МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Факультет права, публічного управління
та національної безпеки
Кафедра правознавства
Кваліфікаційна робота
на правах рукопису

Заріцький Олександр Юрійович

УДК 347.78(477)

КВАЛІФІКАЦІЙНА РОБОТА

Правові та організаційні основи протидії деструктивному інформаційному впливу в Україні: шляхи удосконалення

081 Право

Подається на здобуття освітнього ступеня «Магістр»

кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ О.Ю. Заріцький

Керівник роботи
Черниш Роман Федорович,
кандидат юридичних наук, доцент

Житомир – 2021

Висновок кафедри правознавства за результатами попереднього захисту:

_____

Протокол засідання кафедри _____ № __ від «___»_____20__ р.

Завідувач кафедри правознавства

к.ю.н., доцент _____ Р. Д. Ляшенко
(підпис)

«___» _____ 2021 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти Заріцький Олександр Юрійович захистив кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою_____
за шкалою ECTS _____
за національною шкалою _____

Секретар ЕК

_____ Т.П. Святогор
(підпис)

АНОТАЦІЯ

Заріцький О.Ю. Правові та організаційні основи протидії деструктивному інформаційному впливу в Україні: шляхи удосконалення. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістра за спеціальністю 081 Право. Поліський національний університет, Житомир, 2021.

В кваліфікаційній роботі охарактеризовано розвиток і організацію нормативно-правового регулювання інформаційної безпеки України. Досліджено класифікацію загроз інформаційній безпеці. Визначено суб'єктів забезпечення інформаційної безпеки. Обґрунтовано пріоритети розвитку правових основ державної політики України у сфері інформаційної безпеки. Визначено шляхи удосконалення механізму протидії сучасним загрозам деструктивного інформаційного впливу в умовах гібридної війни проти України.

Ключові слова: гібридна війна, державна інформаційна політика, інформаційна безпека, інформаційний захист, інфраструктура, негативний вплив, суб'єкти державної влади.

SUMMARY

Zaritskyi O. "Legal and organizational bases of counteraction to destructive information influence in Ukraine: ways of improvement" - Manuscript.

Master's work for Master "Master" specialty 081 Law. Polissya National University, Zhytomyr, 2021.

The qualification work describes the development and organization of legal regulation of information security of Ukraine. The classification of information security threats has been studied. The subjects of information security have been identified. The priorities of development of legal bases of the state policy of Ukraine in the field of information security are substantiated. Ways to improve the mechanism of counteraction to modern threats of destructive information influence in the conditions of hybrid war against Ukraine are determined.

Key words: hybrid war, state information policy, information security, information protection, infrastructure, negative impact, subjects of state power.

ЗМІСТ

ВСТУП

Актуальність дослідження. Сучасні умови глобальних та регіональних інформаційних протистоянь, руйнівних комунікативних впливів, зіткнення різноспрямованих державних інформаційних інтересів, розповсюдження інформаційної агресії, захист інформаційного простору держав та гарантування інформаційної безпеки обумовлюють пріоритетність стратегічних завдань сучасних держав у системі глобальних інформаційних відносин. Збереження інформаційного суверенітету, створення результативної і дієвої системи безпеки в сфері інформації виступає актуальною проблемою і для нашої країни, яка часто стає об'єктом зовнішніх інформаційних експансійних впливів, технологій, що маніпулюють суспільною свідомістю, а також руйнівного інформаційного вторгнення [18]. В таких умовах захист українського інформаційного простору від негативних впливів інформаційно-психологічного характеру, операцій та інформаційних війн, гарантування безпеки у цій сфері та інформаційного суверенітету набувають особливого значення і трансформуються у фактори збереження української національної ідентичності та функціонування України як суверенної та незалежної держави. Важливість зазначених питань обумовила вибір теми наукового дослідження та свідчить про її актуальність.

Інформаційну безпеку та питання захисту інформаційного простору України досліджували багато науковців. Зокрема, питання інформаційної безпеки розглянуті у працях В. Горбуліна [2], М. Левицької [13], В. Ліпкана [14-15], А. Прозорова [32], О. Тихомирова [35], Т. Ткачука [36-37], Р. Хмелевського [39] та інших. У працях цих науковців інформаційна безпека представлена невід'ємним складовим елементом національної безпеки. Проте, детального дослідження заслуговують питання чіткого окреслення інформаційних загроз, дослідження їхніх джерел, а також визначення та обґрунтування шляхів удосконалення протидії деструктивним інформаційним впливам.

Мета і завдання дослідження. Метою роботи є всебічне дослідження правових та організаційних основ протидії деструктивному інформаційному

впливу в Україні та розробка пропозицій по удосконаленню захисту національного інформаційного простору.

Завдання дослідження:

- охарактеризувати розвиток і організацію нормативно-правового регулювання інформаційної безпеки України;

- дослідити класифікацію загроз інформаційній безпеці України;

- визначити суб'єктів забезпечення інформаційної безпеки України;

- обґрунтувати пріоритети розвитку правових основ державної політики України у сфері інформаційної безпеки;

- визначити шляхи удосконалення механізму протидії сучасним загрозам деструктивного інформаційного впливу в умовах гібридної війни проти України.

