DOI: 10.18372/2307-9061.64.16896
УДК 343.97:342.5(045)

С. Я. Лихова,
доктор юридичних наук, професор
ORCID ID: https://orcid.org/0000-0003-4755-7474

В. П. Сисоєва,
кандидат юридичних наук
ORCID ID: https://orcid.org/0000-0003-1673-3682

ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mails: sofiia.lykhova@npp.nau.edu.ua, viktoriia.sysoieva@npp.nau.edu.ua

Мета: *визначення основних напрямків діяльності правоохоронних органів у забезпеченні інформаційної безпеки держави, а також аналіз нормативного закріплення та практичного проведення цієї діяльності.* ***Методи:*** *дослідження проводилося із застосуванням діалектичного підходу, методів аналізу, синтезу, а також низки загальнонаукових та спеціально-правових методів дослідження.* ***Результати:*** *ефективне забезпечення інформаційної безпеки правоохоронними органами передбачає пошук нових форм та способів її забезпечення, горизонтальну та вертикальну взаємодію на внутрішньодержавному та міжнародному рівнях, юридичний аналіз розроблення відомчих нормативно-правових актів, що регулюють цю діяльність.* ***Обговорення:*** *правоохоронні органи в межах своєї компетенції зобов'язані протидіяти загрозам інформаційної безпеки. Для виконання повноважень із забезпечення інформаційної безпеки правоохоронні органи використовують низку методів. Одним із основних є метод адміністративного-правового регулювання.*

Ключові слова: *інформаційна безпека; правоохоронний орган; кібербезпека; інформація; інформаційні технології; персональні дані.*

Постановка проблеми та її актуальність. Забезпечення інформаційної безпеки залишається досить важливим завданням, яке стоїть перед кожною державою. Одним із основних суб'єктів її забезпечення є правоохоронні органи, адже саме вони покликані захищати суспільство і державу від протиправних посягань, а також підтримувати стан законності, громадської безпеки та правопорядку. На жаль, розвиток інформаційних технологій у сучасному суспільстві, окрім позитивних нововведень, також часто створює негативні наслідки: виникають нові види загроз інформаційній безпеці; удосконалюються способи приховування правопорушень, вчинених в інформаційній сфері; збільшується обсяг негативних наслідків від таких правопорушень тощо.

Правоохоронні органи, основне завдання яких можна сформулювати як забезпечення законності у суспільстві, захист прав та інтересів громадян, протидія кримінальним та іншим правопорушенням, не можуть залишатися осторонь проблеми забезпечення інформаційної безпеки. Однак нормативно-правове закріплення напрямків їхньої діяльності в сфері забезпечення інформаційної безпеки містить певні особливості, а також зазнає частих змін, що викликає необхідність дослідження окресленої проблематики.

Аналіз досліджень і публікацій з проблеми. Проблемам забезпечення інформаційної безпеки присвятили чисельні наукові праці вітчизняні і зарубіжні вчені, серед яких В.Б. Авер'янов, С.М. Алфьоров, К.І. Бєляков, С.В. Ващенко, Г.В. Дугінець, Ю.Д. Кунєв, С.Я. Лихова, А.Ю. Нашинець, С.Г. Онопрієнко, В.В. Середа, І.М. Сопілко, І.М. Шопіна та багато інших. Науково-інформаційною основою статті стали праці таких науковців, як І.Д. Казанчук, В.П. Яценко, П.О. Яковлєв, О.Г. Колб та інші.

Метою статті є визначення основних напрямків діяльності правоохоронних органів у забезпеченні інформаційної безпеки держави, а також аналіз нормативного закріплення та практичного проведення цієї діяльності.

Виклад основного матеріалу. У вітчизняному правовому просторі містяться чисельні дефініції поняття «інформаційна безпека». Як зазначає С. Усик, говорячи про органи державної влади взагалі, сьогодні можна склались дві тенденції у визначенні поняття та структури інформаційної безпеки. Представники гуманітарного напряму пов'язують інформаційну безпеку лише із забезпеченням державної таємниці. Представники силових структур пропонують поширити сферу інформаційної безпеки практично на всі питання й відносини в інформаційній сфері. «Хто володіє інформацією, той володіє світом». Інформаційна безпека суспільства й держави характеризується ступенем їх захищеності, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості тощо) щодо небезпечних, дестабілізуючих, деструктивних дій, які шкодять інтересам країни. Отже, під захистом інформації розуміється комплекс заходів, які здійснюються власником інформації щодо виокремлення своїх прав на володіння й розпорядження інформацією, створення умов, які обмежують її поширення, виключають чи суттєво ускладнюють несанкціонований, незаконний доступ до таємної інформації та її носіїв. Інформація, що захищається, може містити різні категорії відомостей, з установленим ступенем їх секретності та мати свої особливості регулювання збереження її цілісності [1, с. 271]. Цілком погоджуючись з зазначеною тезою С. Усик, варто додати, що правоохоронні органи, як представники силових структур, в першу чергу покликані забезпечити ефективну протидію посяганням на інформаційну безпеку. В нашій країні є широкий перелік державних органів, що об'єднані назвою «правоохоронні органи», і вони різняться своїми функціями, специфікою та методами діяльності, підпорядкованістю органам державної влади тощо.

Крім того, на законодавчому рівні створені належні умови для забезпечення інформаційної безпеки в Україні. Так, у ч. 1 ст. 17 Конституції України проголошено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу; у ч. 2 ст. 34 – кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [2]. З огляду на те, що згідно зі ст. 3 Закону України «Про національну безпеку України» [3] об'єктами національної безпеки є людина і громадянин (їхні життя і гідність, конституційні права і свободи, безпечні умови життєдіяльності); суспільство (його демократичні цінності, добробут та умови для сталого розвитку); держава (її конституційний лад, суверенітет, територіальна цілісність та недоторканність); території, навколишнє природне середовище (від надзвичайних ситуацій), можна стверджувати, що національна безпека являє собою комплексний феномен (метасистему), складовими якого є безпека відповідних об'єктів у кожній сфері їх життєдіяльності. Проте, вважаємо, слід погодитися з О.Г. Колбом та Р.О. Колбом, що практика свідчить про суттєві правові прогалини, суперечності та неузгодженості між нормами Конституції України та законами і іншими нормативно-правовими актами, що регулюють питання інформаційної діяльності в нашій державі. Мова, наприклад, ведеться про захист конфіденційної інформації про особу без її згоди. Зокрема, досить поширеними у сьогоденні є так звані «журналістські розслідування», які нічого спільного з положеннями законів, що регулюють діяльність журналістів в Україні, не мають [4, с. 91].

Однак, як слушно зазначає Ю.Д. Кунєв, визначальною складовою інформаційної безпеки є її правовий компонент, який полягає в наявності системи правових норм та гарантій їх дієвості за напрямами реалізації функцій держави у сфері інформаційної діяльності: регулятивної та охоронної. Таким чином, предмет правового забезпечення інформаційної безпеки утворюється сукупністю суспільних відносин, пов'язаних з інформацією, інформаційною діяльністю, інформаційною інфраструктурою і правовим статусом суб'єктів інформаційної сфери, що належать до об'єктів національних інтересів, а також із проявом загроз безпеці цих об'єктів [5, с. 98]. Один із найбільш чисельних правоохоронних органів – Національна поліція України – містить у своєму складі спеціальний підрозділ – Департамент кіберполіції, який відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність.

Згідно з відомчою регламентацією, до основних завдань Департаменту кіберполіції входять: участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; а також сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень.

