КОНСТИТУЦІЙНЕ ТА АДМІНІСТРАТИВНЕ ПРАВО

DOI: 10.18372/2307-9061.59.15597
УДК 342.9(045)

В. В. Калетнік,
аспірант

СУЧАСНИЙ СТАН АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ: ТЕОРЕТИКО-ПРАВОВИЙ АНАЛІЗ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mail: human-rights@online.ua

Мета: *аналіз сучасного стану адміністративно-правового забезпечення інформаційної безпеки в Україні, напрацювання науково обґрунтованих пропозицій та рекомендацій з цього питання.* ***Методи дослідження:*** *у дослідженні автор використовував методи теоретичного аналізу та аналізу змісту, монографічний метод, метод систематизації для виявлення та конкретизації авторської позиції в рамках досліджуваних питань. При підготовці висновків та рекомендацій за результатами дослідження був використаний метод узагальнення.* ***Результати дослідження:*** *визначено напрями підвищення ефективності адміністративно-правового забезпечення інформаційної безпеки в Україні на основі реалізації комплексу організаційно-правових заходів.* ***Обговорення:*** *динамічний розвиток інформаційного суспільства зумовлює потребу постійної трансформації адміністративно-правового забезпечення інформаційної безпеки держави.*

Ключові слова: *адміністративно-правове забезпечення; кібероборона; інформаційна безпека; національна безпека; дезінформація; агенти впливу.*

Постановка проблеми та її актуальність. В умовах динамічного розвитку інформаційного суспільства безпекова ситуація у світі змінюється настільки швидко, що нормативно-правове та термінологічне забезпечення діяльності компетентних органів відповідальних за безпеку держави, в тому числі в інформаційній сфері, фактично значно запізнюється, що змушує їх діяти часом в умовах часткового правового вакууму.

Крім того, пандемія COVID-19 значно прискорила процеси, які до того розвивалися досить повільно. Зокрема, глобальна ізоляція населення за місцем проживання зумовила глибше занурення у віртуальний кіберпростір, у якому люди більше зазнають впливу інформаційного цунамі, причому переважно деструктивного характеру.

Тому, сьогодні назріла необхідність дослідження питання адміністративно-правового забезпечення інформаційної безпеки, від якого залежить ефективність реалізації адміністративно-правових заходів, у кінцевому підсумку – ступінь захищеності охоронюваних державних, громадських інтересів та інформаційних прав людини та громадянина.

Аналіз останніх досліджень і публікацій. Наукове осмислення концептуальних засад та окремих аспектів цієї проблеми здійснили в своїх роботах такі науковці, як: В.Б. Авер'янов, О.Ф. Андрійко, Ю.П. Битяк, В.Т. Білоус, Н.П. Бортник, М.П. Вавринчук, Т.О. Гаврилюк, В.П. Горбулін, Д.В. Дубов, Д.Г. Заброда, О.М. Музичук, В.К. Колпаков, Т.О. Коломоєць, О.В. Кузьменко, Р.А. Калюжний, І.О. Корецька, Д.М. Лук'янець, Н.Р. Нижник, О.І. Остапенко,

О.В. Олійник, В.М. Олуйко, І.Д. Пастух, Г.П. Ситник, І.М. Сопілко, В.О. Шамрай та інші.

Разом із тим, віддаючи належне важливості та науковій цінності наявних досліджень, значні зміни організаційно-правових основ у цій сфері вимагають подальшого наукового осмислення і аналізу питання формування концептуальних теоретико-правових засад адміністративно-правового забезпечення інформаційної безпеки в Україні.

Мета роботи – аналіз сучасного стану адміністративно-правового забезпечення інформаційної безпеки в Україні, напрацювання науково обґрунтованих пропозицій та рекомендацій із цього питання, спрямованих на подальше вдосконалення правозастосовної практики у цій сфері.

Виклад основного матеріалу. Серед науковців, які займалися дослідженням зазначеної проблематики, не існує єдиних поглядів щодо трансформації інформаційного законодавства України, що є логічним, зважаючи на складність та динаміку сучасних інформаційних процесів, які відбуваються в умовах становлення національної правової системи [14]. Але ні в кого не викликає сумніву, що сучасний стан українського інформаційного законодавства потребує вжиття термінових заходів щодо його удосконалення.

Так, В. Горбулін та М. Биченко вважають, що головною причиною невідповідності інформаційного законодавства України сучасним вимогам є несформованість у суспільній і науковій думці цілісного розуміння про інформаційну безпеку з позиції права та юридичної науки. Наразі, системно-функціональний підхід до формування права й нормотворчості є актуальним завданням, зумовленим відсутністю належної систематизації чинного інформаційного законодавства. У зв'язку з відсутністю методологічних основ інформаційної нормотворчості виникають труднощі об'єктивного і суб'єктивного характеру при формуванні системи нормативно-правового регулювання інформаційної безпеки [16]. Важливими засадами трансформації та розвитку інформаційного законодавства може стати адекватне сучасним умовам формування у свідомості науковців та правників повної картини інформаційної безпеки у всій повноті аспектів, зокрема психологічному, технічному та правовому.

Варто зазначити, що Закон України «Про інформацію» не містить визначення поняття «інформаційної безпеки», що є серйозним упущенням вітчизняного законодавця. У ст. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» надається визначення поняття «інформаційна безпека» – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [5].

Також, законодавство не містить чіткого переліку суб'єктів інформаційної безпеки, наразі в Законі України «Про інформацію» суб'єктами визначені: фізичні особи, юридичні особи, об'єднання громадян та суб'єкти владних повноважень [2]. Інший перелік визначений у Законі України «Про доступ до публічної інформації», відповідно до якого до суб'єктів віднесено: запитувачів інформації (фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень); розпорядників інформації; структурний підрозділ або відповідальну особу з питань запитів на інформацію розпорядників інформації [1].

Національне інформаційне законодавство характеризується декларативністю великої кількості норм без розкриття шляхів їх реалізації, що у свою чергу впливає на рівень реалізації норм права, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки. Крім того, до джерел загроз інформаційної безпеки України можна віднести: наявність великої кількості бланкетних (відсильних) норм права, значного масиву абстрактних, суб'єктивних понять, які потребують офіційного трактування чи чіткого визначення, а також відсутність закріплення ба-

зових дефініцій, таких як «інформаційна безпека» [15].

Слід зауважити, що у відносно прогресивній Доктрині інформаційної безпеки України (далі – Доктрина) введеній в дію Указом Президента України від 25 лютого 2017 року № 47/2017, також присутня низка недоліків. Так, у другому розділі Доктрини зазначено, що її метою є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни [7]. Але зазначена мета більш властива іншому документу, який визначатиме основні засади державної інформаційної політики, особливо її структуру та зміст. Наразі таким документом може стати Стратегія інформаційної безпеки, відпрацювання якої задекларовано в Стратегії національної безпеки України, введеної в дію Указом Президента України від 14 вересня 2020 року № 392/2020 [6].

Якщо вести мову за кібербезпеку, то варто зауважити, що не зважаючи на те, що Україна вимушена зіштовхуватися з російською агресією у кіберпросторі з початку гібридної війни в 2014 році, об'єктивно визнання кібероборони (складової оборони держави) відбулося в Україні лише в березні 2016 року після Указу Президента України про введення в дію Стратегію кібербезпеки України. В ній визначено, що «основу національної системи кібербезпеки становлять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи». В даному документі вперше для Міністерства оборони України і Генерального штабу Збройних Сил України були визначені нові задачі, серед яких підготовка держави до відбиття агресії в кіберпросторі і забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури [8].

Уже в жовтні 2017 року вступив у силу Закон України «Про основні засади забезпечення кібербезпеки України», в якому визначено дещо інший, аніж у Стратегії, за пріоритетністю і складу перелік основних суб'єктів національної системи кібербезпеки. Перш за все, Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, а далі не лише Міністерство оборони України, але й Генеральний штаб Збройних Сил України, а також розвідувальні органи і Національний банк України [4].

Втім, Закон про кібербезпеку уже чітко розподілив задачі між цими суб'єктами. Наприклад, Державній службі спеціального зв'язку та захисту інформації України довірений кіберзахист об'єктів критичної інфраструктури, а також попередження, виявлення і реагування на кіберінциденти і кібератаки та усування їх наслідків. Національна поліція займається захистом прав і свобод людини і громадянина, інтересів суспільства від злочинних посягань у кіберпросторі; здійснює заходи з попередження, виявлення, припинення і розкриття кіберзлочинів. Служба безпеки України проводить, між іншим, контррозвідувальні і оперативно-розшукові заходи, направлені на боротьбу з кібертероризмом і кібершпіонажем. Для Міністерства оборони України і Генерального штабу Збройних Сил України в рамках Стратегії кібербезпеки України основні задачі наведені без змін. А також передбачений кіберзахист критичної інформаційної інфраструктури в умовах правового режиму воєнного чи надзвичайного стану.

На жаль, у нормативно-правових актах залишаються невизначеними структури системи кібероборони держави, склад, функції і задачі суб'єктів її забезпечення, а також об'єкти кібероборони. Виконання основних задач із забезпечення кібероборони держави у відповідності із законодавством покладається на Міністерство оборони та Генеральний штаб Збройних Сил України, які повинні спільно приймати заходи щодо кібероборони для захисту суверенітету держави і забезпечення її обороноздатності, запобігання збройного конфлікту і відсічі збройної агресії. Ще більше питань виникає до формуван-

ня і діяльності підрозділів, які відповідають за інформаційно-психологічні тематичні операції.

Заходи із забезпечення кібероборони і нарощення кібероборонних можливостей держави поки відсутні в Стратегічному оборонному бюлетені і в державних програмах із розвитку Збройних Сил України, їх озброєння і воєнної техніки. А затверджені урядом щорічні плани заходів з реалізації Стратегії кібербезпеки України до 2020 року не містили заходи із забезпечення Міністерством оборони України та Генеральним штабом Збройних Сил України кібероборони держави. До речі, на 2019 і 2020 роки такі плани уряду взагалі не затверджувалися.

Іншим ризиком є відсутність реально напрацьованих механізмів координації діяльності в сфері інформаційної безпеки. Слід зазначити, що необхідність централізації діяльності, дієвих алгоритмів координації та контролю в тексті Доктрини інформаційної безпеки України задекларовані. Але, з іншого боку, механізми зазначеного не розкриті. Так, Рада національної безпеки і оборони України отримала завдання координації діяльності, не маючи при цьому необхідних повноважень та ресурсів, які притаманні центральним органам виконавчої влади [11]. Тут особливо необхідно налагодити на співпрацю і з громадським сектором (у Доктрині зазначене питання не достатньо розкрите), здатним до активних інформаційних заходів, що, до речі, визначено і в Законі «Про національну безпеку України» [3].

Ще більше питань виникає до формування і діяльності підрозділів, які відповідають за інформаційно-психологічні контенти операції і за активну протидію у цій сфері. Робота створеного в 2014 році і скасованого у 2019 році Міністерства інформаційної політики продемонструвала нездатність такої організації стати ефективним органом, тому представляється своєчасним і логічним створення таких профільних підрозділів у структурах розвідки, Служби безпеки України, Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, які повинні скласти силу інформаційної протидії і кібероборони.

Наразі, одним із дієвих кроків щодо протидії інформаційному впливу було створення у березні цього року Центру протидії дезінформації (далі – Центр) як робочого органу Ради національної безпеки і оборони України. Відповідне рішення Ради національної безпеки і оборони України було введено в дію Указом Президента України від 19 березня 2021 року № 106/2021 [9]. Як зазначив керівник Офісу президента України, на Центр покладаються завдання щодо аналізу інформаційних загроз, координації зусиль усіх державних органів і представників громадянського сектору з протидії дезінформації та ворожій пропаганді [13]. Тобто Центр, по суті, виконуватиме функції координатора з питань забезпечення інформаційної безпеки.

Варто зазначити, що запропонована конфігурація Центру дещо хаотична, але і при такій структурі можна досягти позитивних результатів, а розробка та введення в дію оновленої Стратегії інформаційної безпеки сприятиме цьому. Хоча досвід спостережень за розробкою проекту закону «Про протидію дезінформації» вселяє певну занепокоєність у тому, що керівництво країни все ж дослухатиметься до експертної спільноти.