Об'єкт дослідження. Процес забезпечення інформаційної безпеки України.

Предмет дослідження. Шляхи удосконалення протидії деструктивному інформаційному впливу в Україні.

Методи дослідження. Методологічну основу складає діалектичний метод пізнання суспільних явищ і процесів. В роботі використовуються також загальноприйняті в юридичній науці методи наукового пізнання: формально-юридичний (підрозділи 1.1; 1.2; 1.3; 2.1), системно-структурний (1.2; 1.3; 2.2), порівняльно-правовий (2.1; 2.2), історичний та інші загальнонаукові та спеціальні методи.

Практичне значення одержаних результатів: Узагальнено механізм протидії деструктивному інформаційному впливу в Україні, запропоновано шляхи його удосконалення, які можуть бути використані у правозастосовній діяльності відповідними органами. Отримані результати дослідження можуть бути застосовані при викладанні курсу «Інформаційної безпеки України» в вищих навчальних закладах.

Апробація результатів дослідження. Окремі результати та висновки, отримані в ході проведеного дослідження, були викладені в науковій фаховій статті у виданні, що індексується в Google Scholar, у міжнародній реферативній

базі даних «Index Copernicus International» (Польща). (Черниш Р.Ф., Ігнатюк М.В., Заріцький О.Ю. Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти. Юридичний науковий електронний журнал. №11. 2021.

Структура та обсяг роботи. Структура роботи відповідає завданням дослідження. Магістерська робота виконана на 39 сторінках, містить вступ, два розділи і п’ять підрозділів, висновки до кожного розділу, загальні висновки, список використаних літературних джерел з 42 найменувань.

РОЗДІЛ 1
ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

1.1. Розвиток і організація нормативно-правового регулювання інформаційної безпеки України

Інформаційна безпека виступає інтегрованим компонентом національної безпеки і позиціонується як пріоритетна функція держави. З одного боку, інформаційна безпека спрямована на забезпечення якісного всебічного інформування громадян та необмеженого доступу до різних інформаційних джерел, а з іншого – передбачає контроль за непоширенням дезінформації, сприяння суспільній цілісності, охорону інформаційного суверенітету, протидію негативним інформаційним впливам пропагандистського та психологічного характеру, а також захист державного інформаційного простору від різних маніпуляцій дій та інформаційних війн. Розв'язання комплексної проблеми інформаційної безпеки надасть можливість, по-перше, захистити суспільні і державні інтереси, по-друге, гарантувати права громадян на користування інформацією всебічного, об'єктивного та якісного характеру.

Вітчизняний дослідник Б. Кормич виокремлює два аспекти характеристики інформаційної безпеки відносно поняття національної безпеки. З одного боку, інформаційна безпека трактується як самостійний компонент національної безпеки будь-якої держави, а з іншого – інтегрований складовий елемент будь-якої іншої безпеки: військової, економічної, політичної тощо. На думку вченого, оптимальним є таке визначення інформаційної безпеки – це такий стан захищеності життєво важливих інтересів особистості, суспільства і країни, за якого мінімізується завдання збитків через неповноту, невчасність і невідповідність інформації, негативний інформаційний вплив, негативні наслідки реалізації інформаційних технологій, а також через заборонене розповсюдження інформації [11].

Забезпеченню інформаційної безпеки України, безпеки державних інтересів в інформаційному напрямку сприятиме пріоритетний розвиток відповідної системи нормативно-правового забезпечення протидії загрозам цих інтересів та впорядкування правотворчого процесу в сфері використання та розповсюдження інформації.

Необхідність такого розвитку системи нормативно-правового забезпечення обумовлена певними факторами. По-перше, в умовах функціонування правової держави та громадянського суспільства основні функції органів державної влади, на які покладено основну відповідальність за національну безпеку, мають регулюватися визначеними правовими нормами, спрямованими на забезпечення громадянських конституційних прав і свобод. Правотворчість у цьому напрямку націлена на нормативне закріплення завдань протидії загрозам національної безпеки України, засобів та методів їх виконання, забезпечення погоджувальної політики владних органів. По-друге, курс України на інтеграцію в міжнародне співтовариство істотно розширює можливості закріплення державної інформаційної безпеки шляхом участі в розвитку міжнародно-правових норм у цій сфері, формування міжнародної системи забезпечення інформаційної безпеки як в світовому масштабі, так і в рамках кожної окремої країни. По-третє, реалізація гарантій громадянських прав та свобод, захисту державних інтересів нашої країни передбачає суттєве збільшення ролі владних органів в регулюванні відповідних суспільних відносин, присутність прозорої та зрозумілої державної політики у цьому напрямку [28].

Ю. Максименко під нормативно-правовим регулюванням інформаційної безпеки України визначає таку форму владного правового впливу на інформаційні відносини у суспільстві, яка реалізується державою з метою їх упорядкування, закріплення і забезпечення.

Також вчений підкреслює, що у сьогоднішніх умовах існування українського суспільства одним із найважливіших напрямів стратегії адміністративно-правового забезпечення інформаційної безпеки нашої країни

виступає аналіз та удосконалення нормативно-правового регулювання в цьому напрямку [17].

Н. Новицька зазначає, що система правового регулювання інформаційної безпеки представляє собою масив правових норм, які регулюють відносини в цій області, правові відносини, які формуються на підставі застосування правових норм, та відповідні акти правозастосовного характеру.

Правові норми формують собою базу забезпечення інформаційної безпеки і обумовлюють ефективність діяльності держави, суспільства та окремих громадян в напрямку захисту національних інтересів України в сфері споживання і використання інформації. До складу такої нормативно-правової бази відносяться і норми міжнародних договорів України, закони України, акти Президента України, постанови уряду, нормативно-правові документи органів державної влади, які спрямовані на регулювання відносин у досліджуваному напрямку [21].

З урахуванням різноманітності нормативно-правових документів, спрямованих на регулювання суспільних відносин в напрямку інформаційної безпеки України, доцільно охарактеризувати ключові з них. Так, нормативно-правове регулювання інформаційної безпеки України здійснюється:

- Конституцією України, прийнятою 28.06.1996р.;
- Законами України: «Про інформацію» від 02.10.1992 р. № 2657-XII;
- «Про основи національної безпеки України» від 19.06.2003р. №964-IV;
- «Про науково-технічну інформацію» від 25.06.1993р. №3322-XII;
- «Про Національну програму інформатизації» від 04.02.1998 №74/98-ВР;
- «Про поштовий зв'язок» від 04.10.2001р. №2759-III та іншими базовими законами України;
- Доктриною інформаційної безпеки України, затвердженою Указом Президента України «Про рішення Ради національної безпеки і оборони України від 29.12.2016р. «Про Доктрину інформаційної безпеки України» [30].

Наведені нормативно-правові документи спрямовані на регулювання питань забезпечення інформаційної безпеки, інформаційного захисту, охорони

та захисту державної таємниці, конфіденційних інформаційних відомостей, інформаційних ресурсів та ін. [37].

Сучасні автори підкреслюють кількісний пріоритет нормативних правових документів, націлених на врегулювання інформаційно-технічної безпеки відносно психологічної та інформаційної безпеки в площині прав та свобод громадян, що викликано, на думку А. Прозорова, стрімким розвитком інформаційних технологій, а отже, важливістю оперативного реагування на зміни існуючих стандартів у цьому напрямку [41].

Ключовим недоліком нормативно-правового регулювання інформаційної безпеки в нашій країні представляється його розгалуження через велику кількість нормативно-правових документів різної юридичної сили. Дуже часто виникає ситуація, коли важливі і нагальні питання нормативно вирішуються з допомогою підзаконних нормативно-правових актів. Також важливим недоліком в результативному забезпеченні інформаційної безпеки України постає неузгодженість нормативно-правових документів як між собою, так і з положеннями діючої Конституції [41].

Характерною рисою українського інформаційного законодавства виступає декларативність багатьох юридичних норм без зазначення шляхів їх реалізації, що обумовлює невисокий рівень ефективності їх застосування у напрямку регулювання суспільних відносин щодо забезпечення інформаційної безпеки. До того ж, присутність великої кількості бланкетних або відсильних правових норм, певного масиву абстрактних або суб’єктивних понять, яким необхідне офіційне тлумачення або чіткіше трактування, а також відсутність закріплення фундаментальних основних дефініцій виступають джерелами загроз українській інформаційній безпеці. Дослідження нормативно-правової бази в області забезпечення інформаційної безпеки нашої країни свідчить про необхідність удосконалення відповідного законодавства [32].

Питання забезпечення державних інтересів і державної безпеки в сфері отримання і використання інформації на сьогоднішній день не втрачають своєї актуальності. Інформаційна безпека забезпечується здійсненням єдиної

державної політики в напрямку національної інформаційної безпеки, системою економічних, політичних та організаційних заходів у відповідності з існуючими і можливими загрозами та небезпеками національних інтересів (особистих, суспільних та державних) в інформаційній сфері.

Для досягнення і підтримання необхідного рівня національної безпеки в інформаційному напрямку розробляється система юридичних норм, спрямованих на регулювання відносини в інформаційній сфері, виокремлюються ключові напрями діяльності органів державного управління, засновуються або реорганізовуються органи та сили забезпечення інформаційної безпеки, формується механізм контролю за їхньою діяльністю [41].

Заслуговує на увагу точка зору В. Ліпкана, який зазначає, що робота системи забезпечення інформаційної безпеки не може обмежуватися значною кількістю нормативно-правових документів. Це не свідчить про закінченість процесу формування ключових елементів системи забезпечення інформаційної безпеки. В цьому контексті доцільно також враховувати загальну несформованість системи забезпечення національної безпеки, а також невизначеність державної інформаційної політики. До того ж, недосконаліть нормативно-правового регулювання досліджуваних процесів негативно впливає і на якість державного управління у вказаній сфері [15].

Таким чином, недоліки нормативно-правової бази щодо врегулювання правових відносин в інформаційній сфері значно ускладнюють настання якісних змін у цьому секторі суспільних відносин. Сьогодні через відсутність чітко визначених і взаємопов’язаних заходів та теоретичних розробок щодо забезпечення інформаційної безпеки країни виникає ціла низка перешкод на шляху повноцінної реалізації державою її обов’язку по забезпеченню інформаційної безпеки як невід’ємного компонента національної безпеки. Ефективну систему протидії правопорушенням в інформаційній сфері може створити тільки розробка і реалізація обґрунтованої державної політики [41].

1.2. Класифікація загроз інформаційній безпеці України

Про складність і багатошаровість системи загроз національній безпеці нашої країни свідчить наявність великої кількості критеріїв, за якими вони можуть бути класифіковані. Наприклад, з політологічної точки зору загрози національній безпеці можуть бути розподілені таким чином:

- відповідно до місця знаходження джерела – зовнішні та внутрішні;
- відповідно до масштабів імовірних наслідків – загальнонаціональні, регіональні, локальні, одиничні;
- відповідно до рівня сформованості – потенційні або реальні;
- відповідно до рівня суб'єктивного сприйняття – завищені, занижені, мінімальні, умовні, адекватні;
- відповідно до характеру створення – загрози природного, техногенного або соціального характеру;
- відповідно до сфери життєдіяльності – загрози в сфері економіки, політики, оборони, екології, культури, міжнародних відносин, а також інформаційній, науково-технічній, соціальній та духовній сферах [37] тощо.

Відповідно до норм Закону України «Про основи національної безпеки України» [30], система існуючих та імовірних загроз виступає основою для виокремлення в рамках національної безпеки (відповідно до джерел, характеру і особливостей загроз) зовнішньополітичної, внутрішньополітичної, державної, воєнної, економічної, соціальної, гуманітарної, екологічної та інформаційної безпеки, а також безпеки державного кордону [41].

Проте, враховуючи визначення національної безпеки, на якому побудований вказаний закон, перелік областей і напрямків, в яких можуть проявися загрози національній безпеці, не є вичерпним. Так, з урахуванням джерел і середовища виникнення загроз національним інтересам, їх традиційно поділяють на зовнішні та внутрішні [2]. Проте сучасні обставини свідчать про певну умовність такого поділу, викликану тим, що загрози зовнішнього

характеру можуть мати внутрішні джерела, а також поєднуватися із загрозами внутрішніми.

Як вже зазначалося, всі компоненти структури національної безпеки є взаємопов'язаними, проте доцільно зауважити, що деякі види безпеки є не тільки самостійними, але й такими, яким притаманні відповідні виміри в інших напрямках життєдіяльності суспільства, створюючи фундамент забезпечення їх безпеки. Серед таких «інтегративних» видів, на думку С. Пирожкова та О. Майбороди, важливе місце посідає інформаційна безпека.

Відповідно, загрози інформаційного характеру можуть бути спрямовані до різноманітних елементів державної безпеки, але їх негативна дія завжди опосередковуватиметься нанесенням шкоди інформаційній безпеці країни. Наприклад, економічна безпека в існуючих умовах інформаційно-мережевої економіки в першу чергу залежить від безпеки інформаційного характеру, тому що ключовим ресурсом розвитку виробництва в таких обставинах виступає інформаційний продукт [40].

Швидке формування і стрімкий розвиток глобального інформаційного простору, розповсюдженість інформаційно-комунікаційних технологій у всіх сферах життєдіяльності зумовили відповідний розвиток інформаційного суспільства в Україні та виведення на перший план проблем інформаційної безпеки. В таких обставинах одним із ключових напрямків забезпечення інформаційної безпеки державою представлено створення комплексної системи оцінки загроз інформаційного характеру та відповідного реагування [29].

Загрози національній безпеці України в інформаційній сфері можуть бути представлені у вигляді сукупності умов та факторів, які становлять небезпеку життєво необхідним державним, суспільним та особистим інтересам у зв'язку з імовірністю негативного інформаційного впливу на свідомість та поведінку громадян країни, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру. З урахуванням наведеного визначення, система загроз інформаційній безпеці може включати такі категорії: загрози безпеці інформації та відповідної інфраструктури; загрози безпеці суб'єктів інформаційного

напрямку та соціальних зв'язків між ними від дій (або впливів) інформаційного характеру; загрози існуючому і законному порядку реалізації прав та інтересів суб'єктів інформаційної площини [24].

Серед найважливіших характеристик загроз інформаційній безпеці країни доцільно звернути увагу на наступні:

- вибірковість – означає направленість загрози на завдання шкоди конкретним визначеним характеристикам об'єкта безпеки;

- передбачуваність – мається на увазі присутність ознак виникнення загрози, що надає можливість заздалегідь прогнозувати імовірність виникнення загрози та виокремлювати конкретні об'єкти, на які вона буде націлена;

- шкідливість – означає можливість заподіяти об'єкту безпеки шкоди різного ступеня тяжкості [4].

Закон України «Про основи національної безпеки України» визначає однією з ключових загроз інформаційній безпеці дії (спроби), спрямовані на маніпулювання суспільною свідомістю, зокрема, шляхом розповсюдження недостовірних, неповних або упереджених інформаційних даних [30]. Доктрина інформаційної безпеки України (2016р.) виокремлює наступні загрози інформаційній безпеці держави: розповсюдження у світовому інформаційному просторі спотвореної, недостовірної та упередженої інформації, що шкодить державним інтересам; зовнішні інформаційні впливи деструктивного характеру на суспільну свідомість за допомогою ЗМІ та мережі Інтернет; інформаційні впливи деструктивного характеру, направлені на підрив конституційного устрою, суверенітету, територіальної єдності та недоторканності держави; демонстрація сепаратистських поглядів в ЗМІ або мережі Інтернет за ознаками етнічної, мовної, релігійної належності [5].

Вітчизняна дослідниця Р. Марутян найвагомішою загрозою національній безпеці України в інформаційному напрямку визначає здійснення іноземними країнами негативного впливу інформаційно-психологічного характеру на суспільну свідомість українських громадян та світову громадськість шляхом реалізації інформаційних акцій та кампаній, специфічних інформаційних

операцій. Це здійснюється через систематичне розповсюдження викривлених, неповних або необ'єктивних відомостей про Україну та притаманні їй політичні процеси. Усе це має політичну та економічну основу, тому здійснює вплив на зовнішню та внутрішню державну політику, а також погіршує її міжнародний імідж. Мета подібних інформаційних операцій полягає у забезпеченні своїх національних інтересів інших країн [19].

На думку У. Ільницької, сукупність загроз національній безпеці України в інформаційному напрямку формується наступними: виявлення обмеження свободи слова та доступу громадян до інформації; перекручення, спотворення, блокування, приховування, упереджене та суб'єктивне відображення інформації; протизаконне її розповсюдження; відкриті неправдиві інформаційні дані; інформаційне завойовування з боку інших країн та руйнувальне інформаційне вторгнення в державний інформаційний простір, коли держави з більшим інформаційним потенціалом використовують можливість посилити свій вплив на населення менш могутньої країни; створення і функціонування у державному інформаційному просторі неконтрольованих інформаційних потоків; розповсюдження через засоби масової інформації культу насильства, жорстокості; неспішність входження України в інформаційний простір світового масштабу; нерозважливість національної інформаційної політики та відсутність важливої інфраструктури в інформаційній площині; розповсюдження дезінформації через Інтернет [9].

Р. Хмелевський зазначає, що навіть розгорнуті переліки загроз не можуть бути вичерпними та стабільними. Це пояснюється тим, що джерела загроз можуть бути різноманітними: людина, технічні засоби, моделі, алгоритми, програмні та технологічні схеми обробки, зовнішнє оточення тощо [39].

Отже, технічний аспект не є центральним у структурі інформаційної безпеки. З урахуванням наведених класифікацій, доцільно забезпечувати не тільки безпеку інформаційних даних від знищення, спотворення або блокування, але й загальну інформаційну безпеку суспільства.

1.3. Суб’єкти забезпечення інформаційної безпеки України

Особистісна, суспільна та державна безпека, в тому числі й інформаційна, як складне і багаторівневе явище, може одночасно характеризуватися як процес та показник стану реалізації державних інтересів. При цьому основними принципами забезпечення інформаційної безпеки виступають:

- додержування і захист прав і свобод людини і громадянина;
- законність;
- системний і комплексний характер застосування владними органами держави заходів забезпечення безпеки;
- пріоритетність попереджувальних заходів при забезпеченні безпеки;
- взаємодія органів державної влади з міжнародними організаціями, громадянсько-суспільними інститутами, громадянами та іншими суб’єктами для забезпечення національної безпеки інформаційного характеру.

Реалізація наведених принципів можлива за умови формування системи забезпечення державної безпеки, невід’ємним компонентом якої виступає система забезпечення інформаційної безпеки. Важливу роль в ефективній організації системи забезпечення національної інформаційної безпеки відіграє її суб’єктний склад, сфера повноважень суб’єктів забезпечення інформаційної безпеки та відповідна організація взаємодії між ними [20].

Система забезпечення інформаційної безпеки як компонент системи забезпечення державної безпеки характеризується відповідними силами та засобами. В цьому контексті сили доцільно представити як суб’єктний склад системи забезпечення інформаційної безпеки, а засоби – як технології, а також технічні, програмні, лінгвістичні, юридичні, організаційні засоби, зокрема, телекомунікаційні канали, які використовуються для збирання, формування, аналізу, передачі або прийому інформаційних даних щодо стану державної безпеки та застосування заходів, направлених на її посилення [41].

В сучасних обставинах розвитку інформаційного суспільства дотримання інформаційної безпеки представляється функцією кожного з суб’єктів

інформаційної сфери. При цьому синергетичні особливості інформаційної безпеки пояснюють наявність певного дуалізму: кожен суб'єкт може одночасно бути об'єктом інформаційної безпеки, а з другого боку – джерелом імовірних і реальних загроз або каналом їх розповсюдження. Саме тому ефективність забезпечення інформаційної безпеки залежить від можливостей не тільки спеціально призначених для цього державних організацій, але й кожного суб'єкта інформаційних відносин стосовно свого самозахисту в інформаційній сфері. В той же час, держава характеризується особливою позицією серед суб'єктів забезпечення інформаційної безпеки, адже, як зазначає О. Тихомиров, це єдиний суб'єкт, потенціал якого, поряд з економічними, політичними та ідеологічними засобами опосередкованого впливу, містить також можливості прямої управлінської дії, спрямованої на врегулювання інформаційних відносин за допомогою юридичних засобів [35].

З урахуванням положень ст.17 Конституції України [10], забезпечення інформаційної безпеки віднесено до найважливіших функцій держави нарівні із захистом українського суверенітету та територіальної цілісності. Діяльність держави у цьому напрямку здійснюється через відповідні владні органи. Так, визначено коло суб'єктів, які відповідають за забезпечення державної безпеки та здійснення комплексу інших заходів аналогічного спрямування. До цих суб'єктів належать військові формування та правоохоронні державні органи, зміст і порядок функціонування яких визначені в законодавчому порядку.

У відповідності з положеннями ст.12 Закону України «Про національну безпеку України» [30], сектор національної безпеки і оборони формують чотири взаємопов'язані елементи: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та їх об'єднання, які можуть у добровільному порядку брати участь у забезпеченні безпеки держави. Функції та компетенція елементів сектору безпеки і оборони встановлюються вітчизняним законодавством.

Склад сектору безпеки і оборони формують: Міністерство оборони України, Збройні сили України, Державна спеціальна служба транспорту, Міністерство внутрішніх справ України, Національна гвардія України,

Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Управління державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, органи розвідки, центральний орган виконавчої влади, діяльність якого спрямована на формування та реалізацію державної військово-промислової політики. Інші органи державної влади та органи місцевого самоврядування реалізують власні функції щодо забезпечення безпеки держави у безпосередній взаємодії з органами, які включені до складу сектору безпеки і оборони [30; 41].

Серед ключових функцій суб'єктів забезпечення державної безпеки, наведених у ст.10 досліджуваного Закону, доцільно звернути увагу саме на ті, які безпосередньо спрямовані на забезпечення інформаційної безпеки:

- розробка та періодичне уточнення державних Стратегії національної безпеки та Воєнної доктрини, інших програмних і стратегічних документів у сфері національної безпеки, планування і реалізація відповідних заходів, спрямованих на протидію чи нейтралізацію загроз українським інтересам;

- формування нормативно-правових документів, необхідних для стабільного та результативного функціонування системи національної безпеки;

- постійне спостереження за впливом на державну безпеку процесів, які відбуваються в соціальному, науково-технологічному, інформаційному секторах суспільства; прогнозування імовірних змін в таких процесах та потенційних загроз національній безпеці;

- прогнозування, визначення та оцінювання імовірних загроз, дестабілізуючих факторів, причин їх формування та наслідків вираження;

- розробка науково обґрунтованих пропозицій і рекомендацій стосовно прийняття управлінських рішень для забезпечення захисту державних інтересів; запобігання та ліквідація впливу загроз і дестабілізуючих факторів на інтереси країни;

- оцінювання ефективності вжитих заходів, спрямованих на забезпечення національної безпеки, та визначення витрат на їх реалізацію [8].

Особливості здійснення державою функцій забезпечення інформаційної безпеки полягають у тому, що діяльність кожного державного органу здійснюється шляхом використання інформаційної інфраструктури суспільства, формування та споживання ресурсів інформаційного характеру, встановлення відносин із громадянами. Тому державні органи як власники таких ресурсів і відповідної інфраструктури повинні застосовувати спектр заходів, спрямованих на забезпечення збереження ресурсів і безпеки роботи систем інформації, телекомунікації, управління та зв'язку [27].

Доктриною інформаційної безпеки України (2016р.) масив функцій, спрямованих на забезпечення безпеки у сфері отримання і використання інформації, покладено на такі державні органи: Раду національної безпеки і оборони України, Кабінет Міністрів України, відповідні міністерства (зокрема, інформаційної політики, закордонних справ, оборони), Службу безпеки та Державну службу спеціального зв'язку та захисту інформації України, а також органи розвідки [5].

В. Ліпкан доводить, що з урахуванням функціональності суб'єктів система забезпечення інформаційної безпеки формується зі стратегічного, тактичного та оперативного рівнів управління безпекою. До суб'єктів вищого, стратегічного, рівня дослідник відносить Раду національної безпеки і оборони України та Кабінет Міністрів України, відповідно, суб'єктами нижчого, тактичного, рівня виступають центральні органи виконавчої влади, а на оперативному рівні розташовані місцеві органи виконавчої влади [14].

Вітчизняний вчений О. Олійник також пропонує розподілити суб'єктний склад забезпечення інформаційної безпеки за певними рівнями, кожен з яких відповідає можливостям суб'єктів влади по організаційно-функціональному забезпеченню безпеки з урахуванням їх позиціонування в українській Конституції:

перший рівень, загальнодержавний – Верховна Рада, Президент, Рада національної безпеки і оборони, Кабінет Міністрів України;

другий рівень – представлений суб'єктами, які виконують спеціальні повноваження: центральні й місцеві органи виконавчої влади, інші органи державної влади, також судові органи і прокуратура;

третій рівень – включає суб'єктів, функціонування яких пов'язане із застосуванням тих електронних, телекомунікаційних засобів та інформаційних технологій, виведення яких з ладу може мати тяжкі наслідки на особистому, суспільному чи державному рівнях: підприємства, установи й організації ключових важливих інфраструктур;

четвертий рівень: громадяни та громадські об'єднання, а також засоби масової інформації державної та приватної власності [23].

Українська авторка М. Левицька пропонує схожу класифікацію суб'єктів, що можуть забезпечувати інформаційну безпеку:

суб'єкти, функціонування яких безпосередньо спрямоване на реалізацію завдань забезпечення безпеки, як комплексно, так і окремо: Рада національної безпеки і оборони України, правоохоронні органи, інші державні виконавчі органи спеціального спрямування;

суб'єкти, для яких ця діяльність ключова, проте це не єдиний її напрямок: вищі органи законодавчої, виконавчої та державної влади;

суб'єкти, які беруть участь у забезпеченні інформаційної безпеки, але за рамками власних основних функцій: різноманітні організації держави або громадськості [13].

Таким чином, з урахуванням комплексного характеру сучасних загроз інформаційній безпеці України та специфіки функціональних завдань, суб'єктний склад системи забезпечення безпеки може бути представлений спеціально уповноваженими суб'єктами, для яких це виступатиме головним напрямом діяльності, та суб'єктами, які можуть брати участь у її забезпеченні.

ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ

Перший розділ дослідження присвячено організаційно-правовим аспектам забезпечення інформаційної безпеки в Україні.

Дослідження розвитку і організації нормативно-правового регулювання інформаційної безпеки України дозволило зробити висновок, що в сучасних умовах інформаційних протистоянь національний інформаційний простір України представляється недостатньо захищеним від негативних інформаційно-психологічних впливів і загроз внутрішнього і зовнішнього характеру. Тому захист інформаційного суверенітету, формування потужної та результативної системи інформаційної безпеки нашої країни, розробка ефективних стратегій і тактик протидії інформаційним загрозам повинні бути пріоритетними завданнями органів державної влади та недержавних інститутів.

Загрози національній безпеці України в інформаційній сфері можуть бути представлені у вигляді сукупності умов та факторів, які становлять небезпеку життєво необхідним державним, суспільним та особистісним інтересам у зв'язку з імовірністю негативної інформаційної впливової дії на свідомість та поведінку громадян країни, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру. Аналіз існуючих класифікацій загроз інформаційній безпеці України свідчить про відсутність єдиного усталеного підходу до виділення їх окремих видів, кожен з дослідників може застосовувати певні суб'єктивні критерії, тому їх перелік не буде вичерпним.

Серед суб'єктів забезпечення інформаційної безпеки України доцільно виокремлювати спеціально уповноважені державні органи, для яких забезпечення безпеки виступатиме ключовим завданням і напрямом діяльності, та суб'єктів, які можуть брати участь у її забезпеченні.

РОЗДІЛ 2
ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: СУЧАСНІ ВИКЛИКИ ТА МЕХАНІЗМИ ПРОТИДІЇ НЕГАТИВНИМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВАМ

2.1. Пріоритети розвитку правових основ державної політики України у сфері інформаційної безпеки

В сучасних умовах глобальних суспільних перетворень і формування єдиного світового інформаційного простору в системі державної безпеки країн ключова роль належить саме інформаційній безпеці. Так, на думку вітчизняного дослідника А. Кузьменка, сучасні інформаційно-комунікаційні технології за можливостями і масштабом свого впливу на політику, економіку, ідеологію та інші аспекти громадського життя мають більш вирішальний та всеохоплюючий характер. Це свідчить про важливість забезпечення інформаційної безпеки як напрямку діяльності кожної з існуючих в країні владних структур [12].

Український вчений В. Пилипчук звертає увагу на важливості досягнення максимально можливої ефективності державної інформаційної політики з метою забезпечення національної безпеки. Ефективність державної інформаційної безпеки, на думку вченого, має забезпечуватися:

- формуванням науково обґрунтованої державної політики та стратегії в сфері отримання і використання інформації;

- здійсненням неперервного спостереження за наявністю актуальних загроз інформаційній безпеці держави;

- визначенням дієвих заходів для забезпечення безпеки в усіх її напрямках, зокрема, захисту від загроз інформаційного характеру та реалізації права громадян на отримання і користування правдивою інформацією [25].

До основних факторів і чинників, які можуть підвищувати або знижувати ефективність інформаційного захисту України, Ю. Лісовська відносить:

- запровадження цілісної та динамічної державної політики у досліджуваній сфері з урахуванням багатоаспектності інформаційного захисту;

- перспективні вектори змін світового інформаційного простору;

- геополітична та економічна специфіка країни;

- відповідний рівень розвитку суспільної свідомості;

- розвиток правових концептуально-доктринальних засад та ефективного інформаційного законодавства [16].

З урахуванням наведених факторів можливо визначити основні завдання державної інформаційної політики України. Зокрема, О. Данільян до переліку таких основних завдань відносить наступні:

1) забезпечення захисту інформаційного суверенітету країни з урахуванням сучасних тенденцій глобалізації суспільства, особливої уваги потребує захист процесів формування масової суспільної свідомості;

2) гарантування достатнього рівня забезпеченості інформацією для прийняття рішень з боку владних органів, підприємств та громадян;

3) створення необхідних умов для реалізації конституційно закріплених громадянських прав і свобод на інформацію;

4) управління різноманітними загрозами реального або потенційного характеру, спрямоване на формування необхідних умов для реалізації інтересів громадян, суспільства і держави [3].

Вітчизняні науковці Р. Шаповал та В. Клочко визначають державну політику у сфері забезпечення інформаційної безпеки України як відповідну діяльність державно-правових інститутів, спрямовану на управління загрозами й небезпеками реального чи потенційного характеру для гарантування можливостей реалізації інтересів громадян, суспільства або країни [42].

На думку дослідника Я. Жаркова, політика держави по забезпеченню інформаційної безпеки може бути охарактеризована як невід'ємний компонент загальної політики національної безпеки і представляє собою офіційно закріплену систему поглядів, а також діяльність владних та керівних державних органів практичного характеру, мета якої полягає у забезпеченні такого стану

соціальних суб’єктів, за якого вплив будь-якої загрози інформаційного характеру не зменшить рівень їх інформаційної безпеки нижче мінімально необхідного [7].

Узагальнюючи вищенаведене, єдина загальнодержавна політика в сфері забезпечення інформаційної безпеки може бути представлена у вигляді системи економічних, політичних та організаційних заходів, які відповідають наявним або можливим загрозам національній інформаційній безпеці, а також можливостям держави по управлінню такими ризиками. З урахуванням цього, політика держави в сфері інформаційної безпеки може бути сформована за трьома ключовими напрямками:

1) захист громадянських прав і свобод в інформаційній сфері;

2) захист національної безпеки і державного ринку в сфері інформації;

3) захист національних економічних інтересів в сфері інформації, а також національних виробників інформаційного продукту [11].

Єдність і взаємодія зазначених напрямків національної політики у сфері інформаційного захисту країни повинна бути забезпечена відповідними правовими механізмами, закріпленими на рівні законодавства:

- чіткі та обґрунтовані мета і завдання національної політики;

- порядок взаємодії інститутів держави і громадськості;

- налагодження системи інформування суб’єктів, діяльність яких пов’язана зі сферою забезпечення інформаційного захисту країни, про наявні або можливі проблеми і загрози, виявлення їх джерел, а також адекватні заходи щодо попередження, нейтралізації та усунення імовірних наслідків;

- порядок організації та узгодження ключових дій суб’єктів різних сфер життєдіяльності суспільства й держави з приводу адекватного реагування на виявлені можливі та існуючі загрози;

- основні засади управління, координації і контролю на загальнодержавному рівні у сфері забезпечення інформаційного захисту [22].

Аналіз наведених вимог до забезпечення захисту інформаційної безпеки в Україні свідчить про наступне:

- в українському правовому просторі відсутній ключовий документ – Стратегія розвитку інформаційної сфери, а прийнята Доктрина інформаційної безпеки має здебільшого декларативний і несистематичний характер;

- відсутні концептуальні документи гуманітарного напрямку, які теж повинні бути охопленими державною інформаційною політикою (бібліотечна і архівна справи, книговидавництво, національний імідж, офіційні комунікації);

- у вітчизняних умовах державне регулювання сфери інформаційного захисту і безпеки здійснюється з урахуванням середньострокових, а не довгострокових прогнозів і планів;

- відсутній загальний логічний підхід до формування основного масиву нормативно-правових документів державної політики у сфері інформаційної безпеки: наприклад, ідентичні за видом документи можуть розроблятися із застосуванням різних підходів, також відсутня взаємна підпорядкованість окремих видів нормативних документів.

До того ж, зазначає вітчизняний науковець Ю. Руденко, сучасна українська інформаційна інфраструктура знаходиться на етапі свого формування. Про це свідчить відсутність масштабного нормативно-правового підґрунтя відносин у сфері масової інформації. