника. — [2-е вид.]. — К. : Знання, 2009. — 414 с.
17. Марущак А. І. Інформаційне право: доступ до інформації : [навч посіб.] / А. І. Марущак. — К. : КНТ, 2007. — 535 с.
18. Марущак А. І. Інформаційне право : регулювання інформаційної діяльності : [навч посіб.] / А. І. Марущак. — К. : Скіф ; КНТ, 2008. — 344 с.
19. Марущак А. І. Правомірні засоби доступу громадян до інформації : [навч.-практ. посіб.] / А. І. Марущак. — Біла Церква : Буква, 2006. — 432 с.
20. Цимбалюк В. С. Інформаційне право (основи теорії і практики) : [монографія] / В. С. Цимбалюк. — К. : Освіта України, 2010. — 388 с.
21. Копылов В. А. Информационное право : [учеб.] / В. А. Копылов. — М. : Юристъ, 2005. — 512 с.
22. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. / [А. Б. Стоцький, А. М. Гуз, А. І. Марущак та ін.]; за заг. ред. В. С. Сідака. — К. : Європ. ун-т, 2006. — 232 с.
23. Ботвінкін О. В. Інформація з обмеженим доступом, що не є державною таємницею, в законодавстві України : [аналіт. огляд] / О. В. Ботвінкін, В. П. Ворожко. — К. : НА СБ України, 2006. — 96 с.
24. Марущак А. І. Правові основи захисту інформації з обмеженим доступом : [курс лекцій] / А. І. Марущак. — К. : КНТ, 2007. — 208 с.
25. Носік Ю. В. Права на комерційну таємницю в Україні : [монографія] / Ю. В. Носік. — К. : КНТ, 2007. — 240 с.
26. Сляднева Г. О. Право суб'єкта господарювання на комерційну таємницю та його захист : автореф дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.04 «Політичні проблеми міжнародних систем та глобального розвитку» / Г. О. Сляднева. — Донецьк., 2005. — 16 с.
27. Радутний О. Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю (аналіз складів злочинів) : автореф дис. на здобуття наук. ступеня доктора юрид. наук : спец. 12.00.08 «Кримінальне право та криминологія ; кримінально-виконавче право» / О. Е. Радутний. — Х., 2002. — 36 с.
28. Нікіфоров Г. К. Підприємництво та правовий захист комерційної таємниці : [навч.-практ. посіб для вищ. навч. закл.] / Г. К. Нікіфоров, С. С. Нікіфоров. — К. : Олан, 2001. — 208 с.
29. Гетманцев Д. О. Банківська таємниця : особливості її нормативно-правового регулювання в Україні та в законодавстві зарубіжних країн : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне

- право і процес ; фінансове право ; інформаційне право»/ Д. О. Гетманцев. — К., 2003. — 23 с.
30. Дідук А. Г. Правовий режим конфіденційної інформації: цивільно-правовий аспект : дис. ... канд. юрид. наук : 12.00.03 / Алла Григорівна Дідук. — Х., 2008. — 243 с.
  31. Брижко В. М. Організаційно-правові питання захисту персональних даних : дис. ... канд. юрид. наук : 12.00.07 / Валерій Михайлович Брижко. — К., 2004. — 221 с.
  32. Організаційно-правові основи охорони конфіденційної інформації, що є власністю держави : навч. посіб. / [В. В. Макаренко, С. В. Суслін, С. М. Сидоренко та ін.]. — К. : Наук.-вид. відділ НА СБ України, 2008. — 73 с.
  33. Рудик М. В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом : дис. ... канд. юрид. наук : 12.00.08 / Михайло Вікторович Рудик. — Х., 2007. — 221 с.
  34. Цивільний кодекс України : прийнятий 16 січ. 2003 р. // Відомості Верховної Ради України. — 2003. — № 40–44. — Ст. 356.
  35. Кулініч О. О. Інформація з обмеженим доступом як об'єкт цивільних відносин : дис. ... канд. юрид. наук : 12.00.03 / Ольга Олексіївна Кулініч. — Одеса, 2006. — 200 с.
  36. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу : [навч. посіб] / А. М. Гуз. — К. : КНТ, 2007. — 260 с.
  37. Фатьянов А. А. Тайна как социальное и правовое явление. Ее виды / А. А. Фатьянов // Государство и право. — 1998. — № 6. — С. 5–14.
  38. Беляков К. І. Інформаційне право: аналіз термінологічно-понятійного апарату / К. І. Беляков // Науковий вісник Київського національного університету внутрішніх справ. — К., 2007. — Вип. 3. — С. 67–79.
  39. Про інформацію : Закон України від 2 жовт. 1992 р. // Відомості Верховної Ради України. — 1992. — № 48. — Ст. 650.
  40. Про державну таємницю : Закон України від 21 січ. 1994 р. // Відомості Верховної Ради України. — 1994. — № 16. — Ст. 93.
  41. Угода між Кабінетом Міністрів України та Урядом Республіки Білорусь про співробітництво в галузі технічного захисту інформації [Електронний ресурс] : від 22 січ. 2003 р. — Режим доступу : <http://zakon.rada.gov.ua>.
  42. Угода між Кабінетом Міністрів України та Урядом Республіки Таджикистан про співробітництво в галузі технічного захисту інформації [Електронний ресурс] : від 2 квіт. 2004 р. — Режим доступу : <http://zakon.rada.gov.ua>.
  43. Угода між урядом України та урядом Російської Федерації в галузі технічного захисту інформації [Електронний ресурс]. — Режим доступу : <http://zakon.rada.gov.ua>.
  44. Угода між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом : від 5 черв. 2003 р. // Офіційний вісник України. — 2004. — № 25. — Ст. 1639.
  45. Угода між Кабінетом Міністрів України та Урядом Словацької Республіки про взаємну охорону інформації з обмеженим доступом: від 22 лип. 2006 р. // Офіційний вісник України. — 2008. — № 99. — Ст. 3282.

46. Угода між Україною та Угорською Республікою про взаємну охорону інформації з обмеженим доступом : від 15 лист. 2006 р. // Офіційний вісник України. — 2008. — № 24. — Ст. 720.
47. Угода між Україною та Республікою Словенія про обмін та взаємну охорону інформації з обмеженим доступом : від 6 квіт 2008 р. ; ратиф. 2 груд. 2009 р. // Офіційний вісник України. — 2009. — № 29. — Ст. 961.
48. Угода між Кабінетом Міністрів України та Урядом Алжирської Народної Демократичної Республіки про охорону інформації з обмеженим доступом : від 7 квіт. 2008 р. // Офіційний вісник України. — 2009. — № 49. — Ст. 554.
49. Угода між Кабінетом Міністрів України та Урядом Республіки Македонія про взаємну охорону інформації з обмеженим доступом : від 29 черв. 2009 р. // Офіційний вісник України. — 2011. — № 3. — Ст. 162.
50. Угода між Кабінетом Міністрів України та Урядом Йорданського Хашимітського Королівства про взаємну охорону інформації з обмеженим доступом Електронний ресурс] : підпис. 14 берез. 2011 р. — Режим доступу : [http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=400\\_017](http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=400_017)
51. Про Основи національної безпеки України : Закон України від 19 черв. 2003 р. // Відомості Верховної Ради України. — 2003. — № 39. — Ст. 351.
52. Баскаков В. Ю. Захист інформації з обмеженим доступом в умовах боротьби з організованою злочинністю / В. Ю. Баскаков // Боротьба з організованою злочинністю і корупцією (теорія і практика). — К., 2011. — № 24. — С. 263–269.
53. Баскаков В. Інформація з обмеженим доступом : аналіз термінологічно-понятійного апарату / В. Баскаков // Підприємництво, господарство і право. — 2011. — № 5. — С. 124–127.
54. Бачило И. Л. Информационное право / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов ; под ред. Б. Н. Топорнина. — СПб. : Юридический центр Пресс, 2001. — 789 с.
55. Ахлибининский Б. В. Информация и система / Б. В. Ахлибининский. — Л. : Лениздат, 1969. — 432 с.
56. Кураков Л. П. Информация как объект правовой защиты / Л. П. Кураков, С. Н. Смирнов. — М. : Гелиос, 1998. — 240 с.
57. Тарасенко Ф. П. Введение в курс теории информации / Ф. П. Тарасенко. — Томск : Том. гос. ун-т, 1963. — 345 с.
58. Кохановська О. Класифікація та види інформації у доктрині права і законодавстві України / О. Кохановська // Підприємництво, господарство і право. — 2002. — № 3. — С. 78–81.
59. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. // Офіційний вісник України. — 2011. — № 10. — Ст. 446.
60. Капіца Ю. М. Проблеми правової охорони комерційної таємниці, ноу-хау та конфіденційної інформації в праві України : реферативний огляд чинного законодавства України та практика його застосування / Ю. М. Капіца ; за ред. В. В. Цветкова, Є. Б. Кубко. — К.: Салком, 2000. — 296 с.
61. Алексенцев А. И. О составе защищаемой информации / А. И. Алексенцев // Безопасность информационных технологий. — 1999. — № 2. — С. 4–9.



62. Лопатин В. Н. Правовая охрана и защита коммерческой тайны / В. Н. Лопатин // Законодательство. — 1998. — № 11. — С. 14–21.
63. Лопатин В. Н. Концепция развития законодательства в сфере обеспечения информационной безопасности Российской Федерации : проект / В. Н. Лопатин. — М. : Гос. Дума, 1998. — 158 с.
64. Гражданское право : в 2 т. : учеб. [для студ. высш. учеб. завед. / отв. ред. проф. Е. А. Суханов. — [2-е изд., перераб. и доп.]. — М. : БЕК, 1998—. — Т. 1. — 1998. — 816 с.
65. Андрощук А. Секретна інформація як об'єкт правової охорони / А. Андрощук // Інтелектуальна власність. — 1999. — № 3–4. — С. 27–32.
66. Об утверждении сведений колнфиденциального характера [Электронный ресурс] : указ Президента Российской Федерации. — Режим доступа : <http://www.rg.ru/2006/07/29/informacia-dok.html>.
67. О информации, информатизации и защите информации [Электронный ресурс] : Закон Российской Федерации от 25 янв. 1995 г. — Режим доступа : <http://www.rg.ru/2006/07/29/informacia-dok.html>.
68. Пилипенко Ю. С. Общетеоретические аспекты института тайны / Ю. С. Пилипенко // Государство и право. — 2009. — № 7. — С. 19–24.
69. Кормич Б. А. Інформаційне право : [підруч.] / Б. А. Кормич. — Х. : БУРУН і К., 2011. — 334 с.
70. Про захист суспільної моралі : Закон України від 20 лист. 2003 р. // Відомості Верховної Ради України. — 2004. — № 14. — Ст. 192.
71. Господарський кодекс України : Закон України від 16 січ. 2003 р. // Відомості Верховної Ради України. — 2003. — № 18. — Ст. 144.
72. Митний кодекс України : Закон України від 13 берез. 2012 р. // Відомості Верховної Ради України. — 2012. — № 44–45, № 46–47, № 48. — Ст. 552.
73. Про правовий режим земель охоронних зон об'єктів магістральних трубопроводів : Закон України від 17 лют. 2011 р. // Офіційний вісник України. — 2011. — № 22. — Ст. 898.
74. Про землі енергетики та правовий режим спеціальних зон енергетичних об'єктів : Закон України 9 лип. 2010 р. // Відомості Верховної Ради України. — 2011. — № 1. — Ст. 1.
75. Про правовий режим воєнного стану : Закон України 6 квіт 2000 р. // Відомості Верховної Ради України. — 2000. — № 28. — Ст. 224.
76. Про правовий режим надзвичайного стану : Закон України від 16 берез. 2000 р. // Відомості Верховної Ради України. — 2000. — № 23. — Ст. 176.
77. Угода СНД про правовий режим інформаційних ресурсів Прикордонних військ держав-учасниць Співдружності Незалежних Держав[Електронний ресурс] : від 25 лист. 1998 р. — Режим доступу : <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi>.
78. Про ратифікацію Договору між Україною і Республікою Польща про правовий режим українсько-польського державного кордону, співробітництво та взаємну допомогу з прикордонних питань : постан. Верховної Ради України від 12 січ. 1991 р. // Відомості Верховної Ради України. — 1993. — № 36. — Ст. 365.

79. Ганшина К. А. Французско-русский словарь : 51 000 слов / К. А. Ганшина. — [изд. 7-е, стереотип.]. — М. : Рус. яз., 1977. — 912 с.
80. Латино-русский словарь / [состав. Д. И. Фомицкий ] ; ред. Л. Ф. Цымлова, Т. А. Ширяева. — Ростов-на-Дону : Феникс, 1998. — 704 с.
81. Ожегов С. И. Словарь русского языка : 70 000 слов / С. И. Ожегов ; под ред. Н. Ю. Шведовой ; АН СССР ; Ин-т русского яз. — М.: Рус. яз., 1989. — 924 с.
82. Новий тлумачний словник української мови : 42000 слів : у 4 т. / [уклад.: В. Я. Яременко, О. М. Сліпушко]. — К. : Аконті, 2000 — . — Т. 3 : ОБЕ — РОБ. — 2000. — 927 с. — (Серія. «Нові словники»).
83. Словник іншомовних слів / гол.ред. О. С. Мельничук. — К. : Гол. ред. УРЕ, 1977. — 746 с.
84. Большой энциклопедический словарь. — [2-е изд.]. — М. : БРЭ ; СПб. : Норинт, 1998. — 1456 с.; Словарь иностранных слов / гл. ред. Ф. Н. Петрова. — М.: Рус. яз., 1983. — 608 с.
85. Крестьянінов О. О. Адміністративно — правові режими як особливий інститут державного управління / О. О. Крестьянінов // Держава і право : зб. наук. праць. Юрид. і політ. науки / [голов. ред. колег. Ю. С. Шемшученко] ; Ін-т держ. і права ім. В. М. Корецького НАН України. — К., 2001. — Вип. 12. — 568 с.
86. Ківалов С. В. Адміністративне право України : [навч.-метод. посіб.] / С. В. Ківалов, Л. Р. Біла. — [2-е вид., перероб. і доповн.]. — Одеса : Юрид. літ., 2002. — 312 с.
87. Познышев С. В. Основы пенитенциарной науки / С. В. Познышев. — М. : Главлит, 1923. — 342 с.
88. Утевский Б. С. Советская исправительно-трудовая политика / Б. С.Утевский. — М. : Советское законодательство, 1934. — 256 с.
89. Алексеев С. С. Общие дозволения и общие запреты в советском праве / С. С. Алексеев. — М. : Юрид. лит., 1989. — 288 с.
90. Матузов Н. И. Правовые режимы: вопросы теории и практики / Н. И. Матузов, А. В. МАлько // Изв. вузов. Правоведение. — 1996. — №1. — С. 16–29.
91. Шамсумова Э. Ф. Правовые режимы (теоретический аспект): дисс. ... канд. юрид. наук : 12.00.01 / Эмма Файсаловна Шамсумова. — Екатеринбург, 2001. — 213 с.
92. Корельский В. М. Теория государства и права : [учеб. для вузов] / под ред. В. М. Корельского, В. Д. Перевалова. — М. : Инфра — М, 1997. — 570 с.
93. Загальна теорія держави і права : [підруч.] / за ред. М. В. Цвіка, В. Д. Ткаченка, О. В. Петришина. — Х. : Право, 2002. — 432 с.
94. Исаков В. Б. Правовые режимы и их совершенствование / В. Б. Исаков // XXVI съезд КПСС и развитие теории права : межвуз. сб. науч. трудов. —Свердловск, 1982. — С. 34–39.
95. Бахрах Д. Н. Административное право России : [учеб. для вузов] / Д. Н. Бахрах. — М. : Норма, 2002. — 444 с.
96. Бахрах Д. Н.Административное право : [учеб. для вузов] / Д. Н. Бахрах, Б. В. Россинский, Ю. Н. Стариков. — [3-е изд., пересмотр. и доп]. — М. : Норма, 2007. — 816 с.

97. Розанов И. С. Административно-правовые режимы по законодательству РФ, их назначение и структура / И. С. Розанов // Государство и право. — 1996. — № 9. — С. 84–91.
98. Рушайло В. Б. Административно-правовые режимы : [монография]. / В. Б. Рушайло. — М. : Щит — М, 2000. — 264 с.
99. Административное право Украины : [учеб.] / под ред. проф. Ю. П. Битяка. — [2-е изд., перераб. и доп.]. — Х. : Право, 2003. — 576 с.
100. Административное право : [учеб.] / под ред. Ю. М. Козлова, Л. Л. Попова. — М. : Юрист, 2000. — 728 с.
101. Ковальова М. В. Адміністративно-правові режими підприємницької діяльності в Україні : дис. ... канд. юрид. наук : 12.00.07 / Марина Вікторівна Ковальова. — Х., 2007. — 197 с.
102. Тихомиров Ю. А. Административное право и процесс : полный курс / Ю. А. Тихомиров. — М. : Тихомирова М. Ю., 2001. — 652 с.
103. Крестьянинов А. А. Место таможенных режимов в системе административно-правовых режимов / А. А. Крестьянинов // Проблемы законности: [респ. міжвідом. наук. зб. / відп. ред. В. Я. Тацій]. — Х., 1999. — Вип. 37. — С. 90–96.
104. Адміністративне право України. Академічний курс : [підруч.] : у 2 т. : Т. 1 : Загальна частина / [ред. колегія : В. Б. Авер'янов (голова)]. — К. : Юридична думка, 2005. — 624 с.
105. Магда С. О. Забезпечення прав, свобод та реалізації обов'язків громадян в умовах надзвичайних адміністративно-правових режимів : дис. ... канд. юрид. наук : 12.00.07 / Світлана Олександрівна Магда. — Х, 2008. — 224 с.
106. Нелюбин С. Я. Режим лицензирования в Российской Федерации : административно-правовой аспект : дисс. ... канд. юрид. наук : 12.00.14 / Сергей Яковлевич Нелюбин. — М., 2004. — 183 с.
107. Ефремов А.А. Информация как объект интеллектуальной собственности [Электронный ресурс] / А. А. Ефремов. — Режим доступа : <http://www/info.law.hut.ru/works/>.
108. Савельев Д.А. Информация и интеллектуальная собственность как объекты гражданского права [Электронный ресурс] / Д. А. Савельев. — Режим доступа : <http://www.law.agava.ru/inf-pravo/works/>.
109. Тихомиров Ю. А. Курс административного права и процесса : [учеб.] / Ю. А. Тихомиров. — М. : Юрид. лит., 1998. — 798 с.
110. Бахрах Д. Н. Административное право России : [учеб. для студ. вузов, обуч. по спец. «Юриспруденция»] / Д. Н. Бахрах. — М. : НОРМА: ИНФРА, 2000. — 624 с.
111. Білоконь М. В. Надзвичайні адміністративно-правові режими як правове забезпечення охорони громадського порядку в надзвичайних ситуаціях / М. В. Білоконь // Право і безпека. — Х., 2004. — Т. 3, № 3. — С. 41–44.
112. Дерев'янку П. В. Вдосконалення правового забезпечення надзвичайних режимів / П. В. Дерев'янку // Науковий вісник Нац. акад. внутр. справ України. — К., 2005. — № 5. — С. 70–77.

113. Ківалов С. В. Спеціальні адміністративні режими: сутність та правове регулювання / С. В. Ківалов // Наукові праці Одеської нац. юрид. акад. / голов. ред. С. В. Ківалов ; Одеська нац. юрид. акад. — Одеса, 2002. — Т. 1. — С. 159–169.
114. Кузніченко С. О. Проблеми класифікації надзвичайних ситуацій / С. О. Кузніченко // Вісник Нац. ун-ту внутр. справ. — Х., 2002. — № 18. — С. 247–252.
115. Маилян С. С. О классификации административно-правовых режимов / С. С. Маилян // Современное право. — 2002. — № 10. — С. 24–27.
116. Оборотов Ю. М. Правові режими : поняття і види / Ю. М. Оборотов // Вісник Одеського ін-ту внутр. справ. — Одеса, 2004. — № 3. — Ч. 2. — С. 39–42.
117. Бахрах Д. Н. Административное право : [учеб.] / Д. Н. Бахрах. — М. : БЕК, 1996. — 368 с.
118. Бляхман Б. Я. Правовой режим в системе регулирования социальных отношений : [науч. изд.] / Б. Я. Бляхман. — Кемерово, 1999. — С.7–47.
119. Корнев А. П. Принципы современного административного права / А. П. Корнев // Изв. вузов. Правоведение. — 1967. — № 3. — С. 72–78.
120. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления [Электронный ресурс]. — Режим доступа : // <http://www.rg.ru/2009/02/13/dostup-dok.html>.
121. Білоскурська О. В. Про єдність прав і обов'язків людини і громадянина / О. В. Білоскурська // Держава і право : зб. наук. праць. Юрид. і політ. науки / [голов. редкол. Ю. С. Шемшученко]. — К., 2002. — Вип. 16. — С. 120–123.
122. Колпаков В. К. Адміністративне право України : [підруч.] / В. К. Колпаков О. В. Кузьменко. — К. : Юрінком Інтер, 2003. — 544 с.
123. Стеценко С. Г. Адміністративне право України : [навч. посіб.] / С. Г. Стеценко. — К. : Атака, 2008. — 624 с.
124. Про участь громадян в охороні громадського порядку і державного кордону : Закон України від 22 черв. 2000 р. // Відомості Верховної Ради України. — 2000. — № 40. — Ст. 338.
125. Про комітети Верховної Ради України : Закон України від 4 квіт. 1995 р. // Відомості Верховної Ради України. — 1995. — № 19. — Ст. 134.
126. Конституція України : прийнята 28 черв. 1996 р. // Відомості Верховної Ради України. — 1996. — № 30. — Ст. 141.
127. Ліпкан В. А. Адміністративно-правове регулювання національної безпеки України : [монографія] / В. А. Ліпкан. — К. : Текст, 2008. — 440 с.
128. Про Раду національної безпеки і оборони України : Закону України від 5 берез. 1998 р. // Відомості Верховної Ради України. — 1998. — № 35. — Ст. 237.
129. Про Кабінет Міністрів України : Закон України від 7 жовт. 2010 р. // Відомості Верховної Ради України. — 2011. — № 9. — Ст. 58.
130. Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис. ... канд. юрид. наук : 12.00.07 / Олександр Володимирович Логінов. — К., 2005. — 237 с.
131. Виконавча влада і адміністративне право / за заг. ред. В. Б. Аверьянова. — К. : Ін-Юре, 2002. — 668 с.

132. Державне управління : теорія і практика / за заг. ред. В. Б.Аверьянова. — К. : Юрінком Інтер, 1998. — 432 с.
133. Про оптимізацію системи центральних органів виконавчої влади : указ Президента України від 9 груд. 2010 р.// Офіційний Вісник України. — 2010. — № 94. — Ст. 3334.
134. Про створення Державного департаменту інтелектуальної власності : постанов. Кабінету Міністрів України від 4 квіт. 2000 р. // Офіційний Вісник України. — 2000. — № 14. — Ст. 568
135. Про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : Указ Президента України // Офіційний Вісник України. — 2011. — № 52. — Ст. 2068.
136. Про додержання прав людини під час проведення оперативно-технічних заходів : указ Президента України від 07 лист. 2005 р. // Офіційний Вісник України. — 2005. — № 45. — Ст. 2834.
137. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лют. 2006 р. // Офіційний вісник України. — 2006. — № 13. — Ст. 856.
138. Про державні секрети [Електронний ресурс] : проект Закону України. — Режим доступу : <http://www.sbu.gov.ua>.
139. Про захист персональних даних : Закон України від 1 черв. 2010 р. // Відомості Верховної Ради України . — 2010. — № 34. — Ст. 481.
140. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних : Закон України від 6 лип. 2010 р. // Відомості Верховної Ради України. — 2010. — № 46. — Ст. 542.
141. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» [Електронний ресурс] : Закон України набирає чинності з 1 січ. 2012 р. — Режим доступу : <http://www.zpd.gov.ua/R/indexResources.html>.
142. Про Положення про Державну службу України з питань захисту персональних даних : указ Президента України від 6 квіт. 2011 р. // Офіційний вісник України. — 2011. — № 28. — Ст. 1160.
143. Про затвердження Положення про Державну архівну службу України : указ Президента України від 6 квіт. 2011 р. // Офіційний вісник України. — 2011. — № 28. — Ст. 1164.
144. Про затвердження Положення про Державну службу інтелектуальної власності України : указ Президента України від 8 квіт. 2011 р. // Офіційний вісник України. — 2011. — № 29. — Ст. 1244.
145. Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України : дис. ... канд. юрид. наук : 12.00.07 / Олег Вікторович Олійник. — К., 2006. — 199 с.

146. Мастяниця Й. У. Інформаційні ресурси України : проблеми державного управління : [монографія] / Й. У. Мастяниця, О. В. Соснін, Л. Є. Шиманський. — К. : НІСД, 2002. — 141 с.
147. Мірошник Ю. П. Організаційно-правові засади охорони державної таємниці в Україні / Ю. П. Мірошник // Науковий вісник НАВСУ. — К., 2004. — Вип. 4. — С. 51–57.
148. О государственной тайне : Закон Азербайджана [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/az/secret.htm>.
149. О государственной и служебной тайне : Закон Армении [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/am/secret.htm>.
150. О государственных секретах : Закон Белоруссии [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/by/secret.htm>.
151. О государственной тайне : Закон Грузии [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/ge/secret.htm>.
152. О государственных секретах : Закон Казахстана [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/ge/secret.htm>.
153. О защите государственных секретов Киргизской Республики : Закон Киргизии [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/ge/secret.htm>.
154. О государственной тайне : Закон Латвии [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/ge/secret.htm>.
155. О государственной и служебной тайне : Закон Литвы [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/ge/secret.htm>.
156. О государственной тайне : Закон Молдавии [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/ge/secret.htm>.
157. О государственной тайне : Закон Таджикистана [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/ge/secret.htm>.
158. О защите государственных секретов : Закон Туркмении [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/ge/secret.htm>.
159. О защите государственных секретов : Закон Узбекистана [Электронный ресурс]. — Режим доступа : <http://www.medialaw.ru/exussrlaw/l/ge/secret.htm>.
160. Потеря секретов в Казахстане ... и на гавайском пляже // Независимое военное обозрение. — 2002. — № 24. — С. 7.
161. В ФБР подворовывают // Независимое военное обозрение. — 2001. — № 36. — С. 7.
162. Шаров Б. Без грифу таємно / Б. Шаров // Юридичний вісник України. — 2002. — № 12. — С. 4.
163. Благодарний А. М. Адміністративна відповідальність за порушення законодавства про державну таємницю : дис. ... канд. юрид. наук : 12.00.07 / Андрій Миколайович Благодарний. — К., 2006. — 200 с.
164. Северин Л. І. Правове забезпечення захисту інформації : [навч. посіб.] / Л. І. Северин, С. Л. Северин, А. В. Дудатьєв. — Вінниця : ВНТУ, 2004. — 145 с.

165. Про внесення змін до Закону України «Про державну таємницю» : Закон України від 21 верес. 1999 р. // Відомості Верховної Ради України. — 1999. — № 49. — Ст. 428.
166. Про внесення зміни до статті 9 Закону України «Про державну таємницю» : Закон України від 19 черв. 2003 р. // Відомості Верховної Ради України. — 2003. — № 45. — Ст. 361.
167. Про внесення змін та визнання такими, що втратили чинність, деяких законів та інших актів Верховної Ради України у зв'язку з прийняттям Закону України «Про статус народного депутата України» : Закон України від 19 лют. 2004 р. // Відомості Верховної Ради України. — 2004. — № 23. — Ст. 320.
168. Про внесення змін до Закону України «Про державну таємницю» : Закон України від 21 трав. 2008 р. // Відомості Верховної Ради України. — 2008. — № 27–28. — Ст. 252.
169. Про внесення змін до Закону України «Про державну таємницю» : Закон України від 6 лип. 2010 р. // Відомості Верховної Ради України. — 2010. — № 46. — Ст. 537.
170. Про внесення змін до деяких законодавчих актів України щодо приведення їх у відповідність із Конституцією України : Закон України від 7 жовт. 2010 р. // Відомості Верховної Ради України. — 2011. — № 10. — Ст. 63.
171. Про внесення змін до деяких законодавчих актів України щодо врегулювання трудових відносин у разі відмови у наданні допуску до державної таємниці : Закон України від 3 лют. 2011 р. // Відомості Верховної Ради України. — 2011. — № 33. — Ст. 329.
172. Про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці : постан. Кабінету Міністрів України від 19 берез. 2008 р. // Офіційний вісник України. — 2008. — № 58. — Ст. 1957.
173. Питання Державного комітету з питань державних секретів : постан. Кабінету Міністрів України від 4 серп. 2010 р. // Офіційний вісник України. — 2010. — № 66. — Ст. 2381.
174. Про затвердження Переліку психічних захворювань (розладів), які можуть завдати шкоди охороні державної таємниці і за наявності яких допуск до державної таємниці громадянину не надається : наказ МОЗ України від 13 трав. 2002 р. № 174/136 // Офіційний вісник України. — 2002. — № 22. — Ст. 1085.
175. Ответственность за государственные преступления. Часть вторая: Иные государственные преступления / [Богатиков Д. И., Бушуев И. А., Иванов Н. М. и др.] ; общ. ред. В. И. Курляндского, М. П. Карпушина. — М. : Юрид. лит., 1965. — 292 с.
176. Україна у WikiLeaks : політика без грифу. — К. : Фенікс, 2011. — 192 с.
177. Уголовное право УССР. Особенная часть : [учеб.] / под ред. М. И. Бажанова, П. С. Матышевского, В. В. Сташиса. — К. : Вища школа, 1989. — 503 с.
178. Про Службу безпеки України : Закон України від 25 берез. 1992 р. // Відомості Верховної Ради України. — 1992. — № 27. — Ст. 382.



179. Про затвердження Зводу відомостей, що становлять державну таємницю України : наказ Голови Служби безпеки України від 12 серп. 2005 р. // Офіційний вісник України. — 2005. — № 34. — Ст. 2089.
180. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 24 січ. 2006 р. // Офіційний вісник України. — 2006. — № 6. — Ст. 324.
181. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 25 квіт. 2006 р. // Офіційний вісник України. — 2006. — № 19. — Ст. 1400.
182. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 12 жовт. 2006 р. // Офіційний вісник України. — 2006. — № 44. — Ст. 2970.
183. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 26 лют. 2007 р. // Офіційний вісник України. — 2007. — № 17. — Ст. 670.
184. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 28 груд. 2007 р. № 949 // Офіційний вісник України. — 2008. — № 5. — Ст. 129.
185. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 17 черв. 2008 р. // Офіційний вісник України. — 2008. — № 52. — Ст. 1757.
186. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 27 лист. 2008 р. // Офіційний вісник України. — 2008. — № 92. — Ст. 3061.
187. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : Наказ Служби безпеки України від 16 берез. 2009 р. № 146 // Офіційний вісник України. — 2009. — № 29. — Ст. 981.
188. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 25 лист. 2009 р. // Офіційний вісник України. — 2009. — № 99. — Ст. 3443.
189. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 24 лют. 2010 р. // Офіційний вісник України. — 2010. — № 17. — Ст. 795.
190. Про внесення змін та доповнень до Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 23. лип. 2010 р. // Офіційний вісник України. — 2010. — № 62. — Ст. 2172.
191. Приказ отправляют в отставку // Независимое военное обозрение. — 2004. — № 8. — С. 7.
192. Мірошник Ю. Державна таємниця як складова забезпечення національної безпеки України / Ю. Мірошник // Право України. — 2004. — № 9. — С. 32–34.
193. Постанова судді Жовтневого районного суду м. Харкова Савченка І. Б. від 14 лист. 2001 р.
194. Про внесення змін до Кодексу України про адміністративні правопорушення щодо встановлення відповідальності за порушення законодавства про дер-

- жавну таємницю : Закон України від 21 верес. 1999 р. // Відомості Верховної Ради України. — 1999. — № 49. — Ст. 429.
195. Про внесення змін до деяких законодавчих актів України: Закон України від 11 трав. 2004 р. // Відомості Верховної Ради України. — 2004. — № 32. — Ст. 394.
196. Про внесення змін до деяких законодавчих актів України щодо діяльності Державної служби спеціального зв'язку та захисту інформації України : Закон України від 19 берез. 2009 р. // Відомості Верховної Ради України. — 2009. — № 32–33. — Ст. 485.
197. Кодекс про адміністративні правопорушення : Закон України від 7 груд. 1984 р. // Відомості Верховної Ради Української РСР. — 1984. — додаток до № 50. — Ст. 1122.
198. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, від 28 січ. 1981 р. // Офіційний вісник України. — 2011. — № 1. — Ст. 85.
199. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних, від 8 лист. 2001 р. // Офіційний вісник України. — 2011. — № 1. — Ст. 86.
200. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 лип. 1994 р. // Відомості Верховної Ради України. — 1994. — № 31. — Ст. 286.
201. Про державну службу : Закон України від 16 груд. 1993 р. // Відомості Верховної Ради України. — 1993. — № 52. — Ст. 490.
202. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16 лист. 1992 р. // Відомості Верховної Ради України. — 1993. — № 1. — Ст. 1.
203. Про професійних творчих працівників та творчі спілки : Закон України від 7 жовт. 1997 р. // Відомості Верховної Ради України. — 1997. — № 52. — Ст. 312.
204. Про культуру : Закон України від 14 груд. 2010 р. // Відомості Верховної Ради України. — 2011. — № 24. — Ст. 168.
205. Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення : постан. Кабінету Міністрів України від 25 трав 2011 р. // Офіційний вісник України. — 2011. — № 45. — Ст. 1833.
206. Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних [Електронний ресурс] : Директива 95/46/ЄС Європейського парламенту та Ради Європейського Союзу від 24 жовт. 1995 р. — Режим доступу : <http://www.evropa.eu.int/ISPO/legal/en/dataprot/directiv/directiv.html>.
207. Висновок Головного юридичного управління щодо законопроекту «Про захист персональних даних» [Електронний ресурс]. — Режим доступу : <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi>.
208. У справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г.Устименка) [Електронний ресурс] : рішення Конституційного Суду України

від 30 жовт. 1997 р. — Режим доступу : <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi>.

209. Про захист персональних даних : Закон України від. 1 лип. 2010 р. // Відомості Верховної Ради України. — 2010. — № 34. — Ст. 481.
210. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. // Відомості Верховної Ради України. — 2003. — № 36. — Ст. 275.

# КОРИСНА БІБЛІОГРАФІЯ ЗА ТЕМОЮ ДОСЛІДЖЕННЯ

## Праці наукової школи Ліпкана В. А. з інформаційної тематики

1. Ліпкан В. А. Інформаційна безпека України : [Глосарій] / В. А. Ліпкан, Л. С. Харченко, О. В. Логінов. — К.: Текст, 2004. — 136 с.
2. Ліпкан В. А. Правові та організаційні засади взаємодії суб'єктів протидії торгівлі людьми [монографія] / В. А. Ліпкан, О. В. Кушнір ; за заг. ред. В. А. Ліпкана. — К. : О. С. Ліпкан, 2013. — 376 с.
3. Ліпкан В. А. Систематизація інформаційного законодавства України : [монографія] / В. А. Ліпкан, В. А. Залізняк ; за заг. ред. В. А. Ліпкана. — К. : О. С. Ліпкан, 2012. — 304 с.
4. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: [Навчальний посібник] / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. — К.: КНТ, 2006. — 280 с.
5. Шепета О. В. Адміністративно-правові засади технічного захисту інформації : [монографія] / О. В. Шепета. — К. : О. С. Ліпкан, 2012. — 296 с.
6. Баскаков В. Адміністративно-правовий режим захисту інформації з обмеженим доступом: окремі аспекти / В. Баскаков // Інформаційні технології в глобальному управлінні : матеріали наук.-практ. конференції (Київ, 29 жовтня 2011 р.). — К. : ФОП Ліпкан О.С., 2011. — С. 47–51.
7. Баскаков В. Захист інформації з обмеженим доступом в умовах боротьби з організованою злочинністю / В. Баскаков, В. Ліпкан // Боротьба з організованою злочинністю і корупцією (теорія і практика). — 2011. — № 24. — С. 263–269. (здобувачу належить визначення інформації з обмеженим доступом)
8. Баскаков В. Захист інформації з обмеженим доступом: окремі аспекти / В. Баскаков // Актуальні проблеми правоохоронної діяльності : матеріали наук.-практ. конференції (Київ, 20 грудня 2010 р.). — К. : ФОП Ліпкан О.С., 2010. — С. 59–61.
9. Баскаков В. Захист інформації з обмеженим доступом: розвиток вітчизняного законодавства / В. Баскаков // Підприємництво, господарство і право. — 2011. — № 4. — С. 126–128.
10. Баскаков В. Інформація з обмеженим доступом: аналіз термінологічно-понятійного апарату / В. Баскаков // Підприємництво, господарство і право. — 2011. — № 5. — С. 124–127.

11. Баскаков В. Інформація з обмеженим доступом: поняття та ознаки / В. Баскаков // Актуальні проблеми державотворення : матеріали науково-практичної конференції (Київ, 28 червня 2011 р.). — К. : ФОП Ліпкан О.С., 2011. — С. 47–49.
12. Баскаков В. Тенденції адміністративної відповідальності у сфері інформаційної безпеки / В. Баскаков, О. Стоєцький // Актуальні проблеми правоохоронної діяльності : матеріали наук.-практ. конференції (Київ, 20 грудня 2010 р.). — К. : ФОП Ліпкан О.С., 2010. — С. 64–66. (здобувачу належать інформаційно-правові дефініції понять, висвітлених в публікації).
13. Баскаков В. Ю. Захист інформації з обмеженим доступом у контексті міжнародної інформаційної безпеки : аналіз термінологічно-понятійного апарату / В. Ю. Баскаков // Національна і міжнародна безпека в сучасних трансформаційних процесах : матеріали наук.-практ. конференції (Київ, 29 грудня, 2011 р.). — К. : ФОП Ліпкан О.С., 2011. — С. 55–59.
14. Баскаков В. Ю. Поняття та зміст інформації з обмеженим доступом / В. Ю. Баскаков // Правова інформатика. — 2012. — № 33(1). — С. 7–14.
15. Дімчогло М. І. Завдання інформатизації в контексті розвитку інформаційного суспільства в Україні / М. І. Дімчогло // Інформаційні стратегії в глобальному управлінні : матеріали наук.-практ. конференції. — К., 2011. — С. 36–37.
16. Дімчогло М. І. Консолідація інформаційного законодавства у сучасних правових системах (на прикладі законодавства окремих країн) / М. І. Дімчогло // Правові та політичні проблеми сучасності. — К., 2012. — С. 23–27.
17. Дімчогло М. І. Консолідація інформаційного законодавства України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / М. І. Дімчогло ; Нац. авіаційний ун-т. — К., 2012. — 18 с.
18. Дімчогло М. І. Консолідація інформаційного законодавства як напрям боротьби з тероризмом / М. І. Дімчогло // Інформаційні технології боротьби з тероризмом : матеріали наук.-практ. конференції. — К., 2012. — С. 22–24.
19. Дімчогло М. І. Консолідація як вид систематизації інформаційного законодавства / М. І. Дімчогло // Правова інформатика. — 2012. — № 1 (33). — С. 15–24.
20. Дімчогло М. І. Окремі принципи інформаційних правовідносин / М. І. Дімчогло // Національна і міжнародна безпека в сучасних трансформаційних процесах : матеріали наук.-практ. конференції. — К., 2011. — С. 59–61.
21. Дімчогло М. І. Консолідація конституційних положень щодо інформаційних правовідносин у законодавстві / М. І. Дімчогло // Підприємництво, господарство і право. — 2012. — № 6. — С. 39–42.
22. Дімчогло М. І. Основи теорії консолідації інформаційного законодавства / М. І. Дімчогло // Підприємництво, господарство і право. — 2012. — № 5. — С. 41–46.
23. Залізник В. А. Інформаційна безпека як інститут інформаційного права України / В. А. Залізник // Актуальні проблеми зміцнення державності і національної єдності України : матеріали наук.-практ. конференції. — К., 2010. — С. 46–48.
24. Залізник В. А. Міжнародно-правове регулювання права на інформацію / В. А. Залізник // Підприємництво, господарство і право. — 2010. — № 8. — С. 69–72.