Іншою важливою проблемою залишається підривна (деструктивна) діяльність агентів впливу. Сучасні зовнішні деструктивні впливи в інформаційній сфері та внутрішні руйнівні процеси, породжені, в тому числі, діяльністю агентів впливу (іноземних агентів) зумовлюють необхідність у прийнятті низки змін до Законів України: «Про громадські об'єднання», «Про благодійну діяльність та благодійні організації», «Про очищення влади», «Про інформацію» щодо протидії деструктивній діяльності агентів впливу в інформаційній сфері, передбачивши [12]: обов'язкове маркування усіх інформаційних матеріалів організацій, які виконують функції іноземного агента, незалежно від того, чи розповсюджується така інформація через друковані засоби масової інформації чи Інтернет; введення обмежень на діяльність засобів масової інформації з капіталом із держави-агресора, для перешкоджання розгортанню інформаційно-психологічних операцій в медіапросторі; при-

зупинення діяльності окремих неурядових організацій, що слугують платформою для внутрішньої дестабілізації. Також, наразі, відсутній механізм віднесення фізичних та юридичних осіб до агентів впливу (іноземних агентів). Як варіант можливо ввести «реєстр іноземних агентів» за зразком існуючих у США та Австралії.

Для України питання пошуку та протидії агентам впливу стоїть особливо гострим, формування достатньої нормативно-правової бази для притягнення таких осіб до відповідальності, механізмів їх чіткої ідентифікації та недопущення використання поняття «агент впливу» для обмеження свободи слова та думки і досі залишається невирішеним. Прийняття українського аналогу діючого в США з 1938 року Закону «Про реєстрацію іноземних агентів» було б цінною підмогою у боротьбі проти російського впливу в Україні [9, 17].

На превеликий жаль, незважаючи на швидкий розвиток інформаційного суспільства, серед інформаційного законодавства України зустрічаються і такі, які безнадійно застаріли. Як приклад можна навести прийнятий ще в 2007 році Верховною Радою України Закон «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки», а в 2013-му схвалену Кабінетом Міністрів Стратегію розвитку інформаційного суспільства в Україні, які за минулі роки не були застосовані на практиці, і зараз залишаються у статичному, незмінному стані.

З метою зменшення негативних наслідків для суспільства від деструктивних інформаційних впливів, особливо під час пандемії, необхідно провести корекцію інформаційного законодавства держави з урахуванням розглянутих вище особливостей.

Висновки. Основи інформаційного законодавства України у сфері інформаційної безпеки вже покладені, наразі чинна законодавча база потребує трансформації з урахуванням вимог та викликів сьогодення, що в цілому сприятиме зміцненню інформаційної безпеки України та підвищенню її міжнародного авторитету як демократичної і правової держави.

Отже, оцінка сучасного стану адміністративно-правового забезпечення інформаційної безпеки в Україні, в аспекті напрацювання науково обґрунтованих пропозицій з цього питання, актуалізувала необхідність сфокусувати увагу на таких першочергових заходах щодо трансформації інформаційного законодавства України:

– переглянути понятійно-категоріальну базу, доповнивши Закон України «Про інформацію» поняттям «інформаційна безпека», узгодивши невідповідності щодо переліку суб'єктів інформаційних відносин у Законах України «Про інформацію», «Про доступ до публічної інформації»;

– привести у відповідність нормативно-правові акти України різної юридичної сили, що стосуються сфери кібербезпеки щодо переліку основних суб'єктів національної системи кібербезпеки із зазначеним у Законі України «Про основні засади забезпечення кібербезпеки України»;

– визначити структуру системи кібероборони держави, склад, функції і задачі суб'єктів її забезпечення, а також об'єкти кібероборони у нормативно-правових актах;

– у зв'язку зі створенням Центру протидії дезінформації як координаційного органу, продовжити роботу щодо напрацювання та імплементації реальних механізмів координації діяльності у сфері інформаційної безпеки шляхом прийняття Закону України «Про дезінформацію»;

– прийняти низку змін до Законів України: «Про громадські об'єднання», «Про благодійну діяльність та благодійні організації», «Про очищення влади», «Про інформацію» шляхом законодавчого закріплення поняття «агент впливу», передбачивши чіткі механізми їх ідентифікації та протидії деструктивній діяльності агентів впливу в інформаційній сфері.

Наостанок слід зазначити, що у зв'язку зі швидким розвитком інформаційного суспільства адміністративно-правове забезпечення інформаційної безпеки держави потребує постійної трансформації. Тому, пошук шляхів ефективного подолання проблем, пов'язаних із необхідністю удосконалення адміністративно-правового забезпечення інформаційної безпеки в Україні, має ґрунтуватися насамперед на глибокому аналізі

всіх суспільно-політичних, економічних і соціальних процесів, які відбуваються в державі.

Література

1. Про доступ до публічної інформації: Закон України від 13 січ. 2011 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст 314.