Для виконання повноважень із забезпечення інформаційної безпеки правоохоронні органи використовують низку методів. Одним із основних є метод адміністративного-правового регулювання. В основі сутності цього методу лежить владний вплив держави в особі її органів та посадових осіб на певну сферу суспільних відносин або поведінку суб'єктів задля досягнення максимального регулюючого впливу норм адміністративного права в інтересах забезпечення правопорядку, безпеки і захисту прав і свобод особи. Методи адміністративно-правового регулювання характеризують систему, організацію самих юридичних способів і засобів упорядкування суспільних відносин у певній сфері, у тому числі й у сфері забезпечення інформаційної безпеки. Адміністративно-правовий метод регулювання містить ідеї і засади регулювання у певній області виконавчо-розпорядчої діяльності держави [6, с. 12]. Оскільки така сфера державного управління, як забезпечення інформаційної безпеки, є складною і передбачає не лише застосування широкого спектру організаційно-правових заходів управління, а й урахування тенденцій застосування новітніх досягнень розвитку інформаційно-технічної галузі, методи адміністративно-правового регулювання зазначеної сфери характеризуються особливими властивостями [7, с. 67]. В межах використання адміністративно-правового методу правоохоронними органами у забезпеченні інформаційної безпеки варто зазначити, що цей метод є універсальним для правоохоронної діяльності та дозволяє використовувати надані державою повноваження для усунення небезпеки посягання на інформаційну безпеку.

Крім того, варто погодитися з П.О. Яковлєвим стосовно того, що методи адміністративно-правового регулювання забезпечення інформаційної безпеки держави відображають систему управлінського впливу на процеси захисту національної інформаційної інфраструктури, відвернення явних та потенційних загроз інформаційному середовищу України, впорядкування інформаційних відносин тощо. Особливістю зазначених методів є їх значний функціональний потенціал, адже спектр впорядкованих ними відносин є широким і має вагоме соціальне значення. Оскільки динамічний розвиток засобів обробки інформації сприяє постійному удосконаленню інформаційної зброї, питання про оптимізацію і удосконалення нормативної основи здійснення державного регулювання забезпечення інформаційної безпеки залишається актуальним. Відповідно, перспективним напрямом наукових досліджень є вироблення пропозицій щодо оптимізації адміністративно-правової основи здійснення управлінської діяльності у сфері забезпечення інформаційної безпеки України [7, с. 69].

Варто також звернути увагу на те, що поряд із терміном «інформаційна безпека», відомчі нормативно-правові акти правоохоронних органів містять також поняття «кібербезпека». Для співставлення цих категорій варто навести думку І.М. Сопілко, яка зауважує: «…хоча кібербезпеку можна розглядати як підмножину інформаційної безпеки, обидва цих типи безпеки своєю основною метою мають захист даних. Інформаційна безпека орієнтована на захист від будь-яких загроз важливих даних, як у цифровій, так і в аналоговій формі. А кібербезпека зосереджена на цифровій інформації, також нерозривно пов'язана із такими категоріями як кіберзлочини, кібератаки тощо … Культура інформаційної безпеки, так само як і кібербезпеки, вимагає безперервного поліпшення. Персонал організації повинен усвідомлювати масштаби і спільну місію щодо забезпеченню безпеки у своїй роботі. Також з боку влади важливо приділяти достатню увагу розробці нових і поліпшенню наявних методів протидії порушенням у даній сфері, чому, безсумнівно, буде сприяти запозичення досвіду провідних країн світу і гармонізація чинного законодавства із нормативними актами ЄС [8, с. 113]. Дійсно, в більшості випадків, говорячи про забезпечення інформаційної безпеки правоохоронними органами, ми маємо на увазі саме забезпечення кібербезпеки. Але важливо розуміти, що цим поняття забезпечення інформаційної безпеки не обмежується.

Крім того, правоохоронні органи в межах своєї компетенції зобов'язані протидіяти загрозам інформаційної безпеки, в тому числі – інформаційного тероризму. Законодавство України не містить визначення інформаційного тероризму. Закон України «Про боротьбу з тероризмом» містить поняття «технологічний тероризм», яке не збігається з дефініцією «інформаційний тероризм», а Закон України «Про основні засади забезпечення кібербезпеки України» містить визначення «кібертероризму», який можна визнати лише одним із різновидів інформаційного тероризму [9, с. 172]. В цьому аспекті варто звернути увагу на важливість взаємодії між правоохоронними та іншими органами для усунення таких небезпек. Зважаючи на важливість спільних дій у боротьбі з кіберзлочинами на міжнародному рівні, Департамент кіберполіції Національної поліції України активно співпрацює з правоохоронними органами багатьох країн (США, Велика Британія, Франція, Німеччина, Польща, Італія тощо), а також з правоохоронними міжнародними організаціями (Європол, Інтерпол, NCFTA тощо).

І.Д. Казанчук та В.П. Яценко характеризують систему кібербезпеки в Україні сьогодні як слабку. На їхню думку, ситуація складається таким чином, що наразі кожен має піклуватися про свою кібербезпеку самостійно у випадках, коли ділиться масивом персональних даних у мережі. Наразі ніхто, крім кіберполіції, і на тому рівні, на якому вона це може робити, не говорить про важливість підвищення правосвідомості у сфері цифрової безпеки. Хоча необхідно розповідати про кібербезпеку в закладах середньої і вищої освіти й підвищувати кваліфікацію працівників, діяльність яких пов'язано з обробкою персональних даних. Також важливий технічний компонент – це забезпечення цілісності, конфіденційності та доступності інформації інженерно-технічними заходами. Сьогодні велике значення надається комунікаційній складовій, яка вимагає розвитку системи моніторингу та формування контенту для соціальних мереж. В умовах формування інформаційного суспільства кожна людина має бути проінформована про структуру й особливості діяльності кіберполіції. Тому наразі актуальним завданням є створення реальних стратегічних і тактичних документів, також слід чітко поділити сфери відповідальності між суб'єктами кібербезпеки [10, с. 36-37]. Отже, розвиток інформаційних технологій обов'язково повинен супроводжуватися подальшим удосконаленням діяльності із забезпечення інформаційної безпеки правоохоронними органами.

Висновки. Ефективне забезпечення інформаційної безпеки правоохоронними органами передбачає пошук нових форм та способів її забезпечення, горизонтальну та вертикальну взаємодію на внутрішньодержавному та міжнародному рівнях, юридичний аналіз розроблення відомчих нормативно-правових актів, що регулюють цю діяльність. Основне завдання правоохоронних органів у цій галузі полягає у забезпеченні захисту прав та інтересів громадян в ін-

формаційному просторі та протидії посяганням на інформаційну безпеку.

Література

1. Усик С. Дослідження правового механізму забезпечення інформаційної безпеки в умовах надзвичайних ситуацій. *Науковий вісник: «Державне управління»*. 2020. № 4 (6). С. 266-280.

2. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

3. Про національну безпеку України: Закон України від 21 черв. 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355

4. Колб О.Г., Колб Р.О. Нормативно-правові неузгодженості та суперечності інформаційної діяльності – одна із загроз національної безпеки України. *Вісник пенітенціарної асоціації України*. 2020. № 3 (13). С. 90-97. DOI: https://doi.org/10.34015/2523-4552.2020.3.09

5. Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2021. № 1(58). С. 95-102. DOI: https://doi.org/10.18372/2307-9061.58.15314

6. Авер'янов В.Б. Нова доктрина українського адміністративного права: концептуальні позиції. *Право України*. 2006. № 5. С. 11–15.

7. Яковлєв П.О. Методи адміністративно-правового регулювання забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2020. Випуск 61. Том 2. С. 66-69.

8. Сопілко І.М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2021. № 2(59). С. 110-115. DOI: https://doi.org/10.18372/2307-9061.59.15603

9. Леонов Б.Д., Лихова С.Я. Інформаційний тероризм як загроза національній безпеці України. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2021. № 2(59). С. 170-176. DOI: https://doi.org/10.18372/2307-9061.59.15615

10. Казанчук І.Д., Яценко В.П. Особливості правового регулювання діяльності національної поліції України у сфері забезпечення інформаційної безпеки в Україні. *Право і безпека*. 2020. № 4(79). С. 32-38.

References

1. Usyk S. Doslidzhennia pravovoho mekhanizmu zabezpechennia informatsiinoi bezpeky v umovakh nadzvychainykh sytuatsii. *Naukovyi visnyk: «Derzhavne upravlinnia».* 2020. № 4 (6). S. 266-280.

2. Konstytutsiia Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

3. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21 cherv. 2018 r. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355

4. Kolb O.H., Kolb R.O. Normatyvno-pravovi neuzghodzhenosti ta superechnosti informatsiinoi diialnosti – odna iz zahroz natsionalnoi bezpeky Ukrainy. *Visnyk penitentsiarnoi asotsiatsii Ukrainy.* 2020. № 3 (13). S. 90-97.

5. Kuniev Yu.D. Pravove zabezpechennia informatsiinoi bezpeky yak predmet pravovoho doslidzhennia. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu. Seriia: Yurydychnyi visnyk «Povitriane i kosmichne pravo».* Kyiv: NAU, 2021. № 1 (58). S. 95-102.

6. Averianov V.B. Nova doktryna ukrainskoho administratyvnoho prava: kontseptualni pozytsii. *Pravo Ukrainy*. 2006. № 5. S. 11–15.

7. Iakovliev P.O. Metody administratyvno-pravovoho rehuliuvannia zabezpechennia informatsiinoi bezpeky Ukrainy. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia «Pravo».* 2020. Vypusk 61. Tom 2. S. 66-69.

8. Sopilko I.M. Informatsiina bezpeka ta kiberbezpeka: porivnialno-pravovyi aspekt. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu. Seriia: Yurydychnyi visnyk «Povitriane i kosmichne pravo».* Kyiv: NAU, 2021. № 2 (59). S. 110-115.

9. Leonov B.D., Lykhova S.Ya. Informatsiinyi teroryzm yak zahroza natsionalnii bezpetsi Ukrainy. *Naukovi pratsi Natsionalnoho*

aviatsiinoho universytetu. Seriia: Yurydychnyi visnyk «Povitriane i kosmichne pravo». Kyiv: NAU, 2021. № 2 (59). S. 170-176.

10. Kazanchuk I.D., Yatsenko V.P. Osoblyvosti pravovoho rehuliuvannia diialnosti natsionalnoi politsii Ukrainy u sferi zabezpechennia informatsiinoi bezpeky v Ukraini. *Pravo i bezpeka.* 2020. № 4 (79). S. 32-38.

Sofiia Lykhova, Viktoriia Sysoieva

ACTIVITIES OF LAW ENFORCEMENT BODIES OF UKRAINE IN THE SPHERE OF ENSURING INFORMATION SECURITY

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mails: sofiia.lykhova@npp.nau.edu.ua, viktoriia.sysoieva@npp.nau.edu.ua

Purpose: *determination of the main areas of activity of law enforcement agencies in ensuring the information security of the state, as well as analysis of regulatory consolidation and practical implementation of this activity.* ***Methods:*** *the research was conducted using a dialectical approach, methods of analysis, synthesis, as well as a number of general scientific and special legal research methods.* ***Results:*** *effective provision of information security by law enforcement agencies involves the search for new forms and methods of its provision, horizontal and vertical interaction at the domestic and international levels, legal analysis of the development of departmental regulations regulating this activity.* ***Discussion:*** *law enforcement agencies are obliged to counter threats to information security within their competence. Law enforcement agencies use a number of methods to implement information security powers. One of the main ones is the method of administrative and legal regulation.*

Ensuring information security remains a rather important task facing every state. One of the main subjects of its provision are law enforcement agencies, because they are called to protect society and the state from illegal encroachments, as well as maintain the state of legality, public safety and law and order. Unfortunately, the development of information technologies in modern society, in addition to positive innovations, also often creates negative consequences: new types of threats to information security arise; methods of concealing offenses committed in the information sphere are being improved; the amount of negative consequences from such offenses.

Law enforcement agencies, whose main task can be formulated as ensuring legality in society, protecting the rights and interests of citizens, countering criminal and other offenses, cannot remain aloof from the problem of ensuring information security. However, the regulatory and legal consolidation of the directions of their activities in the field of ensuring information security contains certain features and also undergoes frequent changes.

Key words: *information security; law enforcement agency; cyber security; information; Information Technology; personal data.*

Стаття надійшла до редакції 31.08.2022