25. Залізник В. А. Особливості систематизації інформаційного законодавства України / В. А. Залізник // Імперативи розвитку юридичної та безпекової науки : матеріали наук.-практ. конф., (Київ, 15 квіт. 2010 р.). — К., 2010. — С. 48–50.
26. Залізник В. А. Правова свідомість в умовах становлення інформаційного суспільства в Україні / В. А. Залізник // Розвиток правової свідомості сучасного суспільства : матеріали міжнар. наук.-практ. інтернет-конференції. — Тернопіль, 2009. — С. 73–75.
27. Залізник В. А. Систематизація інформаційного законодавства / В. А. Залізник // Підприємництво, господарство і право. — 2010. — № 9. — С. 140–143.
28. Залізник В. А. Систематизація інформаційного законодавства України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / В. А. Залізник ; Нац. ун-т біоресурсів і природокористування України. — К., 2011. — 18 с.
29. Залізник В. А. Системний підхід при дослідженні систематизації інформаційного законодавства України / В. А. Залізник // Філософські, методологічні і психологічні проблеми права : тези доп. III Всеукр. наук.-теорет. конф., (Київ, 23 квіт. 2010 р.) / [ред. кол. : В. В. Коваленко, М. В. Костицький, О. М. Джужа та ін.]. — К., 2010. — С. 56–57.
30. Залізник В. А. Удосконалення інформаційного законодавства України : методологічні засади / В. А. Залізник // Підприємництво, господарство і право. — 2010. — № 2. — С. 59–61.
31. Залізник В. А. Удосконалення інформаційного законодавства: стан та перспективи / В. А. Залізник // Національні проблеми юридичної науки. — Хмельницький, 2009. — Вип. 4. — С. 63–64.
32. Ліпкан В. А., Максименко Ю .Є. Удосконалення нормативно-правових засад боротьби з кіберзлочинністю як необхідна умова євроінтеграції // Проблеми європейської інтеграції і транскордонного співробітництва: Матеріали II Міжнародної науково-практичної конференції, м. Луцьк, 29–30 вересня 2005 р. / За ред. В.Й. Лажніка і С.В. Федонюка. —Луцьк: РВВ «Вежа» Волин. держ. ун-ту ім. Лесі Українки, 2005. — 542 с. — С. 192–197.
33. Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / О. В. Логінов ; Нац. акад. внутр. справ України. — К., 2005. — 20 с.
34. Логінов О. В. Деякі аспекти інформаційного забезпечення діяльності Уряду України / О. В. Логінов // Сучасні проблеми управління : зб. матеріалів II Міжнар. наук.-практ. конф. / [уклад. Б. В. Новиков, І. І. Федорова та ін.]. — К., 2003. — Ч. 1. — С. 127–130.
35. Логінов О. В. Гносеологічний аспект управління інформаційною безпекою України / О. В. Логінов // Науковий вісник Юридичної академії МВС України. — Дніпропетровськ, 2004. — № 2. — С. 153–161.
36. Логінов О. В. Інформаційна безпека: потребнісний та гносеологічний підходи / О. В. Логінов // Забезпечення прав людини та громадянина в умовах рефор-

- мування політичної та правової системи України : тези доп. наук.-практ. конференції / НАВС. — К., 2004. — С. 253–256.
37. Логінов О. В. Класифікація загроз та небезпек інформаційній безпеці системи органів державного управління України / О. В. Логінов // Міліція України : наук.-практ. зб. — 2004. — № 8. — С. 12–16.
  38. Логінов О. В. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління / О. В. Логінов // Науковий вісник Юридичної академії МВС України. — Дніпропетровськ, 2003. — № 3. — С. 199–205.
  39. Максименко Ю .Є. Міжнародно-правові та європейські засади забезпечення безпеки інформаційного суспільства // Актуальні проблеми забезпечення національної безпеки України / Матеріали науково-практичної конференції (м. Київ, 6 грудня 2005 р.) / Київський націон. ун-т внутр. справ. — К.: Текст, 2005. — 206 с. — С. 58–66.
  40. Максименко Ю. Є. Актуальні проблеми боротьби з інформаційним тероризмом // Науково-практичний збірник. Актуальні проблеми юридичних наук у дослідженнях учених. — 2004. — № 31. — С. 10–12.
  41. Максименко Ю. Є. Вхідження до глобального інформаційного простору: проблеми та перспективи // Європейські інтеграційні процеси і транскордонне співробітництво: міжнародні відносини, економіка, політика, географія, історія, право: Тези доповідей II Міжнародної науково-практичної конференції студентів, аспірантів і молодих науковців, м. Луцьк, 19–20 травня 2005 р. / За ред. В.Й. Лажніка і В.С. Федонюка. — Луцьк: РВВ «Вежа» Волин. держ. ун-ту ім. Лесі Українки, 2005. — 510 с. — С. 161–163.
  42. Максименко Ю. Є. Деякі аспекти визначення поняття національної безпеки // Науковий вісник Юридичної академії МВС. — 2004. — № 3. — С. 77–81.
  43. Максименко Ю. Є. Діяльність Київського національного університету внутрішніх справ у сфері підготовки фахівців із інформаційної безпеки України // Проблеми національної і міжнародної безпеки / Матеріали науково-практичної конференції (Київ, 27 квітня 2007 р.) / Київський нац. університет внутр. справ. — К.: Текст, Щорічник, — № 2. — 2007. — 146 с. — С. 138–145.
  44. Максименко Ю. Є. Європейські засади забезпечення безпеки інформаційного суспільства // Європейські інтеграційні процеси і транскордонне співробітництво: Матеріали III Міжнародної науково-практичної конференції, м. Луцьк, 18–19 травня 2006 р. у 2-х томах (уклад. В.Й. Лажніка, С.В. Федонюка). — Луцьк: РВВ «Вежа» Волин. держ. ун-ту ім. Лесі Українки, 2006.– 468 с. — С. 108–110.
  45. Максименко Ю. Є. Нормативно-правове регулювання інформаційної безпеки України в умовах євроінтеграції // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. Збірник наукових праць / Головний редактор В.Л. Ординський. — Львів, 2006. — Вип. 3. — С. 176–183.
  46. Максименко Ю. Є. Побудова інформаційного суспільства в Україні в контексті інтеграції до Європейського Союзу // Матеріали I Міжнародної науково-практичної конференції. — Харків: ХНУ імені В.Н. Каразіна, 2006. — 487 с. — С. 71–73.



47. Максименко Ю. Є. Проблеми правового забезпечення інформаційної безпеки України // *Держава і право: Збірник наукових праць. Юридичні і політичні науки. Спецвипуск.* — К.: Ін-т держави і права ім. В. Корецького НАН України, 2005. — С. 131–134.
48. Максименко Ю. Є. Роль Національної академії внутрішніх справ України в підготовці кадрів по забезпеченню національної безпеки України в інформаційній сфері // *Вісник Луганської академії внутрішніх справ МВС імені 10-річчя незалежності України.* — 2004. — № 3. — С. 84–90.
49. Максименко Ю. Є. Стан нормативно-правового регулювання інформаційної безпеки України в умовах євроінтеграції // *Вісник Харківського національного університету внутрішніх справ.* — 2006. — № 34. — С. 38–45.
50. Максименко Ю. Є. Сучасні проблеми криміналізації інформаційної сфери // *Актуальні проблеми політики: Зб. наук. праць.* / Голов.ред. С.В. Ківалов; відп. за вип. Л.І. Кормич. — Одеса: ПП «Фенікс». — 2005. — Вип.26. — С. 294–299.
51. Максименко Ю. Є. Удосконалення нормативно-правових засад забезпечення безпеки в мережі INTERNET // *Матеріали науково-практичної конференції.* м. Харків, 11–12 квітня 2006 р.: Вид-во Харківського національного ун-ту внутр. справ, 2006. — 274 с. — С. 241–243.
52. Максименко Ю.Є. Визначення поняття інформаційної безпеки з позицій діяльнісного підходу // *Науково-практичний збірник. Актуальні проблеми юридичних наук у дослідженнях учених.* — 2004. — № 32. — С. 16–19.
53. Матвієнко П. Є. Аналіз сучасного етапу розвитку законодавства про комерційну таємницю в Україні / П. Є. Матвієнко // *Підприємництво, господарство і право.* — 2009. — № 12. — С.85–88.
54. Матвієнко П. Є. Доцільність боротьби засобами адміністративного примусу з посяганнями на встановлений порядок обігу інформації, що становить комерційну таємницю / П. Є. Матвієнко // *Держава і право.* — 2009. — № 46. — С.273–276.
55. Матвієнко П. Є. Місце та роль адміністративної відповідальності у системі заходів охорони прав на комерційну таємницю / П. Є. Матвієнко // *Актуальні проблеми юридичної науки: Збірник тез міжнародної наукової конференції «Восьмі осінні юридичні читання» (м. Хмельницький, 13–14 листопада 2009 року) : У 4-х частинах.* — Частина друга: «Конституційне право. Адміністративне право. Фінансове право. Інформаційне право. Земельне право. Аграрне право. Екологічне право. Природоресурсне право. Трудове право і право соціального забезпечення». — Хмельницький: Вид-во Хмельницького університету управління та права, 2009. — С. 115–116.
56. Матвієнко П. Є. Організаційно-правові механізми захисту інформації, яка становить комерційну таємницю / П. Є. Матвієнко // *Юриспруденція : теорія і практика.* — 2009. — № 12. — С.41–45.
57. Матвієнко П. Є. Основні напрями удосконалення системи захисту інформації, яка становить комерційну таємницю для суб'єкта господарювання / П. Є. Матвієнко // *Новітні підходи до державотворення в умовах європейської інтеграції*

- (пам'яті професора Ю. І. Римаренка) : Збірник тез міжвузівської науково-теоретичної конференції. — К. : КНУВС, 2009 — С. 99–102.
- 58.** Матвієнко П. Є. Технічний захист інформації у процесі підготовки кадрів для органів внутрішніх справ / П. Є. Матвієнко // Наука і вища освіта : тези доповідей учасників XVII Міжнар. наук. конф. студентів і молодих науковців, м. Запоріжжя, 9–10 квітня, 2009 р. : у 4 т. / Класичний приватний університет. — Запоріжжя : КПУ, 2009. — Т. 4. — С. 3–4.
- 59.** Матвієнко П. Є. Формування переліку інформації суб'єкта господарювання, яка становить комерційну таємницю / П. Є. Матвієнко // Адвокат. — 2009. — № 5. — С.36–38.
- 60.** Стоєцький О. В. Адміністративна відповідальність за порушення у сфері інформаційної безпеки України : автореф. дис. на здобуття наук ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право»/ О. В. Стоєцький ; Запорізький. нац. ун-т. — Запоріжжя, 2013. — 19 с.
- 61.** Стоєцький О. В. Основні недоліки адміністративно-правового регулювання інформаційної безпеки України / О. В. Стоєцький // Новітні підходи до державотворення в умовах європейської інтеграції (пам'яті професора Ю. І. Римаренка) : зб. тез міжвуз. наук.-теорет. конференції. — К., 2009. — 204 с.
- 62.** Стоєцький О. В. Характеристика адміністративного правопорушення за порушення законодавства про державну таємницю / О. В. Стоєцький // Національна і міжнародна безпека в сучасних трансформаційних процесах : матеріали науково-практичної конференції, (м. Київ, 29 грудня 2011 р.). — К. : ФОП Ліпкан О. С., 2011. — С. 94–96.
- 63.** Стоєцький О. Тенденції адміністративної відповідальності у сфері інформаційної безпеки / В. Баскаков, О. Стоєцький // Актуальні проблеми правоохоронної діяльності : матеріали науково-практичної конференції, (м. Київ, 20 грудня 2010 р.). — К. : ФОП Ліпкан О. С., 2010. — С. 64–66.
- 64.** Стоєцький О. В. Адміністративно-правовий статус Президента України як суб'єкта забезпечення інформаційної безпеки / О. В. Стоєцький // Актуальні проблеми юридичної науки : зб. тез між нар. конф. [«Восьмі осінні юридичні читання»], (м. Хмельницький, 13 — 14 лист. 2009 р.) : у 4 ч. — Хмельницький, 2009. — Ч. 2 : Конституційне право. Адміністративне право. Фінансове право. Інформаційне право. Земельне право. Аграрне право. Екологічне право. Природоресурсне право. Трудове право і право соціального забезпечення. — С. 191–193.
- 65.** Стоєцький О. В. Реалізація адміністративно-правових норм у сфері забезпечення інформаційної безпеки / О. В. Стоєцький // Адвокат. — 2008. — № 12. — С. 36–39.
- 66.** Стоєцький О. В. Суб'єкти забезпечення інформаційної безпеки України: адміністративно-правові засади / О. В. Стоєцький // Підприємництво, господарство і право. — 2009. — № 11. — С. 161–164.

67. Стоєцький О. В. Характеристика інформаційної безпеки як складової інформаційної сфери / О. В. Стоєцький // Підприємництво, господарство і право. — 2009. — № 12. — С. 72–75.
68. Череповський К. П. Гносеологічні аспекти розуміння інформаційного права / К. П. Череповський // Інформаційні стратегії в глобальному управлінні : матеріали міжнар. наук.-практ. конференції. — К., 2011. — С. 96–100.
69. Череповський К. П. Елементи структуризації міжнародного інформаційного права / К. П. Череповський // Правові та політичні проблеми сучасності : матеріали наук.-практ. конференції. — К., 2012. — С. 40–44.
70. Череповський К. П. Інкорпорація інформаційного законодавства України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / К. П. Череповський ; Запоріж. нац. ун-т. — Запоріжжя, 2013. — 19 с.
71. Череповський К. П. Інкорпорація інформаційного законодавства як напрям боротьби з тероризмом / К. П. Череповський // Інформаційні технології боротьби з тероризмом : матеріали наук.-практ. конференції. — К., 2012. — С. 12–14.
72. Череповський К. П. Інкорпорація як етап до кодифікації інформаційного законодавства / К. П. Череповський // Підприємництво, господарство і право. — 2012. — № 5. — С. 47–49.
73. Череповський К. П. Інкорпорація як складова систематизації інформаційного законодавства України / К. П. Череповський // Вісник Запорізького національного університету. — Запоріжжя, 2012. — № 2, ч. II. — С. 177–182.
74. Череповський К. П. Окремі питання інкорпорації міжнародного інформаційного права / К. П. Череповський // Правова інформатика. — 2012. — № 1 (33). — С. 68–76.
75. Череповський К. П. Щодо наукової розробленості інкорпорації інформаційного законодавства / К. П. Череповський // Національна і міжнародна безпека в сучасних трансформаційних процесах : матеріали наук.-практ. конференції. — К., 2011. — С. 69–71.
76. Шепета Е. В. Основные факторы, снижающие темпы развития системы технической защиты информации Украины / Е. В. Шепета // Преимущество и новации в юридической науке : материалы конф. адъюнктов и соискателей / [отв. за вып. С. М. Андреев] ; Омск. Акад.. МВД России. — Омск, 2009. — Вып. 5. — С. 226–228.
77. Шепета О. В. Адміністративно-правові засади технічного захисту інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / О. В. Шепета ; Нац. ун-т держ. податк. Служби України. — Ірпінь, 2011. — 25 с.
78. Шепета О. В. Захист інформації в інформаційно-телекомунікаційних системах / О. В. Шепета // Новітні підходи до державотворення в умовах європейської інтеграції (пам'яті професора Ю. І. Римаренка) : зб. тез міжвуз. наук.-теор. конф. / КНУВС. — К., 2009. — С. 186–188.

- 79.** Шепета О. В. Напрями удосконалення державної політики у сфері технічного захисту інформації в Україні / О. В. Шепета // Інформаційна безпека людини, суспільства, держави. — 2010. — № 4. — С. 42–46.
- 80.** Шепета О. В. Нормативне регулювання технічного захисту інформації в Україні / О. В. Шепета // Держава і право : зб. наук. праць. Юридичні і політичні науки. — К., 2009. — № 46. — С. 283–288.
- 81.** Шепета О. В. Органи державної влади та система технічного захисту інформації України / О. В. Шепета // Підприємництво, господарство і право. — 2010. — № 2. — С. 56–58.
- 82.** Шепета О. В. Органи державної влади та система технічного захисту інформації в Україні / О. В. Шепета // Спеціальна техніка у правоохоронній діяльності : матеріали IV Міжнар. наук.-практ. конф. / КНУВС. — К., 2009. — С. 224–225.
- 83.** Шепета О. В. Організаційно-правові засади взаємодії Держспецзв'язку та Служби безпеки України з питань охорони державної таємниці та технічного захисту інформації / О. В. Шепета // Підприємництво, господарство і право. — 2010. — № 4. — С. 34–36.
- 84.** Шепета О. В. Організаційно-правові засади взаємодії Держспецзв'язку та Служби безпеки України з питань охорони державної таємниці й технічного захисту інформації / О. В. Шепета // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. (м. Київ, 17 берез. 2010 р.) / Нац. акад. СБ України. — К., 2010. — С. 128–133.
- 85.** Шепета О. В. Принципи взаємодії суб'єктів технічного захисту інформації / О. В. Шепета // Імперативи розвитку юридичної та безпекової науки : матеріали наук.-практ. конф., (м. Київ, 15 квіт. 2010 р.). — К., 2010. — С. 50–53.
- 86.** Шепета О. В. Роль та місце законів у системі нормативного регулювання технічного захисту інформації в Україні / О. В. Шепета // Актуальні проблеми юридичної науки : зб. тез міжнар. наук. конф. [«Восьмі осінні юридичні читання»], (м. Хмельницький, 13 — 14 лист. 2009 р.): у 4 ч. — Хмельницький, 2009. — Ч. 2. — С. 218–219.
- 87.** Шепета О. В. Удосконалення інформаційного законодавства України в контексті протидії екстремізму та тероризму / О. В. Шепета // Імперативи розвитку цивілізації. — 2013. — № 1. — С. 67–69.

### **Інформація з обмеженим доступом**

- 1.** Артемов В. Ю. Вдосконалення системи підготовки фахівців в сфері захисту інформації з обмеженим доступом: компетентнісний підхід / В. Ю. Артемов // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. — К., 2009. — Вип. 24. — С. 83–86.
- 2.** Артемов В. Ю. Періодизація процесів становлення й розвитку системи захисту інформації з обмеженим доступом в Україні / В. Ю. Артемов // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. — Київ, 2010. — Вип. 26. — С. 45–49.

3. Баскаков В. Захист інформації з обмеженим доступом: розвиток вітчизняного законодавства / В. Баскаков // Підприємництво, господарство і право. — 2011. — № 4. — С. 126–128.
4. Баскаков В. Інформація з обмеженим доступом: аналіз термінологічно-понятійного апарату / В. Баскаков // Підприємництво, господарство і право. — 2011. — № 5. — С. 124–127.
5. Баскаков В. Захист інформації з обмеженим доступом в умовах боротьби з організованою злочинністю / В. Баскаков, В. Ліпкан // Боротьба з організованою злочинністю і корупцією (теорія і практика). — К., 2011. — № 24. — С. 263–269.
6. Баскаков В. Ю. Поняття та зміст інформації з обмеженим доступом / В. Ю. Баскаков // Правова інформатика. — 2012. — № 33(1). — С. 7–14.
7. Баскаков В. Захист інформації з обмеженим доступом: окремі аспекти / В. Баскаков // Актуальні проблеми правоохоронної діяльності : матеріали наук.-практ. конф., (Київ, 20 груд. 2010 р.). — К., 2010. — С. 59–61.
8. Баскаков В. Тенденції адміністративної відповідальності у сфері інформаційної безпеки / В. Баскаков, О. Стоєцький // Актуальні проблеми правоохоронної діяльності : матеріали наук.-практ. конф., (Київ, 20 груд. 2010 р.). — К., 2010. — С. 64–66.
9. Баскаков В. Інформація з обмеженим доступом: поняття та ознаки / В. Баскаков // Актуальні проблеми державотворення : матеріали наук.-практ. конф., (Київ, 28 черв. 2011 р.). — К., 2011. — С. 47–49.
10. Баскаков В. Адміністративно-правовий режим захисту інформації з обмеженим доступом: окремі аспекти / В. Баскаков // Інформаційні технології в глобальному управлінні : матеріали наук.-практ. конф., (Київ, 29 жовт. 2011 р.). — К., 2011. — С. 47–51.
11. Баскаков В. Ю. Захист інформації з обмеженим доступом у контексті міжнародної інформаційної безпеки : аналіз термінологічно-понятійного апарату / В. Ю. Баскаков // Національна і міжнародна безпека в сучасних трансформаційних процесах : матеріали наук.-практ. конф., (Київ, 29 груд. 2011 р.). — К., 2011. — С. 55–59.
12. Берчак І. Інформація з обмеженим доступом у процесі діяльності засобів масової інформації / І. Берчак // Вісник Львівського університету ім. Івана Франка : зб. наук. праць / Львів. ун-т ім. Івана Франка. — Львів, 2004. — С. 9–15.
13. Беляков К. І. Інформація з обмеженим доступом: проблеми законодавчого регулювання / К. І. Беляков // Науковий вісник НАВСУ. — К., 2004. — Вип. 6. — С. 267–277.
14. Ботвінкін О. В. Інформація з обмеженим доступом, що не є державною таємницею, в законодавстві України : аналіт. огляд / О. В. Ботвінкін, В. П. Ворожко ; Нац. акад. СБ України. Ін-т захисту інформації з обмеженим доступом. — К. : НА СБУ, 2006. — 96 с.
15. Васильченко Т. В. Особливості правового режиму використання та комерціалізації ноу-хау в Україні / Т. В. Васильченко // Підприємництво, господарство і право. — 2011. — № 5. — С. 135–137.

16. Васильченко Т. В. Організаційно-правові особливості впровадження комерційної таємниці / Т. В. Васильченко // Часопис Київського університету права. — К., 2011. — № 2. — С. 141–146.
17. Васильченко Т. В. Актуальні проблеми імплементації норм міжнародного права в законодавство України щодо охорони та захисту комерційної таємниці / Т. В. Васильченко, С. Р. Шевчук // Зовнішня торгівля : економіка, фінанси, право. — 2011. — № 1. — С. 91–95.
18. Васильченко Т. В. Історична ретроспекція виникнення правової охорони комерційної таємниці в Україні / Т. В. Васильченко, С. Р. Шевчук // Зовнішня торгівля: економіка, фінанси, право. — 2011. — № 2. — С. 119–123.
19. Васильченко Т. В. Організаційно-правові особливості впровадження комерційної таємниці в умовах інноваційної економіки / Т. В. Васильченко // Правові проблеми діяльності суб'єктів господарювання в сучасних умовах : зб. матеріалів Круглого столу [«Правові проблеми діяльності суб'єктів господарювання в сучасних умовах»], (м. Київ, 27 квіт. 2001 р.). — К., 2011. — С. 158–162.
20. Васильченко Т. В. Господарсько-правове регулювання охорони комерційної таємниці в умовах інноваційної економіки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.04 «Господарське право, господарсько-процесуальне право» / Т. В. Васильченко ; МАУП. — К., 2011. — 18 с.
21. Гавдьо Ю. Банківська таємниця як окремий вид інформації з обмеженим доступом / Ю. Гавдьо // Юридичний радник : журнал юристів України. — Х., 2007. — № 4. — С. 9–13.
22. Гелич Ю.О. Інформаційні гарантії таємниці особистого життя людини : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / Ю. О. Гелич ; Націон. ун-т біоресурсів і природокористування України. — К., 2010. — 24 с.
23. Гелич Ю. О. Охорона таємниці особистого життя людини за законодавством України / Ю. О. Гелич // Проблеми правознавства та правоохоронної діяльності : зб. наук. праць. — Донецьк, 2009. — № 4. — С. 81–87.
24. Гелич Ю. О. Таємниця особистого життя людини як інститут інформаційного права України / Ю. О. Гелич // Бюлетень Міністерства юстиції України. — 2009. — № 11 (97). — С. 91–98.
25. Гелич Ю. О. Про поняття «інформаційно-правових гарантій таємниці особистого життя людини» / Ю. О. Гелич // Підприємництво, господарство і право. — 2010. — № 2 (170). — С. 27–30.
26. Гелич Ю. О. Класифікація інформаційно-правових гарантій таємниці особистого життя людини / Ю. О. Гелич // Часопис Київського університету права. — К., 2010. — № 2. — С. 156–160.
27. Гелич Ю. О. Принципи гарантування таємниці особистого життя людини в інформаційному праві України / Ю. О. Гелич // Правничий вісник Університету «Крок». — 2010. — № 5. — С. 111–118.
28. Гелич Ю. О. Публічні особи в інформаційному праві України / Ю. О. Гелич, А. І. Марущак // Інформаційна безпека людини, суспільства, держави. — 2010. — №3. — С. 31–34.

29. Гелич Ю. О. Юридична природа соціального партнерства в Україні / Ю. О. Гелич // 130 років Чернівецького університету : матеріали студент. наук. конф. — Чернівці, 2005. — С. 75–76.
30. Гелич Ю. О. Інформаційно-правова сутність таємниці особистого життя людини / Ю. О. Гелич // Актуальні питання кодифікації законодавства України / за заг. ред. В. О. Зайчука. — К., 2009. — Вип. 1. — С. 153–156.
31. Гелич Ю. О. Правова охорона таємниці особистого життя людини в Україні / Ю. О. Гелич // Права людини та механізм їх забезпечення в Україні : матеріали міжвуз. наук.-теорет. конф., (Київ, 4 груд. 2009 р.) / НАВС. — К., 2009. — Ч. 2. — С. 73–76.
32. Гелич Ю. О. До питання про місце інституту таємниці особистого життя людини у системі права України / Ю. О. Гелич // Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів. наук.-практ. конф., (17 берез. 2010 р.) / НА СБУ. — К., 2010. — С. 106–108.
33. Гелич Ю. О. Гарантії таємниці приватного життя людини у інформаційному праві України / Ю. О. Гелич // Особливості розвитку правової держави в умовах активізації євроінтеграційних процесів : проблеми теорії і практики : матеріали Всеукр. наук.-практ. конф., (18 лют. 2010 р.). — К., 2010. — С. 337–338.
34. Гелич Ю. О. Гарантії таємниці особистого життя людини в інформаційному праві України / Ю. О. Гелич // Політ. сучасні проблеми науки : матеріали X Міжнар. наук. конф. студ. та молодих вчених, (7–9 квіт. 2010 р.). — К., 2010. — Т. 2. — С. 107.
35. Гелич Ю. О. Інформаційно-правова сутність таємниці особистого життя людини / Ю. О. Гелич // Тенденції та пріоритети реформування законодавства України : матеріали Всеукр. наук.-практ. конф., (13 берез. 2010 р.). — Запоріжжя, 2010. — Ч.2. — С. 45–47.
36. Гоголь Б. М. Проблеми цивільно-правової охорони комерційної таємниці в Україні / Б. М. Гоголь // Вісник господарського судочинства. — 2004. — № 3. — С. 264–266.
37. Гоголь Б. М. Проблеми цивільно-правової охорони комерційної таємниці у контексті європейської інтеграції України / Б. М. Гоголь // Реформування правової системи України : проблеми і перспективи розвитку в контексті європейських інтеграційних процесів : міжнар. наук.-практ. конф., (Київ, 28–29 квіт. 2004 р.) : зб. наук. праць : в 2 ч. / [редкол.: С. А. Єрохін, В. Ф. Погорілко, Я. М. Шевченко та ін.]. — К., 2004. — Ч. 1. — С. 644–648.
38. Гоголь Б. М. Деякі проблеми цивільно-правового регулювання товарного обігу інформації / Б. М. Гоголь // Правові проблеми сучасності в умовах розвитку юридичної науки : Всеукр. наук.-практ. конф. до Дня науки, (Чернігів, 19 трав. 2005 р.) : зб. матеріалів. — Чернігів, 2005. — С. 254–257.
39. Гоголь Б. М. Комерційна інформація — особливий об'єкт права інтелектуальної власності / Б. М. Гоголь // Другі цивілістичні читання з питань права інтелектуальної власності, присвячені пам'яті професора О. А. Підпригори : матеріали Міжнар. наук.-практ. конференції. — К., 2009. — С. 205–208.



40. Головань С. М. Підходи до електронного документообігу з обмеженим доступом та його захист / С. М. Головань // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. — К., 2009. — Вип. 24. — С. 87–92.
41. Дідук А. Г. Правовий режим конфіденційної інформації: цивільно-правовий аспект: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / А. Г. Дідук; Харьк. націон. ун-т внутр. справ. — Х., 2008. — 23 с.
42. Дідук А. Г. Правовий режим конфіденційної інформації (комерційної таємниці) в Україні / А. Г. Дідук // Вісник Університету внутрішніх справ. — Х., 2000. — Спецвип. — С. 51–54.
43. Дидук А. Г. Конфиденциальная информация: можно ли ее рассматривать как объект права интеллектуальной собственности? / А. Г. Дидук // Технический прогресс и эффективность производства: Вестник Харьк. гос. политех. ун-та. — Х., 2000. — Спецвип. : Интеллектуальная собственность. — С. 115–120.
44. Дідук А. Г. Загальна характеристика інформація з обмеженим доступом в Україні / А. Г. Дідук // Вісник Національного університету внутрішніх справ. — Х, 2001. — Спецвип. — С. 242–246.
45. Дідук А. Г. Аналіз закордонного законодавства щодо конфіденційної інформації, комерційної таємниці / А. Г. Дідук // Вісник Національного університету внутрішніх справ. — Х., 2002. — Вип. 20. — С. 320–325.
46. Дідук А. Г. Поняття «інформації» у цивільному праві / А. Г. Дідук // Проблеми правознавства та правоохоронної діяльності: зб. наук. праць. — Донецьк, 2003. — № 2. — С. 174–181.
47. Дідук А. Г. Конфіденційна інформація: чи може бути суб'єктивне право на неї? / А. Г. Дідук // Актуальні проблеми правового захисту інтелектуальної власності в Україні: матеріали наук.-практ. конференції / НУВС. — Х., 2003. — С. 14–16.
48. Дідук А. Г. Цивільно-правовий захист права на конфіденційну інформацію (комерційну таємницю) / А. Г. Дідук // Актуальні проблеми цивільного права та процесу: матеріали наук.-практ. конф., присвяченої пам'яті професора О. А. Пушкіна / НУВС. — Х., 2005. — С. 65–69.
49. Дідук А. Г. Суб'єктивне право та інтерес щодо конфіденційної інформації / А. Г. Дідук // Охоронюваний законом інтерес в цивільному праві та процесі: матеріали круглого столу / ХНУВС. — Х., 2006. — С. 134–138.
50. Дідук А. Г. Співвідношення понять «комерційна таємниця» та «ноу-хау» / А. Г. Дідук // Новітні тенденції і стратегії розвитку міжнародної торгівлі: фінансово-економічний та правовий аспекти: зб. матеріалів X міжнар. наук.-практ. конференції. — К., 2007. — С. 268–271.
51. Дідук А. Г. Проблемні питання щодо охорони конфіденційної інформації: комерційної таємниці та ноу-хау в Україні / А. Г. Дідук // Проблеми цивільного права та процесу: матеріали наук.-практ. конф., присвяченої пам'яті професора О. А. Пушкіна / ХНУВС. — Х., 2008. — С. 204–208.
52. Дмитренко О. А. Право фізичної особи на власні персональні дані в цивільно-му праві України: автореф. дис. на здобуття наук. ступеня канд. юрид. наук:

- спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / О. А. Дмитренко. — К., 2010. — 19 с.
53. Дмитренко О. А. Проблема правомірності обробки персональних даних при проведенні онлайн-аутентифікації: американський та європейський досвід / О. А. Дмитренко // Адвокат. — 2005. — № 1. — С. 8–11.
  54. Дмитренко О. А. До проблеми відкликання суб'єктом персональних даних згоди на їх обробку у контексті приватноправових відносин / О. А. Дмитренко // Юридична Україна. — 2008. — № 2. — С. 49–52.
  55. Дмитренко О. А. Досвід США у регулюванні приватноправових відносин, пов'язаних з використанням персональних даних / О. А. Дмитренко // 36. наук. праць НДІ приватного права і підприємництва АПРН України. — К., 2008. — № 7. — С. 30–34.
  56. Дмитренко О. А. До проблеми поширення режиму відкритої інформації на персональні дані у світлі практики Європейського суду з прав людини / О. А. Дмитренко // Підприємництво, господарство і право. — 2008. — № 4. — С. 41–44.
  57. Dmytrenko O. NET Passport under the Scrutiny of U.S. and EU Privacy Law: Implications for the Future of Online Authentication / O. Dmytrenko, A. Nardali // A Journal of Law and Policy for the Information Society. — 2005. — Vol. 1. — № 2–3. — P. 619–645.
  58. Dmytrenko O. Does Ukraine Need a Comprehensive Statute to «Control» Private Data Controllers ? / O. Dmytrenko, C. D. Cutler // Washington University Global Studies Law Review. — 2006. — Vol. 5. — № 1. — P. 31–79.
  59. Дмитренко О. А. Приведення правової бази захисту персональних даних у відповідність до стандартів Ради Європи / О. А. Дмитренко // Розвиток цивільного законодавства України: шляхи подолання кодифікаційних протиріч : зб. матеріалів міжнар. наук-прак. конф., (Київ, 28–29 верес. 2006 р.). — К., 2006. — С. 308–311.
  60. Дмитренко О. А. Проблема правомірності мети обробки персональних даних / О. А. Дмитренко // Актуальні питання державотворення в Україні : зб. матеріалів міжнар. наук-прак. конф., (Київ, 24–25 квіт. 2008 р.). — К., 2008. — С. 208–210.
  61. Дмитренко О. А. Соотношение статей 8 и 10 Европейской конвенции при определении границ прав на персональные данные, на свободу выражения и информации / О. А. Дмитренко // Плекання культури прав людини: національна практика застосування : зб. матеріалів міжнар. методологічного семінару, (Київ, 8— 9 лип. 2008 р.). — К., 2008. — С. 167–178.
  62. Желіховський В. М. Правові засади електронної комерції в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / В. М. Желіховський; КНУВС. — К., 2007. — 22 с.
  63. Желіховський В. М. Проблеми розвитку електронної комерції в Україні / В. М. Желіховський // Боротьба з організованою злочинністю і корупцією (теорія і практика) / МНДЦ з проблем боротьби з організованою злочинністю. — К., 2004. — № 9. — С. 206–213.
  64. Желіховський В. М. Правове регулювання електронної комерції: досвід окремих країн світу / В. М. Желіховський // Боротьба з організованою злочинністю і

- корупцією (теорія і практика) / МНДЦ з проблем боротьби з організованою злочинністю. — К., 2004. — № 10. — С. 195–203.
65. Желіховський В.М. Організаційні та правові засади підвищення ефективності розвитку електронної комерції в Україні / В. М. Желіховський // Науковий вісник Нац. акад. внутр. справ України. — К., 2005. — № 6. — С. 259–263.
  66. Желіховський В. М. Електронна комерція як стимулятор розвитку правовідносин у мережі Інтернет / В. М. Желіховський // Правова інформатика : наук. журн. з питань правової інформатики, інформаційного права та інформаційної безпеки. — 2006. — № 4 (12). — С. 68–73.
  67. Желіховський В. М. Поширення електронної комерції в Україні / В. М. Желіховський // Правова інформатика : наук. журн. з питань правової інформатики, інформаційного права та інформаційної безпеки. — 2007. — № 2 (14). — С. 52–56.
  68. Желіховський В. М. Проблеми законодавчого регулювання електронної комерції в Україні / В. М. Желіховський // Науковий вісник Київ. нац. ун-ту внутр. справ України. — К., 2007. — № 3. — С. 135–139.
  69. Желіховський В. М. Недосконалість вітчизняного правового забезпечення у сфері електронної комерції / В. М. Желіховський // Шлях України до економічної безпеки : матеріали наук.-практ. конф. — Х., 2007. — С. 102–105.
  70. Івченко Т. В. Цивільно-правове регулювання комерційної таємниці як об'єкта права інтелектуальної власності в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / Т. В. Івченко. — К., 2009. — 19 с.
  71. Івченко Т. В. Порівняльне дослідження правового режиму конфіденційної інформації / Т. В. Івченко // Держава і право : зб. наук. праць. Юридичні і політичні науки. — К., 2005. — Вип. 27. — С. 365–371.
  72. Івченко Т. В. Деякі питання правового регулювання поняття «ноу-хау» / Т. В. Івченко // Держава і право : зб. наук. праць. Юридичні і політичні науки. — К., 2005. — Вип. 34. — С. 260–265.
  73. Івченко Т.В. Комерційна таємниця: деякі питання охорони, захисту та цивільно-правової відповідальності / Т.В. Івченко // Держава і право : зб. наук. праць. Юридичні і політичні науки. — К., 2007. — Вип. 35. — С. 357–362.
  74. Івченко Т. В. Роль суду в захисті права на комерційну таємницю / Т. В. Івченко // Держава і право : зб. наук. праць. Юридичні і політичні науки. — К., 2007. — Вип. 38. — С. 442–448.
  75. Івченко Т. В. Цивільно-правова охорона комерційної таємниці як об'єкта права інтелектуальної власності в Україні / Т. В. Івченко // Держава і право : зб. наук. праць. Юридичні і політичні науки. — К., 2008. — Вип. 42. — С. 401–408.
  76. Івченко Т. В. Деякі питання правового регулювання поняття комерційної таємниці / Т. В. Івченко // Держава і право : зб. наук. праць. Юридичні і політичні науки. Спец. вип. : Формування правової системи в Україні на сучасному етапі : міжнар. наук. конф., (Дніпропетровськ, 21–22 квіт. 2005 р.). — К., 2005. — Т. 1. — С. 396–399.
  77. Івченко Т. В. Конституційний захист прав інтелектуальної власності на комерційну таємницю / Т. В. Івченко // Права людини в умовах сучасного державот-

- ворення : теоретичні і практичні аспекти : матеріали І Міжнар. наук.-практ. конф., (Суми, 8–9 груд. 2006 р.) : зб. тез. доп. / [редкол.: А.О.Єпіфанов (гол. ред.) та ін.]. — Суми, 2006. — С. 117–119.
- 78.** Івченко Т. В. Історичні особливості правового розвитку комерційної таємниці та ноу-хау / Т. В. Івченко // Держава і право : зб. наук. праць. Юридичні і політичні науки. Спец. вип. : Вітчизняна юридична наукова спадщина і сучасність : Міжнар. наук. конф., (Дніпропетровськ, 27–28 квіт. 2007 р.). — К., 2007. — С. 339–343.
- 79.** Історія охорони державної таємниці в Україні : [монографія] / О. В. Ботвінкін, В. М. Шлапаченко, В. П. Ворожко, А. С. Пашков ; Національна академія Служби безпеки України ; Ін-т захисту інформації з обмеженим доступом. — К. : Нац. акад. СБ України, 2008. — 155 с.
- 80.** Климчук С. Проведення порівняльного аналізу законодавства у сфері інформації з обмеженим доступом України та країн-членів НАТО / С. Климчук, В. Артемов // Юридичний журнал : аналітичні матеріали, коментарі, судова практика / МОН України; НПУ ім. Драгоманова ; Ін-т політології та ін. — К., 2006. — № 11. — С. 40–45.
- 81.** Кулініч О. О. Загальні положення про інформацію з обмеженим доступом у цивільному праві : [монографія] / О. О. Кулініч. — Одеса, 2008. — 242 с.
- 82.** Кулініч О. О. Професійна таємниця як вид інформації з обмеженим доступом / О. О. Кулініч, К. М. Бондарчук // Університетські наукові записки Хмельницького університету управління та права : часопис / Хмельн. ун-т управл. та права. — Хмельницький, 2008. — Вип. 2. — С. 40–44.
- 83.** Ламонова П. П. Класифікація інформації з обмеженим доступом в системі інформаційної безпеки України / П. П. Ламонова // Актуальні проблеми міжнародних відносин : зб. наук. праць / Київ. нац. ун-т ім. Тараса Шевченка ; Ін-т міжнар. відносин ; [ред. кол.: Губерський Л. В. (гол. ред.) та ін.]. — К., 2009. — Вип. 83, ч. 1. — С. 187–189.
- 84.** Ламонова П. Класифікація інформації з обмеженим доступом в системі інформаційної безпеки України / П. Ламонова // Актуальні проблеми міжнародних відносин : зб. наук. праць / Київ. нац. ун-т ім. Тараса Шевченка ; Ін-т міжнар. відносин ; [ред. кол.: Губерський Л. В. (гол. ред.) та ін.]. — К., 2010. — Вип. 89, ч. 2. — С. 146–148
- 85.** Лащук Є. Інформація з обмеженим доступом як предмет злочину / Є. Лащук // Право України. — 2001. — № 3. — С. 75–78.
- 86.** Майданик Р. А. Розділ «Право на персональні дані фізичної особи» / Р. А. Майданик, О. А. Дмитренко // Аномалії в цивільному праві України : [навч.-практ. посіб.] / відп. ред. Р. А. Майданик. — К., 2007. — С. 893–909.
- 87.** Макаренко В. Адміністративно-правові аспекти захисту інформації з обмеженим доступом в Україні, Російській федерації і Казахстані / В. Макаренко, А. Макаренко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні / Нац. тех. ун-т України «КПІ» ; Мін-во освіти і науки України ; Департамент спец. телеком. сист. та захисту інформ. сл. безпеки. — К., 2006. — Вип. 2 (13). — С. 102–108.

- 88.** Марценюк О. Г. Заборонена інформація та її місце у системі інформаційних відносин / О.Г. Марценюк // *Право України*. — 2006. — № 5. — С. 44–48.
- 89.** Марценюк О. Г. Режими доступу до інформації в системі українського права / О. Г. Марценюк // *Юридична Україна*. — 2006. — № 7. — С. 23–29.
- 90.** Марценюк О. Г. Права фізичних і юридичних осіб на медичну конфіденційну інформацію / О. Г. Марценюк // *Медичне право України : правовий статус пацієнтів в Україні та його законодавче забезпечення (генезис, розвиток, проблеми і перспективи вдосконалення) : II Всеукр. наук.-практ. конф., (17–18 квіт. 2008 р.)*. — Львів, 2008. — С. 166–171.
- 91.** Марценюк А. Г. Конфиденциальная информация в системе права на информацию в Украине / А. Г. Марценюк // *Историко-правовые и социально-экономические аспекты развития общества : тезисы докл.V Межвуз. науч.-практ. конф., (5 апр. 2006 г.)*. — Чернигов, 2006. — С. 25–27.
- 92.** Матвієнко П. Є. Аналіз сучасного етапу розвитку законодавства про комерційну таємницю в Україні / П. Є. Матвієнко // *Підприємництво, господарство і право*. — 2009. — № 12. — С. 85–88.
- 93.** Матвієнко П. Є. Формування переліку інформації суб'єкта господарювання, яка становить комерційну таємницю / П. Є. Матвієнко // *Адвокат*. — 2009. — № 5. — С. 36–38.
- 94.** Матвієнко П. Є. Доцільність боротьби засобами адміністративного примусу з посяганнями на встановлений порядок обігу інформації, що становить комерційну таємницю / П. Є. Матвієнко // *Держава і право : зб. наук. праць. Юридичні і політичні науки*. — К., 2009. — № 46. — С. 273–276.
- 95.** Матвієнко П. Є. Організаційно-правові механізми захисту інформації, яка становить комерційну таємницю / П. Є. Матвієнко // *Юриспруденція : теорія і практика*. — 2009. — № 12. — С. 41–45.
- 96.** Матвієнко П. Є. Місце та роль адміністративної відповідальності у системі заходів охорони прав на комерційну таємницю / П. Є. Матвієнко // *Актуальні проблеми юридичної науки : зб. тез міжнар. наук. конф. [«Восьмі осінні юридичні читання»], (м. Хмельницький, 13–14 лист. 2009 р.) : у 4 ч.* — Хмельницький, 2009. — Ч. 2 : Конституційне право. Адміністративне право. Фінансове право. Інформаційне право. Земельне право. Аграрне право. Екологічне право. Природоресурсне право. Трудове право і право соціального забезпечення. — С. 115–116.
- 97.** Матвієнко П. Є. Основні напрями удосконалення системи захисту інформації, яка становить комерційну таємницю для суб'єкта господарювання / П. Є. Матвієнко // *Новітні підходи до державотворення в умовах європейської інтеграції (пам'яті професора Ю. І. Римаренка) : зб. тез міжвуз. наук.-теорет. конференції*. — К., 2009. — С. 99–102.
- 98.** Матвієнко П. Є. Технічний захист інформації у процесі підготовки кадрів для органів внутрішніх справ / П. Є. Матвієнко // *Наука і вища освіта : тези доп. учасників XVII Міжнар. наук. конф. студ. і молодих науковців, (м. Запоріжжя, 9–10 квіт., 2009 р.) : у 4 т. / Класичний приватний університет*. — Запоріжжя, 2009. — Т. 4. — С. 3–4.

99. Мезенцева Н. Б. Деякі аспекти захисту інформації з обмеженим доступом / Н. Б. Мезенцева // Економіка та держава : міжнар. наук.-практ. журнал. — К., 2013. — № 2. — С. 141–144.
100. Носік Ю. В. Права на комерційну таємницю в Україні (цивільно-правовий аспект): автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / О. В. Носік; Київ. нац. ун-т імені Тараса Шевченка. — К., 2006. — 13 с.
101. Носік Ю. В. Підстави виникнення, зміни і припинення прав на комерційну таємницю в Україні / Ю. В. Носік // Бюлетень Міністерства юстиції України. — 2006. — № 1. — С. 86–94.
102. Носік Ю. Міжнародно-правова охорона комерційної таємниці / Ю. В. Носік // Право України. — 2004. — № 11. — С. 131–135.
103. Носік Ю. В. Збереження комерційної таємниці в господарському судочинстві / Ю. В. Носік // Вісник господарського судочинства. — 2003. — № 3. — С. 214–223.
104. Носік Ю. В. Стан і проблеми правового забезпечення розвитку Інтернету в Україні / Ю. В. Носік // Вісник Київського національного університету імені Тараса Шевченка. Сер. Юридичні науки. — К., 2003. — Вип. 49–51. — С. 34–35.
105. Носік Ю. В. Юридичне значення ознак комерційної таємниці / Ю. В. Носік // Приватно-правовий метод регулювання суспільних відносин: стан та перспективи розвитку : зб. тез Міжнар. наук. конф. студ. та аспірантів (25–26 лист. 2005 р.). — К. — Хмельницький, 2005. — С. 266–268.
106. Носік Ю. В. Суб'єкти права на комерційну таємницю в Україні / Ю. В. Носік // Молодь у юридичній науці : зб. тез Міжнар. наук. конф. молодих вчених [«Четверті осінні юридичні читання»], (21–22 жовт. 2005 р.) : у 3 ч. — Хмельницький, 2005. — Ч. 2 : Приватно-правові науки. — С. 216–219.
107. Носік Ю. В. Проблемы процессуально-правовой охраны коммерческой тайны в Украине / Ю. В. Носік // Проблемы развития законодательства и правоприменительной практики : материалы междунар. науч. конф. студ. и аспиранто, (Минск, 29–30 окт. 2004 г.) / [редкол.: Г. А. Шумак (отв. ред.) и др.]. — Минск, 2005. — С. 124–126.
108. Носік Ю. В. Генеза законодавства про комерційну таємницю на території України до 1990 року / Ю. В. Носік // Молодь у юридичній науці : зб. тез доп. Міжнар. наук. конф. молодих вчених [«Треті осінні юридичні читання»]. — Хмельницький, 2004. — С. 202–203.
109. Носік Ю. В. Поняття інформаційних ресурсів за законодавством України / Ю. В. Носік // Держава та право очима молодих дослідників : зб. наук. праць між нар. наук. конф. студ. та аспірантів Київ. нац. ун-ту імені Тараса Шевченка, (29–30 лист. 2001 р.). — К., 2003. — С. 222–224.
110. Носік Ю. Захист банківської таємниці при здійсненні правосуддя господарськими судами / Ю. Носік // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — К., 2002. — Вип. 4. — С. 37–43.
111. Носік Ю. В. Огляд новел кримінального законодавства у сфері комп'ютерно-інформаційних злочинів / Ю. В. Носік // Третя науково-технічна конференція



- «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні»: тези доп. — К., 2001. — С. 27–79.
- 112.** Носік Ю. В. Правовий режим банківської таємниці в Україні / Ю. В. Носік // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — К., 2001. — Вип. 2. — С. 31–39.
- 113.** Носік Ю. В., Прокоф'єв М. І. Правовий режим інформаційних ресурсів в Україні / Ю. В. Носік, М. І. Прокоф'єв // *Бизнес и безопасность*. — 2001. — № 2. — С. 37–41.
- 114.** Носік Ю. В. Охорона і захист інформації власником / Ю. В. Носік // зб. тез доп. учасників II Нац. наук.-практ. конф. студентів, аспірантів та молодих вчених «Системний аналіз та інформаційні технології», (28–30 черв. 2000 р.) / НТУУ «КПІ». — К., 2000. — С. 178–182.
- 115.** Петрашев О. М. Організація професійної діяльності менеджера в сфері захисту інформації з обмеженим доступом / О. Р. Петрашев // *Бизнес и безопасность*. — 2012. — № 2. — С. 78–83.
- 116.** Прохніцький О. В. Інформація з обмеженим доступом як предмет злочину в кримінальному праві України: дис. ... канд. юрид. наук: 12.00.08 / Олег Віталійович Прохніцький; МВС України. — К., 2011. — 236 с.
- 117.** Рудик М. В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.08 «Кримінальне право і кримінологія; кримінально-виконавче право» / М. В. Рудик; Одес. нац. юрид. акад. — Одеса, 2007. — 19 с.
- 118.** Рудик М. В. Понятійний апарат предмета злочину, передбаченого статтею 363 КК України / М. В. Рудик // *Вісник Національного університету внутрішніх справ*. — Х., 2005. — № 29. — С. 131–135.
- 119.** Рудик М. В. Професійна таємниця як об'єкт кримінально-правової охорони / М. В. Рудик // *Вісник Національного університету внутрішніх справ*. — Х., 2005. — № 31. — С. 124–128.
- 120.** Рудик М. В. Суспільна небезпека від незаконного збуту й поширення комп'ютерної інформації з обмеженим доступом / М. В. Рудик // *Вісник Запорізького юридичного інституту*. — Запоріжжя, 2005. — № 3. — С. 120–124.
- 121.** Рудик М. В. До питання про захист комп'ютерної інформації з обмеженим доступом в ОВС / М. В. Рудик // *Актуальні проблеми сучасної науки в дослідженнях молодих учених*. — Х., 2005. — № 8. — С. 49–55.
- 122.** Рудик М. В. Міжнародний досвід протидії незаконному збуту та розповсюдженню конфіденційної інформації / М. В. Рудик, Д. П. Альошин // *Актуальні проблеми держави та права*. — Одеса, 2006. — № 27. — С. 222–228.
- 123.** Рудик М. В. Шляхи вирішення проблеми кваліфікації злочинних посягань на комп'ютерну інформацію з обмеженим доступом / М. В. Рудик // *Актуальні проблеми сучасної науки в дослідженнях молодих учених: зб. наук. праць*. — Х., 2006. — С. 34–37.
- 124.** Рудик М. В. Об'єкт та предмет незаконного збуту та розповсюдження комерційної та банківської таємниці / М. В. Рудик // *Право і безпека*. — Х., 2006. — № 5, ч. 2. — С. 70–72.



125. Самойлова О. С. Кримінально-правова характеристика передачі або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право і кримінологія ; кримінально-виконавче право» / О. С. Самойлова. — К., 2006. — 16 с.
126. Самойлова О. С. Конфіденційна інформація, що є власністю держави, як різновид інформації з обмеженим доступом / О. С. Самойлова // Актуальні проблеми сучасної науки в дослідженнях молодих учених : зб. наук. праць. — Х., 2003. — С. 84–85.
127. Самойлова О. С. Конфіденційна інформація, що є власністю держави як предмет злочину / О. С. Самойлова // Вісник Національного університету внутрішніх справ. — Х., 2004. — Вип. 27. — С. 185–188.
128. Самойлова О. С. Історичний аналіз формування інституту інформації з обмеженим доступом / О. С. Самойлова // Право і безпека. — Х., 2004. — № 3. — С. 77–80.
129. Самойлова О. С. Щодо визнання інформації предметом злочину / О. С. Самойлова // Актуальні проблеми сучасної науки в дослідженнях молодих учених : зб. наук. праць. — Х., 2004. — С. 57–59.
130. Самойлова О. С. Інформація з обмеженим доступом в державному управлінні / О. С. Самойлова // Актуальні проблеми державного управління. — 2004. — № 2 (21), ч. 2. — С. 242–246.
131. Самойлова О. С. Класифікація інформації з обмеженим доступом / О. С. Самойлова // Науковий вісник Юридичної академії МВС України. — Дніпропетровськ, 2004. — № 2. — С. 270–273.
132. Самойлова О. С. Аналіз об'єкта злочину, передбаченого ст. 330 КК України (передача або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави) / О. С. Самойлова // Право і безпека. — Х., 2004. — № 1. — С. 149–151.
133. Самойлова О. С. Особливості суб'єктивної сторони злочину, передбаченого ст. 330 КК України / О. С. Самойлова // Актуальні проблеми сучасної науки в дослідженнях молодих учених : зб. наук. праць. — Х., 2005. — С. 44–47.
134. Самойлова О. С. Особливості об'єктивної сторони передачі або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави / О. С. Самойлова // Вісник Національного університету внутрішніх справ. — Х., 2006. — Вип. 34. — С. 139–144.
135. Самойлова Е. С. Сравнительный анализ правового режима конфиденциальной информации, являющейся собственностью государства, в праве Украины и России / Е. С. Самойлова // Труды международной научной конференции «Информация и информационная безопасность правоохранительных органов». — М., 2003. — С. 48–50.
136. Скулиш Є. Організація захисту інформації з обмеженим доступом — перспективний напрям підготовки фахівців в Україні / Є. Скулиш, А. Марущак, А. Гуз // Вища школа : наук.-практ. вид. — 2012. — № 9. — С. 21–29.

- 137.** Становлення та розвиток системи захисту інформації в імовах форумування тоталітарної системи в СРСР / В. Ю. Артемов, А. С. Пашков, Н. І. Литвиненко, Є. С. Ленков // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. — К., 2010. — Вип. 28. — С. 135–139.
- 138.** Ткачук Т. Інформація з обмеженим доступом на підприємстві : проблеми безпеки та захисту / Т. Ткачук // Право України. — 2011. — № 3. — С. 243–251.
- 139.** Шарабурина О. О. Поняття адміністративно-правового режиму інформації з обмеженим доступом (основні підходи) / О. О. Шарабурина // Часопис Київського університету права : український наук.-теорет. часопис / Київський ун-т права НАН України ; Ін-т держ. і права ім. В. М. Корецького НАН України. — К., 2011. — № 2. — С. 120–123.
- 140.** Шаповалова А. О. Забезпечення охорони банківської таємниці у кримінальному процесі України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика ; судова експертиза ; оперативно-розшукова діяльність»/ А. О. Шаповалова ; КНУВС. — К., 2009. — 22 с.
- 141.** Шаповалова А. О. Поняття банківської таємниці: проблеми захисту у кримінальному процесі / А. О. Шаповалова // Підприємництво, господарство і право. — 2006. — № 10. — С. 138–141.
- 142.** Шаповалова А. О. Банківська таємниця: проблеми охорони та захисту / А. О. Шаповалова // Держава і право : зб. наук. праць. Юридичні і політичні науки. — К., 2006. — Вип. 34. — С. 482–486.
- 143.** Шаповалова А. О. Правові проблеми банківської таємниці / А. О. Шаповалова // Право України. — 2007. — № 2. — С. 102–105.
- 144.** Шаповалова А. О. Питання банківської таємниці в контексті порушення кримінальної справи / А. О. Шаповалова // Юридична Україна. — 2008. — № 1. — С. 57–60.
- 145.** Шаповалова А. О. Проблемні питання порядку розкриття інформації, яка належить до банківської таємниці / А. О. Шаповалова // Еволюція уголовного судопроизводства на постсоветском пространстве : материалы междунар. науч.-практ. конф., (Київ, 22–23 июня 2006 р.) : в 3 кн. / Мін-во освіти і науки України, Університет економіки і права «КРОК». — К., 2006. — Кн. III. — С. 169–174.
- 146.** Шаповалова А. О. Проблеми, які виникають під час виїмки документів, що становлять банківську таємницю / А. О. Шаповалова // Проблеми та перспективи реформування права України очима молодих вчених : тези доп. Всеукр. студент. наук.-практ. конф., (Запоріжжя, 23 берез. 2007 р.) / Мін-во освіти і науки України, Запорізький націонал. ун-т. — Запоріжжя, 2007. — С. 126–128.
- 147.** Шаповалова А. О. Слідчі дії, що дозволяють отримати відомості, які становлять банківську таємницю / А. О. Шаповалова // Проблеми вдосконалення правового забезпечення прав та основних свобод людини і громадянина : матеріали Всеукр. міжвузів. наук. конф. молодих вчених та аспірантів, (Івано-Франківськ, 20 квіт. 2007 р.) / Мін-во освіти і науки України ; Юрид. ін-т Прикарпат. націонал. ун-ту ім. Василя Стефаника. — Івано-Франківськ, 2007. — С. 419–421.

- 148.** Шатковська І. В. Адміністративно-правове забезпечення лікарської таємниці в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / І. В. Шатковська ; Нац. ун-т біорес. і природокрист. — К., 2010. — 25 с.
- 149.** Шатковська І. В. Лікарська таємниця: загальні правові засади / І. В. Шатковська // Науковий вісник Ужгородського національного університету. Серія. Право. — Ужгород, 2009. — № 2. — С. 46–50.
- 150.** Шатковська І. В. Правове регулювання інституту лікарської таємниці (українська історія та міжнародний досвід) [Електронний ресурс] / І. В. Шатковська // Форум права. — 2009. — № 3. — Режим доступу : <http://www.nbu.gov.ua/e-journals/FP/2009-3/09.pdf>.
- 151.** Шатковська І. В. Лікарська таємниця як елемент системи професійної таємниці: теоретико-правовий аспект / І. В. Шатковська // Юриспруденція: теорія і практика. — 2009. — № 11. — С. 14–17.
- 152.** Шатковська І. В. Лікарська таємниця як об'єкт правового регулювання / І. В. Шатковська // Підприємництво, господарство і право. — 2009. — №12. — С. 109–111.
- 153.** Шатковська І. В. Суб'єкти збереження лікарської таємниці (адміністративно-правовий аспект) / І. В. Шатковська // Науковий часопис НПУ імені М.П. Драгоманова. Серія 18. Економіка і право. — К., 2010. — №8. — С. 167–172.
- 154.** Шатковська І. В. Лікарська таємниця та її адміністративно-правове забезпечення в сучасних умовах / І. В. Шатковська // Актуальні проблеми юридичної науки : зб. тез міжнар. наук. конф. [«Сьомі осінні юридичні читання»] : у 4 ч. — Хмельницький, 2008. — Ч. 2. — С. 196–197.
- 155.** Шатковська І. В. Дотримання лікарської таємниці як реалізація права на приватність / І. В. Шатковська // Право на приватність: тенденції і перспективи : тези Всеукр. наук.-практ. конференції / ЛДУВС. — Львів, 2008. — С. 218–220.
- 156.** Шатковская И. В. Конституционное право на сохранение в тайне конфиденциальной информации о человеке и его реализация в медицинской практике Украины / И. В. Шатковская // Конституционные ценности : содержание и проблемы реализации : материалы Междунар. науч.-теорет. конф., (4–6 дек. 2008 г.) : в 2 т. / под ред. Н. В. Витрука, Л. А. Нудненко ; Рос. академия правосудия. — М., 2009. — Ч. 1. — С. 345–349.
- 157.** Шатковська І. В. Медична таємниця в контексті права та біоетики / І. В. Шатковська // Біоетика в системі охорони здоров'я і медичної освіти : матеріали міжнар. наук.-практ. конф., (26–27 берез. 2009 р.) / ЛНМУ імені Данило Галицького. — Львів, 2009. — С. 569–570.
- 158.** Шатковська І. В. Проблеми забезпечення права пацієнта на медичну таємницю / І. В. Шатковська // Актуальні проблеми державотворення в Україні очима молодих учених : зб. наук. праць Міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених Київського національного університету імені Тараса Шевченка, (23–24 квіт. 2009 р.). — К., 2009. — Ч. II. — С. 241–242.
- 159.** Шлома Г.О. Адміністративно-правове забезпечення службової таємниці в органах внутрішніх справ України : автореф. дис. на здобуття наук. ступеня канд.

- юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / Г. О. Шлома ; Дніпропетр. держ. ун-т внутр.. справ. — Дніпропетровськ, 2008. — 22 с.
- 160.** Шлома Г. О. Захист службової інформації органів внутрішніх справ як складова ефективної боротьби з наркоманією / Г. О. Шлома // Науковий вісник Юридичної академії Міністерства внутрішніх справ : зб. наук. праць. — Дніпропетровськ, 2003. — Спец.вип. № 1 (13). — С. 103–109.
- 161.** Шлома Г. О. Режим службової таємниці в органах внутрішніх справ України як елемент системи їх інформаційної безпеки / Г. О. Шлома // Проблеми правознавства та правоохоронної діяльності. — Донецьк, 2006. — №3. — С. 86–101.
- 162.** Шлома Г. О. Характеристика службової таємниці органів внутрішніх справ України як виду інформації з обмеженим доступом / Г. О. Шлома // Науковий вісник Запорізького юридичного інституту ДДУВС. — Дніпропетровськ, 2006. — № 3. — С. 121–131.
- 163.** Шлома Г. О. Завдання та зміст механізму адміністративно-правового забезпечення службової таємниці в органах внутрішніх справ України / Г. О. Шлома // Науковий вісник ДДУВС. — Дніпропетровськ, 2006. — №4. — С. 137–147.
- 164.** Шлома Г. О. Службова таємниця в діяльності органів внутрішніх справ України / Г. О. Шлома // Південноукраїнський правничий часопис. — Одеса, 2006. — № 4. — С. 157–164.
- 165.** Шлома Г. О. Службова таємниця як елемент інформаційних відносин в Україні / Г. О. Шлома // Зб. тез доп. Міжнар. наук. конференції молодих вчених [«Другі осінні юридичні читання»], (14 — 15 лист. 2003 р.). — Хмельницький, 2003. — С. 162–164.
- 166.** Шлома Г. О. Захист інформації як складова системи безпеки підприємства / Г. О. Шлома // Шлях України до економічної безпеки : матеріали наук.-практ. конф., (16 — 17 квіт. 2004 р.) / ХНУВС. — Х., 2004. — С. 89–91.
- 167.** Шлома Г. О. Методика побудови системи інформаційної безпеки організацій, установ та підприємств / Г. О. Шлома // Дні науки : зб. тез доп. : в 3 т. / Гуманітарний університет «ЗІДМУ». — Запоріжжя, 2005. — Т. 3. — С. 94–95.
- 168.** Шлома Г. О. Концептуальні основи формування інституту службової таємниці в діяльності державних органів України / Г. О. Шлома // Юридична наука та правоохоронна діяльність : матеріали міжвуз. наук.-практ. конф. молодих учених [«Проблеми боротьби зі злочинністю очима майбутніх правоохоронців»], (18 трав. 2005 р.) / Юрид. акад. МВС. — Дніпропетровськ, 2005. — С. 39–46.
- 169.** Шлома Г. О. Охорона комерційної та службової таємниць як елемент системи економічної безпеки підприємства / Г. О. Шлома // Актуальні проблеми протидії економічній злочинності, тінізації та корупції в умовах формування ринкової економіки в Україні : матеріали міжнар. наук.-практ. конф., (30 верес. 2005 р.) / [упоряд. І. О. Ревак, О. І. Руда] ; ЛДУВС. — Львів, 2006. — С. 100–103.
- 170.** Шлома Г. О. Недоліки системи забезпечення службової таємниці в органах внутрішніх справ України та шляхи їх усунення / Г. О. Шлома // Інформатизація вищих навчальних закладів МВС України : матеріали наук.-практ. конф., (Харків, 11–12 квіт. 2006 р.) / ХНУВС. — Х., 2006. — С. 245–250.

- 171.** Шлома Г. О. Заходи підвищення забезпечення режиму службової таємниці в органах внутрішніх справ України як чинник інформаційної безпеки держави / Г. О. Шлома // Удосконалення діяльності органів внутрішніх справ України з попередження й розкриття злочинів та інших правопорушень : матеріали Всеукр. наук.-практ. конф., (2 лист. 2007 р. м. Запоріжжя) : у 2 ч. / Юрид. ін-т МВС України. — Запоріжжя, 2007. — Ч. 1. — С. 71–74.
- 172.** Шлома Г. О. Право на інформацію з обмеженим доступом / Г. О. Шлома // Науковий вісник Юридичної академії Міністерства внутрішніх справ. — Дніпропетровськ, 2005. — № 2. — С. 310–315.
- 173.** Шлома Г. О. Зміст, поняття, ознаки інформації як об'єкту інформаційних відносин / Г. О. Шлома // Науковий вісник Юридичної академії Міністерства внутрішніх справ. — Дніпропетровськ, 2005. — № 3. — С. 337–344.
- 174.** Шлома Г. О. Кримінально-правова відповідальність за порушення правил обігу інформації з обмеженим доступом / Г. О. Шлома // Актуальні проблеми протидії злочинності в Україні : матеріали наук.-практ. семінару (21 берез. 2008 р., Дніпропетровський державний університет внутрішніх справ). — Дніпропетровськ, 2008. — С. 44–46.
- 175.** Харламова С. О. Кримінальна відповідальність за незаконні дії з відомостями, що становлять комерційну або банківську таємницю : дис. ... канд. юрид. наук : 12.00.08 / Світлана Олегівна Харламова ; Київський національний ун-т внутрішніх справ. — К., 2007. — 221 с.
- 176.** Ясечко С. Правовий режим інформації з обмеженим доступом у цивільному праві / С. Ясечко // Підприємництво, господарство і право. — 2010. — № 7. — С. 113–115.
- 177.** Ясечко С. В. Правовий режим інформації з обмеженим доступом у цивільному праві / С. В. Ясечко // Підприємництво, господарство і право. — 2010. — № 8. — С. 105–108.
- 178.** Ясечко С. В. Таємниця як режим інформації за Цивільним кодексом України / С. В. Ясечко // Проблеми цивільного права та процесу : матеріали міжнар. наук.-практ. конф., присвяченої пам'яті проф. О. А. Пушкіна, (31 трав. 2008 р.) / ХНУВС. — Х., 2008. — С. 313–315.
- 179.** Ясечко С. В. Множинність правовідносин при реалізації правової охорони інформації з обмеженим доступом / С. В. Ясечко // Зб. тез наук. робіт учасників IV міжнар. цивілістичної наук. конф. студентів та аспірантів / [упоряд.: А. Р. Чанишева, М. В. Матвійко, О. Л. Садовенко та ін.]. — Одеса : Фенікс, 2009. — С. 641–643.
- 180.** Ясечко С. В. Цивільно-правова відповідальність за порушення прав на інформацію з обмеженим доступом / С. В. Ясечко // Проблеми цивільного права та процесу : матеріали міжнар. наук.-практ. конф., присвяченої пам'яті проф. О. А. Пушкіна, (22 трав. 2010 р.) / ХНУВС. — Х., 2010. — С. 164–166.

### Адміністративно-правові режими

1. Бєлєвцєвє В. Адміністративно-правові режими у системі забезпечення національної безпеки України: поняття зміст та значення / В. Бєлєвцєвє // Право України. — 2010. — № 6. — С. 161–166.
2. Бєлєвцєвє В. До питання класифікації адміністративно-правових режимів / В. Бєлєвцєвє // Вісник Академії правових наук України. — X., 2009. — Вип.2 (57). — С. 103–111.
3. Бєлєвцєвє В. Удосконалення адміністративного законодавства з питань режимної діяльності / В. Бєлєвцєвє // Підприємництво, господарство і право. — 2010. — № 11. — С. 153–156.
4. Бєлєвцєвє В. Проблеми стандартизації адміністративно-правових режимів в Україні / В.Бєлєвцєвє // Підприємництво, господарство і право. — 2010. — № 9. — С. 84–87.
5. Бібік В. В. Адміністративно-правовий статус режимів особливих адміністративно-територіальних утворень : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / В. В. Бібік ; Акад. праці і соціал. відносин федерації проф. спілок України. — К., 2011. — 21с.
6. Бідей О. М. Адміністративно-правове забезпечення діяльності ОВС за умов надзвичайного стану : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право»/ О. М. Бідей ; НАВС. — К., 2011. — 16 с.
7. Бідей О. Проблеми вдосконалення законодавчого регулювання режиму надзвичайного стану / О. Бідей // Підприємництво, господарство і право. — 2009. — № 3. — С. 10–12.
8. Біла В. Публічний (правовий) режим адміністративних договорів за участю органів ДПС / В. Біла // Підприємництво, господарство і право. — 2010. — № 8. — С. 24–27.
9. Борисенко Н. А. Адміністративний нагляд міліції за дотриманням правил паспортно-реєстраційної системи : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / Н. А. Борисенко ; Дніпропетр. держ. ун-т внутр. справ. — Дніпропетровськ, 2011. — 20 с.
10. Васильєвє Т. С. Структура адміністративно-правового режиму господарської діяльності / Т. С. Васильєвє // Вісник Харківського національного університету внутрішніх справ. — X., 2011. — № 1 (52). — С. 221–227.
11. Виприцький А. О. Адміністративний примус в умовах надзвичайного стану : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / А. О. Виприцький ; ДДУВС. — Дніпропетровськ, 2011. — 20 с.
12. Гостєв В. В. Поняття та використання адміністративно-правових режимів в сучасних умовах / В. В. Гостєв // Вісник Луганського державного університету внутрішніх справ ім. Е. О.Дідорєнка. — Луганськ, 2010. — Вип. № 1. — С. 174–181.

13. Джафарова О. Структура правового режиму адміністративної діяльності правоохоронних органів України / О. Джафарова // Підприємництво, господарство і право. — 2010. — № 1. — С. 21–24.
14. Колінко Я. А. Надзвичайний стан як особливий державно-правовий режим : конституційно-правовий аспект : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.02 «Конституційне право»/ Я. А. Колінко ; НУ «Юридична академія України ім. Я.Мудрого». — Х., 2011. — 20 с.
15. Кузніченко С. О. Становлення та розвиток інституту надзвичайних адміністративно-правових режимів в Україні : автореф. дис. на здобуття наук. ступеня доктора юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / С. О. Кузніченко ; ХНУВС. — Х., 2010. — 37 с.
16. Магда С. О. Забезпечення прав, свобод та реалізації обов'язків громадян в умовах надзвичайних адміністративно-правових режимів : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право»/ С. О. Магда ; Нац. юрид. акад. України ім.Я.Мудрого. — Х., 2008. — 20 с.
17. Мінка Т. П. Адміністративно-правові режими та їх забезпечення органами внутрішніх справ : автореф. дис. на здобуття наук. ступеня доктора юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право»/ Тетяна Павлівна Мінка ; ДДУВС. — Дніпропетровськ, 2011. — 36 с.
18. Настюк В. Я. Адміністративно-правові режими у сфері національної безпеки та протидії тероризму : [монографія] / В. Я. Настюк ; АПРН України ; Ін-т вивчення проблем злочинності ; СБ України ; Ін-т оперативної діяльності та держ.безпеки. — К. : НКЦ СБ України, 2008. — 244 с.
19. Половніков В. В. Об'єктивна сторона порушень прикордонного режиму: проблеми нормативно-правового регулювання та кваліфікації / В.В. Половніков // Науковий вісник НАВС. — К., 2012. — Вип.1 (80). — С. 82–89.
20. Поповчук С. Сутність правової природи адміністративно-правових режимів в Україні / С. Поповчук // Підприємництво, господарство і право. — 2010. — № 8. — С. 36–39.
21. Приходько Я. Надзвичайний стан у системі державно-правових режимів / Я. Приходько // Підприємництво, господарство і право. — 2010. — № 2. — С. 34–38.
22. Сировой О. Правовий режим відомостей про результати медичного обстеження наречених в Україні / О. Сировой, М. Пришляк // Підприємництво, господарство і право. — 2012. — № 10. — С. 93–96.

### **Кримінально-правові та криміналістичні дослідження інформаційної сфери**

1. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія ; кримінально-вико-



- навче право»/ Д. С. Азаров ; Ін-т держ. і права ім. В. М. Корецького НАН України. — К., 2003. — 18 с.**
2. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика ; судова експертиза» / А. С. Білоусов ; Київ. нац. ун-т ім. Тараса Шевченка. — К., 2008. — 19 с.
  3. Бірюков В. В. Використання комп'ютерних технологій для фіксації криміналістично значимої інформації у процесі розслідування : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика ; судова експертиза» / В. В. Бірюков ; Нац. акад. внутр. справ України. — К., 2001. — 20 с.
  4. Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика ; судова експертиза» / Л. В. Борисова ; Київ. нац. ун-т внутр. справ. — К., 2007. — 19 с.
  5. Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика ; судова експертиза» / А. І. Журба ; Харків. нац. ун-т внутр. справ. — Х., 2008. — 19 с.
  6. Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину) : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія ; кримінально-виконавче право»/ М. В. Карчевський ; Нац. юрид. акад. України ім. Ярослава Мудрого. — Х., 2003. — 19 с.
  7. Красненкова Е. В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами : дисс. ... канд. юрид. наук : 12.00.08 / Елена Валерьевна Красненкова. — М., 2006. — 188 с.
  8. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика ; судова експертиза» / О. І. Мотлях ; Академія адвокатури України. — К., 2005. — 20 с.
  9. Орлов С. О. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія ; кримінально-виконавче право»/ С. О. Орлов ; Нац. ун-т внутр. справ. — Х., 2004. — 20 с.
  10. Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика ; судова експертиза» / Л. П. Паламарчук ; Академія адвокатури України. — К., 2005. — 18 с.
  11. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та кримі-

- налістика ; судова експертиза» / Д. В. Пашнев ; Харків. нац. ун-т внутр. справ. — Х., 2007. — 18 с.
12. Поливанюк В. Д. Особливості розслідування злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика ; судова експертиза» / В. Д. Поливанюк ; Київ. нац. ун-т внутр. справ. — К., 2008. — 17 с.
  13. Розенфельд Н. А. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія ; кримінально-виконавче право» / Н. А. Розенфельд ; Ін-т держ. і права ім. В. М. Корецького НАН України. — К., 2003. — 17 с.
  14. Рудик М. В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія ; кримінально-виконавче право» / М. В. Рудик ; Одес. нац. юрид. акад. — Одеса, 2007. — 19 с.
  15. Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика ; судова експертиза» / О. А. Самойленко ; Харків. нац. ун-т внутр. справ. — Х., 2007. — 20 с.

### Праці В.А.Ліпкана щодо системи знань про безпеку

1. Липкан В. Мультикультурализм и толерантность: грани соотношения / В. Липкан // Формирование толерантного сознания в обществе : материалы VII междунар. антитеррористического форума. — К., 2011. — С. 92–100.
2. Липкан В. А. Национальная безопасность и негосударственная система безопасности // Угроза международной стабильности : аспекты проблемы. — Европейский центр Изобразительных искусств, Братислава, 2013. — С. 90–93.
3. Липкан В. А. Основы права национальной безопасности / В. А. Липкан // Публичное и частное право. — 2009. — № 2. — С. 34–46.
4. Липкан В. Ренессанс безопасности. Негосударственная система безопасности как атрибут государства / В. Липкан, И. Бондаренко // Российские вести. — 11 февраля 2013 г. — № 3–4 (2107–2108). — С. 2.
5. Липкан В. А. Безпековий вимір Стратегії національної безпеки США / В. А. Липкан // Національна і міжнародна безпека в сучасних трансформаційних процесах : матеріали наук.-практ. конф., (Київ, 29 груд. 2011 р.). — К., 2011. — С. 8–11.
6. Липкан В. А. Біла книга: суть та призначення / В. А. Липкан // Адміністративне право в сучасному вимірі : матеріали IV наук.-практ. семінару / [ред. колегія : В. К. Колпаков (голова), О. В. Кузьменко, В. А. Липкан, І. Д. Пастух]. — К., 2010. — С. 19–21.

7. Ліпкан В. А. Державний суверенітет у контексті формування системи міжнародної безпеки / В. А. Ліпкан, О. В. Тюріна // Університетські наукові записки. — 2005. — № 3 (15). — С. 17–23.
8. Ліпкан В. А. Екзистенціальне управління системою національної безпеки / В. А. Ліпкан // Держава і право : зб. наук. праць. Юридичні і політичні науки. — К., 2003. — № 21. — С. 473–479.
9. Ліпкан В. А. Загальнонаукові методи націобезпекознавства / В. А. Ліпкан // Науковий вісник Національної академії внутрішніх справ України. — К., 2003. — № 4. — С. 26–33.
10. Ліпкан В. А. Міждисциплінарний підхід до формування націобезпекознавства / В. А. Ліпкан // Право України. — 2005. — № 1. — С. 94–99.
11. Ліпкан В. А. Об'єкт, предмет і структура націобезпекознавства / В. А. Ліпкан // Право і безпека. — Х., 2002. — № 4. — С. 26–29.
12. Ліпкан В. А. Підходи до аксіології національної безпеки / В. А. Ліпкан // Правові та політичні проблеми сучасності : матеріали наук.-практ. конф., (Луцьк, 22 квіт. 2012 р.). — К., 2012. — С. 8–11.
13. Ліпкан В. А. Проблеми формування інституту безпекового омбудсмана в контексті розбудови правової держави в Україні / В. А. Ліпкан // Право України. — 2010. — № 7. — С. 70–80.
14. Ліпкан В. А. Спеціально наукові методи націобезпекознавства / В. А. Ліпкан // Науковий вісник Національної академії внутрішніх справ України. — К., 2003. — № 3. — С. 63–73.
15. Ліпкан В. А. Теоретична концепція Білої книги / В. А. Ліпкан // Підприємництво, господарство і право. — 2010. — № 9. — С. 80–83.
16. Ліпкан В. А. Теорія національної безпеки : [підруч.] / В. А. Ліпкан. — К. : КНТ, 2009. — 631 с.
17. Ліпкан В. Інтереси держави: інтегральна категорія безпекознавства і державознавства / В. Ліпкан // Актуальні проблеми державотворення : матеріали наук.-практ. конф., (Київ, 28 черв. 2011 р.). — К., 2011. — С. 7–9.
18. Ліпкан В. Інтерпретаційні схеми розвитку систем безпеки / В. Ліпкан, О. Ліпкан // Юридична Україна. — 2006. — № 2. — С. 12–18.
19. Ліпкан В. Націобезпекознавство: проблеми формування категорійно-понятійного апарату / В. Ліпкан, Ю. Максименко // Підприємництво, господарство і право. — 2011. — № 8. — С. 7–11.
20. Ліпкан В. А. Застосування положень тектології при побудові системи національної безпеки / В. А. Ліпкан // Вісник Одеського інституту внутрішніх справ України. — Одеса, 2002. — № 4. — С. 128–132.
21. Ліпкан В. А. Концепція національної безпеки України: підходи до формування / В. А. Ліпкан // Вісник прокуратури. — 2003. — № 10. — С. 85–92.
22. Ліпкан В. А. Націобезпекознавча парадигма / В. А. Ліпкан // Право України. — 2003. — № 2. — С. 120–123.
23. Ліпкан В. А. Національна безпека України : [навч. посіб.] / В. А. Ліпкан. — [2-е вид.]. — К. : КНТ, 2009. — 576 с.

24. Ліпкан В. А. Національна і міжнародна безпека у визначеннях та поняттях / В. А. Ліпкан, О. С. Ліпкан. — [2-вид. доповн. і переробл.]. — К.: Текст, 2008. — 400 с.
25. Ліпкан В. А. Неопарадигма національної безпеки / В. А. Ліпкан // Право України. — 2002. — № 11. — С. 19—23.
26. Ліпкан В. А. Поняття та зміст націоналістичного вчення / В. А. Ліпкан // Право України. — 2003. — № 9. — С. 114—118.
27. Ліпкан В. А. Синергетичний і гомеостатичний підходи до системи національної безпеки / В. А. Ліпкан // Науковий вісник Національної академії внутрішніх справ України. — К., 2003. — № 2. — С. 104—111.
28. Ліпкан В. А. Теорія криз при дослідженні ролі біфуркацій в еволюції системи національної безпеки / В. А. Ліпкан // Держава і право : зб. наук. праць. Юридичні і політичні науки. — К., 2003. — № 22. — С. 61—68.
29. Міжнародна поліцейська енциклопедія : у 10 т. / відп. ред. Ю. І. Римаренко, Я. Ю. Кондратьєв, В. Я. Тацій, Ю. С. Шемшученко. — К., 2003. — Т. 1. — С. 41—57, 404—415, 441—450, 1007—1037.

### Угоди з інформаційних питань

1. Про підписання Угоди між Кабінетом Міністрів України та Урядом Об'єднаних Арабських Еміратів про взаємну охорону інформації з обмеженим доступом [Електронний ресурс] : розпорядж. Кабінету Міністрів України від 6 квіт. 2011 р. — Режим доступу : <http://zakon1.rada.gov.ua>.
2. Про підписання Угоди між Кабінетом Міністрів України та Урядом Республіки Польща про взаємну охорону інформації з обмеженим доступом [Електронний ресурс] : Закон України від 10 трав. 2012 р. — Режим доступу : <http://zakon1.rada.gov.ua>.
3. Про ратифікацію Угоди (у формі обміну нотами) між Кабінетом Міністрів України та Урядом Естонської Республіки про внесення змін та доповнень до Угоди між Кабінетом Міністрів України та Урядом Естонської Республіки про взаємну охорону секретної інформації [Електронний ресурс] : Закон України від 2 груд. 2010 р. — Режим доступу : <http://zakon1.rada.gov.ua>.
4. Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Грецької Республіки про взаємну охорону секретної інформації у сфері оборони [Електронний ресурс] : Закон України від 16 жовт. 2012 р. — Режим доступу : <http://zakon1.rada.gov.ua>.
5. Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Демократичної Соціалістичної Республіки Шрі-Ланка про взаємну охорону секретної інформації [Електронний ресурс] : Закон України від 6 квіт. 2011 р. — Режим доступу : <http://zakon1.rada.gov.ua>.
6. Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Йорданського Хашімітського Королівства про взаємну охорону інформації з обмеженим доступом [Електронний ресурс] : Закон України від 5 жовт. 2011 р. — Режим доступу : <http://zakon1.rada.gov.ua>.

7. Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Республіки Македонія про взаємну охорону інформації з обмеженим доступом [Електронний ресурс] : Закон України від 22 груд. 2010 р. — Режим доступу : <http://zakon1.rada.gov.ua>.
8. Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Республіки Кіпр про взаємну охорону інформації з обмеженим доступом [Електронний ресурс] : Закон України від 9 груд. 2011 р. — Режим доступу : <http://zakon1.rada.gov.ua>.
9. Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Республіки Екваторіальна Гвінея про взаємну охорону секретної інформації [Електронний ресурс] : Закон України 1 груд. 2010 р. — Режим доступу : <http://zakon1.rada.gov.ua>.
10. Угода між Кабінетом Міністрів України та Урядом Естонської Республіки про взаємну охорону секретної інформації [Електронний ресурс] : Закон України від 10 трав. 2004 р. — Режим доступу : <http://zakon1.rada.gov.ua>.

### **Інформаційне право та інформаційна безпека**

1. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : автореф. дис. на здобуття наук. ступеня доктора юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / І. В. Арістова ; Нац. ун-т внутр. справ. — К., 2002. — 39 с.
2. Беляков К. І. Організаційно-правове та наукове забезпечення інформатизації в Україні: проблеми теорії та практики : автореф. дис. на здобуття наук. ступеня доктора юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / К. І. Беляков ; Інститут держави і права ім. В. М. Корецького НАН України. — К., 2009. — 38 с.
3. Бурило Ю. П. Організаційно-правові питання державного управління в інформаційній сфері : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / Ю. П. Бурило ; Київ. нац. економ. ун-т ім. Вадима Гетьмана. — К., 2008. — 18 с.
4. Ващинець І. І. Цивільно-правова охорона авторських прав в умовах розвитку інформаційних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес ; сімейне право ; міжнародне приватне право» / І. І. Ващинець ; Ін-т держ. і права ім. В. М. Корецького НАН України. — К., 2006. — 20 с.
5. Вступ до інформаційної культури та інформаційного права : монографія / [В. М. Брижко, В. Д. Гавловський, Р. А. Калюжний, В. М. Попович, В. С. Цимбалюк, М. Я. Швець, О. І. Яременко] ; за ред. М. Я. Швеця, Р. А. Калюжного. — Ужгород : ІВА, 2003. — 240 с.
6. Глушков В. О. Про проект концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю в Україні / В. О. Глушков, К. І. Беляков,

- С. О. Орлов // Боротьба з організованою злочинністю і корупцією (теорія і практика). — К., 2002. — № 5. — С. 99–105.
7. Дзис С. А. Проблеми авторського права в сфері новітніх комп'ютерних технологій : дис. ... канд. юрид. наук : 12.00.03 / Сергій Анатолійович Дзис ; Київ. нац. ун-т ім. Тараса Шевченка. — К., 2004. — 252 с.
  8. Дидук А. Г. «Право на» інформацію (конфіденціальну інформацію) як «право доступу» / А. Г. Дідук // Проблеми цивільного права та процесу : матеріали міжнар. наук.-практ. конф., присвяченої пам'яті професора О.А. Пушкіна / ХНУВС. — Х., 2007. — С. 216–219.
  9. Дідук А. Г. Наскільки є вірними вихідні посилки, що лежать в основі порозуміння «інформації» як об'єкта цивільного права? / А. Г. Дідук // Актуальні проблеми цивільного права та процесу : матеріали наук.-практ. конф., присвяченої пам'яті професора О. А. Пушкіна / ХНУВС. — Х., 2006. — С. 210–214.
  10. Дмитришин В. С. Набуття та передання авторських прав на комп'ютерні програми : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес ; сімейне право ; міжнародне приватне право» / В. С. Дмитришин ; Ін-т держави і права ім. В. М. Корецького НАН України. — К., 2008. — 20 с.
  11. Е-боротьба в інформаційних війнах та інформаційне право : [монографія]. / В. М. Брижко, М. Я. Швець, В. С. Цимбалюк ; Акад. прав. наук України ; НДЦ прав. інформатики. — К., 2007. — 233 с.
  12. Е-майбутнє та інформаційне право / [В. Брижко, В. Цимбалюк, М. Швець, М. Коваль, Ю. Базанов ] ; за ред. М. Швеця. — К. : НДЦПІ АПРН України, 2006. — 234 с.
  13. Е-майбутнє та інформаційне право / [Брижко В., Цимбалюк В., Швець М., Коваль М., Базанов Ю.]. — [2-е вид., доповн.]. — К. : НДЦПІ АПРН України, 2006. — 232 с.
  14. Іванов Д. А. Інформаційно-правові основи забезпечення безпеки мореплавства : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / Д. А. Іванов ; Одес. нац. юрид. акад. — Одеса, 2008. — 19 с.
  15. Інформаційне право : концептуальні положення до кодифікації інформаційного законодавства : [монографія] / В. С. Цимбалюк. — К. : Освіта України, 2011. — 424 с.
  16. Інформаційне право : нормативні та методологічні засади упорядкування інформаційних відносин : [монографія] / В. М. Брижко, М.Я. Швець ; НДЦ прав. інформатики Акад. прав. наук України. — К., 2009. — 290 с.
  17. Інформаційне право та правова інформатика у сфері захисту персональних даних : [монографія]. / В. Брижко, М. Гуцалюк, В. Цимбалюк, М. Швець. — К. : НДЦПІ АПРН України, 2005. — 333 с.
  18. Інформаційне право України : стан, проблеми, перспективи / О. А. Баранов. — К. : СофтПрес, 2005. — 316 с.
  19. Інформаційні стратегії в глобальному управлінні : матеріали міжнар. наук.-практ. конф., (29 жовт. 2011 р., Київ) / [ред.: В. А Ліпкан] ; Global organization of allied leadership, Acad. of Open Society Security. — К. : Ліпкан О. С., 2011.

20. Калюжний Р. А. Інформатизація, право, управління (організаційно-правові питання) : монографія / [Р. А. Калюжний, О. Д. Крупчан, В. Д. Гавловський, М. В. Гуцалюк, В. С. Цимбалюк, М. Я. Швець] ; за заг. ред. М. Я. Швеця, О. Д. Крупчана. — К. : НДЦ правової інформатики АПрНУ, 2002. — 191 с.
21. Калюжний Р. А. Предмет та методи інформаційного права / Р. А. Калюжний, О. Г. Марценюк // Правова інформатика. — 2008. — № 3 (19). — С. 5–9.
22. Калюжний Р. А. Теоретико-методологічні засади формування науки інформаційного права / Р. А. Калюжний, О. Г. Марценюк // Інформаційне суспільство в Україні : інформаційно-правова культура, освіта, наука : Міжнар. наук.-практ. конф., (16 — 17 трав. 2008 р.). — Суми, 2008. — С. 38–44.
23. Калюжний Р. А. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики : монографія / [Р. А. Калюжний, В. О. Шамрай, В. Д. Гавловський, М. В. Гуцалюк, В. С. Цимбалюк, М. Я. Швець, Ю. В. Яцишин, А. С. Ластовецький] ; за ред. Р. А. Калюжного та В. О. Шамрая. — К. : Акад. ДПС України, 2002. — 296 с.
24. Колісник А. С. Цивільно-правовий захист комп'ютерного програмного забезпечення : дис. ... канд. юрид. наук : 12.00.03 / Артем Семенович Колісник ; Одес. нац. юрид. акад. — Одеса, 2007. — 187 с.
25. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня доктора юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / Б. А. Кормич ; Нац. ун-т внутр. справ. — Х., 2004. — 42 с.
26. Кузенко Л. В. Правове регулювання права громадян на інформацію в сфері державного управління : дис. ... канд. юрид. наук : спец. 12.00.07 / Лариса Володимирівна Кузенко ; Нац. ун-т внутр. справ. — Х., 2003. — 173 с.
27. Кукшинова О. О. Правове регулювання доступу до відкритої інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / О. О. Кукшинова ; НАН України ; Ін-т держави і права ім. В.М. Корецького. — К., 2012. — 20 с.
28. Лисенко О. О. Актуальні питання захисту суспільства від шкідливої інформації / О. О. Лисенко // Вісник Харківського національного університету внутрішніх справ. — Х., 2009. — № 4 (47). — С. 30–37.
29. Лисенко О. О. До проблеми правового регулювання «неналежної» реклами в Україні / О. О. Лисенко // Вісник Харківського національного університету внутрішніх справ. — Х., 2010. — № 2 (49). — С. 219–228.
30. Лисенко О. О. Правові аспекти захисту від інформації, що негативно впливає на суспільну мораль / О. О. Лисенко // Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки. — К., 2010. — Вип. 82. — С. 92–94.
31. Лисенко О. О. Правові аспекти захисту суспільства від дії інформації, що здійснює неусвідомлювану негативну дію на здоров'я людей / О. О. Лисенко // Інформаційна безпека людини, суспільства, держави : наук.-практ. журнал Національної академії СБ України. — 2010. — № 4. — С. 31–34.
32. Лисенко О. О. Правові засади захисту суспільства від дії шкідливої інформації / О. О. Лисенко // Актуальні проблеми сучасної науки в дослідженнях моло-



- дих учених : матеріали наук.-практ. конф., (м. Харків, 5 черв. 2010 р.) / ХНУВС. — Х., 2010. — С. 132–134.
- 33.** Лисенко О. О. Щодо видів шкідливої інформації / О. О. Лисенко // Роль та місце ОВС у розбудові демократичної правової держави : матеріали II Міжнар. наук.-практ. конф., (Одеса, 23 квіт. 2010 р.) / Одес. держ. ун-т внутр. справ. — Одеса, 2010. — С. 42–43.
- 34.** Маруженко О. П. Інформаційне забезпечення законотворчого процесу в Україні : дис. ... канд. юрид. наук : 12.00.07 / Олексій Петрович Маруженко. — К., 2009. — 202 с.
- 35.** Марценюк О.Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / О. Г. Марценюк ; КНУВС. — К., 2009. — 22 с.
- 36.** Марценюк О. Г. Право людини на інформацію в європейському та українському праві / О. Г. Марценюк // Вісник Донецького університету. Серія В. Економіка і право. — Донецьк, 2006. — № 2, т. 2. — С. 429–432.
- 37.** Нестеренко О. В. Чи зможе прийняття законопроекту «Про інформаційну відкритість органів державної влади та вищих посадових осіб України» забезпечити інформаційну відкритість влади / О. В. Нестеренко // Свобода висловлювань і приватність : щокварт. дод. до інформ.-аналіт. бюл. Харк. правозахис. групи «Права людини». — 2005. — № 3. — С. 9–11.
- 38.** Нестеренко О. В. Генезис права на доступ до інформації / О. В. Нестеренко // Актуальні проблеми правознавства : тези доп. та наук. повідомл. учасн. наук. конф. молодих учених та здобувачів / за ред. М. І. Панова. — Х., 2006. — С. 31–33.
- 39.** Нестеренко О. В. До питання заснування інституту спеціалізованого Омбудсман із захисту права на доступ до інформації в Україні / О. В. Нестеренко // Молодь у юридичній науці : зб. тез міжнар. наук. конф. молодих вчених [«Четверті осінні юридичні читання»], (21–22 жовт. 2005 р.) : у 3 ч. — Хмельницький, 2005. — Ч. 1 : Загальнотеоретичні та історичні правові науки. Конституційне право. — С. 201–204.
- 40.** Нестеренко О. В. Законодавче регулювання права на доступ до інформації в Україні: проблеми та шляхи вдосконалення / О. В. Нестеренко // Проблеми державотворення і захисту прав людини в Україні : матеріали XII регіон. наук.-практ. конф., (9 — 10 лют. 2006 р.). — Львів, 2006. — С. 167–168.
- 41.** Нестеренко О. В. Інформаційний омбудсман в механізмі забезпечення прав людини і основоположних свобод / О. В. Нестеренко // Юридична Україна. — № 1. — 2008. — С. 16–21.
- 42.** Нестеренко О. В. Неурядові правозахисні організації в механізмі забезпечення права на доступ до інформації в Україні / О. В. Нестеренко // Конституційно-політичний процес в Україні : ідеї, досвід, проблеми : зб. наук. статей за матеріалами XVIII Харк. політологічних читань. — Х., 2006. — С. 88–89.
- 43.** Нестеренко О. В. Огляд змін до законодавства в сфері регулювання діяльності засобів масової інформації та свободи інформації в Україні у 2005 р. / О. В. Не-

- стеренко // Свобода висловлювань і приватність : щокварт. дод. до інформ.-аналіт. бюл. Харк. правозахис. групи «Права людини». — Х., 2005. — № 4. — С. 3–9.
44. Нестеренко О. В. Підстави обмеження права на доступ до інформації / О. В. Нестеренко // Проблеми законності : респ. міжвідом. наук. зб. — Х., 2007. — Вип. 86. — С. 49–55.
45. Нестеренко О. В. Право на доступ до інформації в Україні: конституційно-правовий аспект: автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / О. В. Нестеренко ; Нац. юрид. акад. України ім. Ярослава Мудрого. — Х., 2008. — 22 с.
46. Нестеренко О. В. Проблеми вдосконалення законодавства України по забезпеченню права на доступ до інформації / О. В. Нестеренко // Проблеми законності : респ. міжвідом. наук. зб. — Х., 2006. — Вип. 83. — С. 110–115.
47. Нестеренко О. В. Проблеми забезпечення права на доступ до інформації: конституційно-правовий аспект / О. В. Нестеренко // Конституція України — основа побудови правової держави і громадянського суспільства : тези доп. та наук. повідомл. учасн. всеукр. наук.-практ. конф. молодих учених та здобувачів, (26 — 27 черв. 2006 р.) / за заг. ред. М. І. Панова. — Х., 2006. — С. 27–30.
48. Нестеренко О. В. Проблеми конституційно-правового регулювання права на інформацію в Україні / О. В. Нестеренко // Проблеми законності : респ. міжвідом. наук. зб. — Х., 2005. — Вип. 75. — С. 7–13.
49. Нестеренко О. В. Фактори, що впливають на реалізацію права на доступ до інформації / О. В. Нестеренко // Простір і час сучасної науки : матеріали Всеукр. наук.-практ. Інтернет-конф., (24 — 26 квіт. 2006 р.). — К., 2006. — С. 29–31.
50. Орлов С. А. Международно-правовые аспекты борьбы с преступлениями в сфере компьютерных технологий / С. А. Орлов // Правові основи захисту комп'ютерної інформації від протиправних посягань : матеріали міжвуз. наук.-практ. конф. — Донецьк, 2000. — С. 32–44.
51. Орлов С. О. Комп'ютерна інформація як предмет злочину / С. О. Орлов // Право і безпека. — Х., 2005. — Т. 4. — № 1. — С. 150–155.
52. Орлов С. О. Кримінальна відповідальність за комп'ютерні злочини у деяких країнах СНД / С. О. Орлов // Вісник Університету внутрішніх справ. — Х., 2000. — Спецвипуск. — С. 161–164.
53. Орлов С. О. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія ; кримінально-виконавче право» / С. О. Орлов ; НУВС. — Х., 2004. — 19 с.
54. Орлов С. О. Порівняльний аналіз відповідальності за правопорушення в комп'ютерній сфері / С. О. Орлов // Науковий вісник НАВСУ. — К., 2000. — Вип. 3. — С. 260–268.
55. Орлов С. О. Проект концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю в Україні / С. О. Орлов // Теорія та практика застосування чинного кримінального та кримінально-процесуального законодавства

- у сучасних умовах : тези доп. наук.-практ. конф., (квітень 2002 р., м. Київ) : у 2 ч./ НАВС України. — К., 2002. — Ч. 2. — С. 159–161.
- 56.** Основи інформаційного права України : навч. посіб. / [В. С. Цимбалюк, В. Д. Гавловський та ін.] ; за ред. М. Я. Швеця, Р. А. Калюжного та П. В. Мельника. — [2-е вид., переробл. і доповн.]. — К. : Знання, 2009. — 414 с.
- 57.** Пастухов О. М. Авторське право у сфері функціонування всесвітньої інформаційної мережі Інтернет : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес ; сімейне право ; міжнародне приватне право»/ О. М. Пастухов ; Ін-т держ. і права ім. В. М. Корецького НАН України. — К., 2002. — 18 с.
- 58.** Правова інформатика: система інформатизація законотворчої, правозастосововчої, правоохоронної, судочинної та правоосвітньої діяльності в Україні : монографія / [В. М. Брижко, І. А. Вознюк, В. Д. Гавловський, О. В. Глодківська, Л. М. Задорожня, Р. А. Калюжний, Ю. А. Клімашевська, В. А. Саницький, В. Ф. Севастьянов, В. М. Смаглюк, В. Г. Хахановський, В. С. Цимбалюк, М. Я. Швець, О. І. Яременко] ; за ред. М. Я. Швеця, Р. А. Калюжного. — Ужгород : ІВА, 2003. — 168 с.
- 59.** Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 2 / ред.: В. І. Найденко ; Нац. техн. ун-т України «КПІ». — К., 2001. — 273 с.
- 60.** Субина Т. В. Техническая защита информации как один из факторов информационной безопасности в органах государственной налоговой службы Украины / Т. В. Субина // Финансовая система России : опыт и перспективы правового регулирования : тез. докл. междунар. науч.-практ. конф. — Красноярск, 2008. — С. 358–364.
- 61.** Субіна Т. В. Адміністративно-правове забезпечення інформаційної безпеки в органах державної податкової служби України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / Т. В. Субіна ; Нац. ун-т держ. податк. служби України. — Ірпінь, 2010. — 24 с.
- 62.** Субіна Т. В. Інформатика як основа формування інформаційного суспільства та як об'єкт правознавства / В. К. Шкарупа, Т. В. Субіна // Правова інформатика. — 2004. — № 4. — С. 22–28.
- 63.** Субіна Т. В. Інформатика, інформатизація, інформаційне суспільство як об'єкт правознавства / В. К. Шкарупа, Т. В. Субіна // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. — К., 2004. — С. 6–11.
- 64.** Субіна Т. В. Інформаційна безпека в електронному банкінгу / Т. В. Субіна // Електронний банкінг (організаційно-правове забезпечення) : [монографія] / за заг. ред. А. М. Новицького. — Ірпінь : Нац. ун-т ДПС України, 2008. — 274 с.
- 65.** Субіна Т. В. Обмен налоговой информацией с другими государствами в польском законодательстве / Я. Орловский, Т. В. Субіна // Міжнародне співробітництво України у сфері оподаткування. Реформування податкової служби України відповідно до європейських стандартів : зб. матеріалів наук.-практ. конференції / НДЦ з проблем оподаткування. — Ірпінь, 2009. — С. 231–233.

66. Субіна Т. В. Питання щодо проблем з'ясування сутності інформації та інформаційного простору як нових чинників суспільних правовідносин / В. К. Шкарупа, Т. В. Субіна // *Правова інформатика*. — 2005. — № 2 (6). — С. 8–12.
67. Субіна Т. В. Структура та функції соціологічної служби в органах ДПС України / Т. В. Субіна // *Корупційні ризики у сфері оподаткування (соціологічне дослідження)* : [монографія] / за заг. ред. С. П. Ріппи. — К. : Леся, 2008. — 208 с.
68. Субіна Т. В. Основні засади формування податкового потенціалу регіонів. Інфраструктура інформатизації податкової служби: стан і перспектива / Т. В. Субіна // *Податкова політика України : стан, проблеми, перспективи* : [монографія] / за ред. З. С. Варналія. — К. : Знання України, 2008. — 675 с.
69. Субіна Т. В. Забезпечення інформаційної безпеки електронної звітності в органах ДПС України / Т. В. Субіна // *Правова інформатика*. — 2009. — № 1 (21). — С. 91–98.
70. Субіна Т. В. Забезпечення інформаційної безпеки при здійсненні електронного оподаткування / Т. В. Субіна // *Організаційно-правове забезпечення електронного оподаткування : зб. тез наук.-практ. круглого столу / НДЦ з проблем оподаткування*. — Ірпінь, 2008. — С. 75–78.
71. Субіна Т. В. Інформаційна безпека у сфері банківської діяльності / Т. В. Субіна // *Організаційно-правові основи протидії податковим та суміжним правопорушенням у сфері електронного банкінгу* : зб. матеріалів наук.-практ. круглого столу / НДЦ з проблем оподаткування ; НДЦ правової інформатики Академії правових наук. — Ірпінь-Київ, 2007. — С. 47–49.
72. Субіна Т. В. Інформаційні технології як засіб формування інформаційного суспільства в Україні / Т. В. Субіна // *Фінансово-правові дослідження : теорія та практика* : зб. тез./ Нац. ун-т ДПС України. — Ірпінь, 2006. — С. 122–125.
73. Субіна Т. В. Міжнародний досвід захисту податкової інформації / Т. В. Субіна // *Проблеми впровадження інформаційних технологій в економіці : матеріали VII міжнар. наук.-практ. конференції* / Нац. ун-т ДПС України. — Ірпінь, 2009. — Ч. 2. — С. 292–294.
74. Субіна Т. В. Сучасні принципи стандартизації державної політики України в інформаційній сфері / Т. В. Субіна, С. В. Фетісова // *Тенденції та перспективи розвитку податкової системи України : матеріали наук.-практ. конференції* / Нац. ун-т ДПС України. — Ірпінь, 2008. — С. 589–593.
75. Субіна Т. В. Теоретико-методологічні підходи до визначення поняття інформаційного права / Т. В. Субіна // *Науковий вісник Національної академії ДПС України*. — Ірпінь, 2006. — № 2 (33). — С. 226–232.
76. Субіна Т. В. Морально-етичні принципи податківця та механізм їхнього запровадження у діяльність органів ДПС України / Т. В. Субіна // *Професійна етика працівника державної податкової служби як складова етики державного службовця України : матеріали доповідей науково-практичної конференції* / Нац. ун-т ДПС України. — Ірпінь, 2005. — С. 302–304.
77. Субіна Т. В. Питання і сутність інформації у просторі держави / Т. В. Субіна // *Науковий вісник Національної академії ДПС України*. — Ірпінь, 2004. — № 4 (26). — С. 210–214.

78. Субіна Т. В. Розвиток інформаційних технологій у банківській діяльності / Т. В. Субіна // Сучасний стан та перспективи розвитку фінансового права : тези доп. міжнар. наук.-практ. конф., (м. Ірпінь) / Науково-дослідний інститут фінансового права. — К., 2007. — С. 194–397.
79. Субіна Т. В. Формування державної політики щодо інформаційної безпеки / Т. В. Субіна // Інформаційне суспільство в Україні : інформаційно-правова культура, освіта, наука : матеріали між нар. наук.-практ. конференції. — Суми, 2008. — С. 180–183.
80. Субіна Т. В. Формування інформаційного законодавства України: проблемні аспекти / Т. В. Субіна // Науковий вісник Національної академії ДПС України. — Ірпінь, 2005. — № 1 (28). — С. 176–181.
81. Тацишин І. Б. Адміністративно-правове забезпечення інформаційних відносин в галузі реклами : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / І. Б. Тацишин ; Львів. держ. ун-т внутр. справ. — Львів, 2009. — 18 с.
82. Цимбалюк В. С. Сутність і зміст правової інформатики (методологічний аспект) / В. С. Цимбалюк // Правова інформатика. — 2005. — № 4 (8). — С. 18–30.
83. Цимбалюк В. С. Сутність і зміст правової інформатики (методологічний аспект) / В. С. Цимбалюк // Правова інформатика. — 2005. — № 4 (8). — С. 18–30.
84. Цимбалюк В. Правова інформатика в діяльності прокуратури України / В. С. Цимбалюк // Правова інформатика. — 2007. — № 2 (14). — С. 18–27.
85. Цимбалюк В. С. Методологія правової інформатики в систематизації податкового законодавства України як чинника боротьби з корупцією / В. С. Цимбалюк // Боротьба з організованою злочинністю і корупцією (теорія і практика) / МНДЦ з проблем боротьби з організованою злочинністю. — К., 2005. — № 11. — С. 176–184.
86. Цимбалюк В. С. Методологія правової інформатики в систематизації податкового законодавства України як чинника боротьби з корупцією / В. С. Цимбалюк // Боротьба з організованою злочинністю і корупцією (теорія і практика) / МНДЦ з проблем боротьби з організованою злочинністю. — К., 2005. — № 11. — С. 176–184.
87. Цимбалюк В. С. Основи інформаційного права України : навч. посіб. / [В. С. Цимбалюк, В. Д. Гавловський, В. В. Грищенко та ін. ] ; за ред. М. Я. Швеця, Р. А. Калужного та П. В. Мельника. — К. : Знання, 2004. — 274 с.
88. Цимбалюк В. С. Основи інформаційного права України : навч. посіб. / [В. С. Цимбалюк, В. Д. Гавловський, В. В. Грищенко та ін. ] ; за ред. М. Я. Швеця, Р. А. Калужного та П. В. Мельника. — К. : Знання, 2009. — 414 с.
89. Цимбалюк В. С. Роль правової інформатики у модернізації прокуратури України / В. С. Цимбалюк // Право України. — 2006. — № 11. — С. 73–77.
90. Шевчук О. М. Адміністративно-правове регулювання у сфері забезпечення інформаційної безпеки : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес ; фінансове право ; інформаційне право» / О. М. Шевчук ; Класич. приват. ун-т. — Запоріжжя, 2011. — 20 с.

## СЛОВА ДЯКИ

Хочемо висловити слова щирої дяки тим, хто своїми змістовними порадами, неординарними думками, конструктивними рекомендаціями, організаційною підтримкою сприяли проведенню досліджень, результатом яких і стало видання цієї роботи.

Передусім хочемо щиро подякувати своїм Батькам за їх Любов, Підтримку та Розуміння, близьким за їх довготерпіння та всіляке сприяння творчій атмосфері, що й стало запорукою нашого натхнення.

Особливу подяку автори висловлюють голові спеціалізованої вченої ради К 26.004.16 у Національному університеті біоресурсів і природокористування України *Володимиру Івановичу Курилу*.

Щиро вдячні шановним опонентам: докторові юридичних наук, професору, заступнику директора з наукової роботи Юридичного інституту Національного авіаційного університету *Калюжному Ростиславу Андрійовичу*, а також кандидату юридичних наук, старшому науковому співробітнику Науково-дослідного центру правової інформатики Національної академії правових наук України *Цимбалюку Віталію Степановичу*.

Під час захисту нами було отримано чимало конструктивних порад від членів спеціалізованої вченої ради, зокрема: *Ірини Вікторівни Арістової, Віктора Валерійовича Ладиченка, Олександра Петровича Свєтличного, Віталія Івановича Семчика, Володимира Казимировича Гіжевського* та інших.

Слова подяки також висловлюємо вченому секретареві спеціалізованої вченої ради К 26.004.16 у Національному університеті біоресурсів і природокористування України, кандидату юридичних наук — *Олексію Юрійовичу Піддубному* за підтримку теми дослідження і чітке документальне супроводження.



Красно дякуємо доктору технічних наук, професорові *Миколи Яковичу Швецю*, доктору юридичних наук, професорові *Ростиславу Андрійовичу Калюжному*, кандидату юридичних наук, старшому науковому співробітнику *Віталію Степановичу Цимбалоку*, які узяли на себе працю бути вимогливими рецензентами та допомогли низкою цінних зауважень, рекомендацій і побажань. Саме їхня ґрунтовна праця сприяла конструктивності та виваженості наукових висновків у роботі.

Вихід цієї праці став можливий також завдячуючи всілякій підтримці керівництва Глобальної Організації Союзницького Лідерства і Академії безпеки відкритого суспільства, а також видавця — *Олени Сергіївни Ліпкан*.

Величезне спасибі за активну підтримку та дієву допомогу у підготовці видання, за інформативно місткі, неординарні поради з теоретико-методологічних і практичних аспектів роботи та конкретні методичні рекомендації з відбору матеріалу й поліпшенню якості його викладення, за розуміння і моральне стимулювання фахівцям:

- 1) Національної академії правових наук України — *Олександру Васильовичу Скрипнюку*, начальнику відділу міжнародних наукових зв'язків, доктору юридичних наук, професору, академіку НАПрН України;
- 2) Верховної Ради України — *Григорію Олександровичу Усатому*, Головному науковому консультанту Комітету законодавчого забезпечення правоохоронної діяльності, кандидату юридичних наук, старшому науковому співробітнику;
- 3) Кабінету Міністрів України — *Олександру Євгеновичу Бухтатому*, Головному спеціалістові Департаменту фахової експертизи Секретаріату Кабінету Міністрів України, кандидату наук з державного управління;
- 4) Юридичного інституту Національного авіаційного університету — *Валерію Костянтинівичу Колпакову*, завідувачому кафедрою конституційного та адміністративного права, доктору юридичних наук, професору;
- 5) Маріупольського державного університету — *Юрію Олексійовичу Волошину*, професору кафедри конституційного,



- адміністративного та міжнародного права, доктору юридичних наук;
- 6) Запорізького національного університету – *Тетяні Олександрівні Коломоєць*, декану юридичного факультету, доктору юридичних наук, професору, заслуженому юристу України;
  - 7) Львівського державного університету внутрішніх справ – *Коваліву Мирославу Володимировичу*, завідувачу кафедри конституційного, адміністративного та міжнародного права, кандидату юридичних наук, професору;
  - 8) Івано-франківського факультету Національного університету «Одеська юридична академія» – *Басаю Віктору Давидовичу*, декану, доктору юридичних наук, професору, академіку Академії наук вищої освіти України;
  - 9) ТОВ «Універсал» – *Олександрову Володимировичу Логінову*, начальникові юридичного відділу, кандидату юридичних наук, доценту;
  - 10) Навчально-наукового інституту менеджменту безпеки Університету економіки та права «КРОК» – *Пригунову Павлу Яковичу*, директору, кандидату психологічних наук, доценту.

Від себе особисто (*Ліпкан В. А.*) хочу низько вклонитися моїм вчителям.

Ушанувати світлу пам'ять свого батька *Анатолія Миколайовича Ліпкана*, який натхненно вкладав у мене свою любов, загартував мій дух до перемог, сформував незламний характер, дав мені шлях у житті, спрямував мою життєву енергію на досягнення шляхетних цілей.

Красно вдячний своїй першій вчительці *Катерині Іванівні Сидоренко*, яка підтримувала мене з перших років навчання, привчала до самостійного осягнення навколишнього середовища, готувала до майбутніх невдач і перемог, і в цілому сприяла становленню мене як особи з чітко сформованою громадянською позицією.

Шаную світлу пам'ять *Сергія Михайловича Штефана*, який після мого закінчення з відзнакою спеціалізованої фізико-математичної школи № 173 м. Києва зумів прищепити мені *любов до*

*права*, спонукав до глибшого розуміння його сутності і призначення у сучасному буремному світі.

Слова дяки хочу сказати *Юрію Валер'яновичу Александрову*, який розпалив жаринку *любові вже до юридичної науки*, надав можливість повірити у власні сили та навернув мене до перших маленьких успіхів – у 1995 році саме під його керівництвом я виборов перемогу на Всеукраїнському конкурсі наукових робіт, що проводила Українська правнича фундація, отримавши премія імені Володимира Суміна.

Хочу згадати добрими словами людину, яка відкрила мені двері до тернистого *шляху науки* – керівника кандидатської дисертації – *Володимира Івановича Антипова*, який був джерелом життєдайної сили і наснаги, еталоном наукового керівника та особистості. Саме він прищепив мені навички до копіткої аналітичної праці, навчив ефективно працювати з матеріалом, наполегливо рухатись вперед, постійно вчитись.

Особлива дяка своєму науковому консультанту по докторській дисертації – *Василію Івановичу Шакуну*, порядність, мудрість і принципова наукова позиція якого сприяли становленню мене як доктора юридичних наук і вченого, здатного самостійно формувати наукові школи, пропагуючи науковий стиль мислення і буття.

Від себе особисто (*Баскаков В.Ю.*) хочу подякувати моєму керівникові кандидатської дисертації доктору юридичних наук, доценту, академіку Академії наук вищої освіти України *Володимиру Анатолійовичу Ліпкану* за його професіоналізм, майстерність, невтомну копітку працю, щоденну підтримку та допомогу в написанні дисертації й виданні монографії.

Спасибі усім нашим Вчителям, ми щиро вдячні і завжди пам'ятатимемо та цінуватимемо Вашу віру в кожного з нас.

Дякуємо усім, хто щиро підтримує нас.

*Наукове видання*

**Ліпкан Володимир Анатолійович  
Баскаков Володимир Юрійович**

# **АДМІНІСТРАТИВНО-ПРАВОВИЙ РЕЖИМ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ**

*Монографія*

Керівник проекту **В.А.Ліпкан**  
Художній редактор *О. Г. Новіков*  
Літературний редактор *О. О. Машкова*  
Випускаючий редактор *О. О. Машкова*  
Коректор *О. С. Ліпкан*  
Дизайн обкладинки: *В. А. Ліпкан*  
Комп'ютерне верстання *Д. Лепешин*  
Відповідальний за випуск *І. Михайленко*

Підписано до друку 05.05.2013 р. Формат 70x100/16. Папір офсетний.  
Гарнітура Times New Roman. Друк офсетний. Умов.друк.арк. S)H' ž  
Наклад 500 прим. Зам. № 1%Ź & ž

**Видавець ФОП Ліпкан Олена Сергіївна**  
03 126, Київ, вул. М.Донця, 23, б, кв. 33  
Тел. +38 098 00.77.888, факс: +38 044 4040 483  
E-mail: **book@market-ua.com.**, сайт: **www.book.market-ua.com.**  
Свідоцтво суб'єкта видавничої справи ДК № 3535 від 27.07.09.

---

Виготівник ТОВ «Дорадо-Друк»  
09000, м.Сквира, вул. Щорса, 7  
Свідоцтво про внесення суб'єкта видавничої справи  
до Державного реєстру ДК № 2600 від 01.09.2006 р.