2. Про інформацію: Закон України від 2 жовт. 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

3. Про національну безпеку України: Закон України від 21 чер. 2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

4. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

5. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09 січ. 2007 р. № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

6. Про рішення Ради національної безпеки і оборони України від 14 вер. 2020 р. «Про Стратегію національної безпеки України»: указ Президента України від 14 вер. 2020 р. № 392. *Офіційний вісник Президента України*. 2020. № 19. Ст. 926.

7. Про рішення Ради національної безпеки і оборони України від 29 груд. 2016 р. «Про Доктрину інформаційної безпеки України»: указ Президента України від 25 лют. 2017 р. № 47. *Офіційний вісник Президента України*. 2017. № 20. Ст. 554.

8. Про рішення Ради національної безпеки і оборони України від 27 січ. 2016 р. «Про Стратегію кібербезпеки України»: указ Президента України від 15 бер. 2016 р. № 96. *Офіційний вісник Президента України*. 2016. № 10. Ст. 198.

9. Про рішення Ради національної безпеки і оборони України від 11 бер. 2021 р. «Про створення Центру протидії дезінформації»: указ Президента України від 19 бер. 2021 р. № 106. *Урядовий кур'єр*. 2021. № 55.

10. Дубов Д.В., Корецька І.О. «В інтересах іншої держави...»: проблеми виявлення та протидії агентам впливу: аналіт. доп. Київ: НІСД, 2018. 48 с.

11. Візір Т.С. Адміністративно-правове регулювання забезпечення інформаційної безпеки в Україні: сучасний стан та перспективи вдосконалення. *Наука онлайн. Міжнародний електронний науковий журнал*. 2019. № 4. URL: https://nauka-online.com/ua/release/2019/4/.
DOI: https://doi.org/10.25313/2524-2695-2019-4

12. Калетнік В.В. Теоретичні аспекти удосконалення національного законодавства в контексті протидії деструктивній діяльності агентів впливу. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право».* Київ: НАУ, 2020. № 3(56). С. 81-88. DOI: https://doi.org/10.18372/2307-9061.56.14895

13. Керівником Центру протидії дезінформації призначено Поліну Лисенко. URL: https://ua.interfax.com.ua/news/general/734913.html

14. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навч. посіб. Ірпінь: Акад. ДПС України, 2000. 304 с.

15. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Право і суспільство*. 2012. № 3. С. 132-137.

16. Ситник Г.П., Олуйко В.М., Вавринчук М.П. Національна безпека України: теорія і практика: навч. посіб. Київ: Кондор, 2007. 616 с.

17. Foreign Agents Registration Act. URL: https://www.law.cornell.edu/uscode/text/ 22/chapter-11/subchapter-II

References

1. Pro dostup do publichnoi' informacii': Zakon Ukrai'ny vid 13 sich. 2011 r. № 2939-VI. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2011. № 32. St 314.

2. Pro informaciju: Zakon Ukrai'ny vid 2 zhovt. 1992 r. № 2657-XII. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 1992. № 48. St. 650.

3. Pro nacional'nu bezpeku Ukrai'ny: Zakon Ukrai'ny vid 21 cher. 2018 r. № 2469-VIII. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2018. № 31. St. 241.

4. Pro osnovni zasady zabezpechennja kiberbezpeky Ukrai'ny: Zakon Ukrai'ny vid 05 zhovt. 2017 r. № 2163-VIII. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2017. № 45. St. 403.

5. Pro osnovni zasady rozvytku informacijnogo suspil'stva v Ukrai'ni na 2007-2015 roky: Zakon Ukrai'ny vid 09 sich. 2007 r. № 537-V. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2007. № 12. St. 102.

6. Pro rishennja Rady nacional'noi' bezpeky i oborony Ukrai'ny vid 14 ver. 2020 r. «Pro Strategiju nacional'noi' bezpeky Ukrai'ny»: ukaz Prezydenta Ukrai'ny vid 14 ver. 2020 r. № 392. *Oficijnyj visnyk Prezydenta Ukrai'ny*. 2020. № 19. St. 926.

7. Pro rishennja Rady nacional'noi' bezpeky i oborony Ukrai'ny vid 29 grud. 2016 r. «Pro Doktrynu informacijnoi' bezpeky Ukrai'ny»: ukaz Prezydenta Ukrai'ny vid 25 ljut. 2017 r. № 47. *Oficijnyj visnyk Prezydenta Ukrai'ny*. 2017. № 20. St. 554.

8. Pro rishennja Rady nacional'noi' bezpeky i oborony Ukrai'ny vid 27 sich. 2016 r. «Pro Strategiju kiberbezpeky Ukrai'ny»: ukaz Prezydenta Ukrai'ny vid 15 ber. 2016 r. № 96. *Oficijnyj visnyk Prezydenta Ukrai'ny*. 2016. № 10. St. 198.

9. Pro rishennja Rady nacional'noi' bezpeky i oborony Ukrai'ny vid 11 ber. 2021 r. «Pro stvorennja Centru protydii' dezinformacii'»: ukaz Prezydenta Ukrai'ny vid 19 ber. 2021 r. № 106. *Urjadovyj kur'jer*. 2021. № 55.

10. Dubov D.V., Korec'ka I.O. «V interesah inshoi' derzhavy...»: problemy vyjavlennja ta protydii' agentam vplyvu: analit. dop. Kyi'v: NISD, 2018. 48 s.

11. Vizir T.S. Administratyvno-pravove reguljuvannja zabezpechennja informacijnoi' bezpeky v Ukrai'ni: suchasnyj stan ta perspektyvy vdoskonalennja. *Nauka onlajn. Mizhnarodnyj elektronnyj naukovyj zhurnal*. 2019. № 4. URL: https://nauka-online. com/ua/release/2019/4/

12. Kaletnik V.V. Teoretychni aspekty udoskonalennja nacional'nogo zakonodavstva v konteksti protydii' destruktyvnij dijal'nosti agentiv vplyvu. *Naukovi praci Nacional'nogo aviacijnogo universytetu. Serija: Jurydychnyj visnyk «Povitrjane i kosmichne pravo»*. Kyi'v: NAU, 2020. № 3(56). S. 81-88. DOI: 10.18372/2307-9061.56.14895

13. Kerivnykom Centru protydii' dezinformacii' pryznacheno Polinu Lysenko. URL: https://ua. interfax.com.ua/news/general/734913.html

14. Nyzhnyk N.R., Sytnyk G.P., Bilous V.T. Nacional'na bezpeka Ukrai'ny (metodologichni aspekty, stan i tendencii' rozvytku): navch. posib. Irpin': Akad. DPS Ukrai'ny, 2000. 304 s.

15. Olijnyk O.V. Normatyvno-pravove zabezpechennja informacijnoi' bezpeky v Ukrai'ni. *Pravo i suspil'stvo*. 2012. № 3. S. 132-137.

16. Sytnyk G.P., Olujko V.M., Vavrynchuk M.P. Nacional'na bezpeka Ukrai'ny: teorija i praktyka: navch. posib. Kyi'v: Kondor, 2007. 616 s.

17. Foreign Agents Registration Act. URL: https://www.law.cornell.edu/uscode/text/ 22/chapter-11/subchapter-II

V. Kaletnik

CURRENT STATE OF ADMINISTRATIVE AND LEGAL ENSURING OF INFORMATION SECURITY IN UKRAINE: THEORETICAL AND LEGAL ANALYSIS

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mail: human-rights@online.ua

Purpose: *analysis of the current state of administrative and legal ensuring of information security in Ukraine, development of scientifically sound proposals and recommendations on this issue.* ***Methods:*** *in the study, the author used methods of theoretical analysis and content analysis, monographic method, method of systematization to identify and specify the author's position within the studied issues. When preparing conclusions and recommendations based on the results of the study, the method of generalization was used.* ***Results:*** *the directions of increase of efficiency of administrative and legal ensuring of information security in Ukraine on the basis of realization of a complex of organizational and legal measures are defined. Emphasis is placed on the fact that the search for ways to effectively overcome the problems associated with the need to improve the administrative and legal support of information security in Ukraine should be based primarily on an in-depth analysis of all socio-political, economic and social processes in the country.* ***Discussion:*** *in the dynamic development of the information society, the security situation in the world is changing so fast that the legal and terminological support of the competent authorities responsible for state security, including in the information sphere, is significantly delayed, forcing them to act sometimes in a partial legal vacuum. In addition, the COVID-19 pandemic significantly accelerated processes that had previously developed rather slowly. Therefore, today there is a need to study the issue of administrative and legal ensuring of information security, which depends on the effectiveness of administrative and legal measures.*

Keywords: *administrative and legal ensuring; cyber defense; information security; national security; misinformation; agents of influence.*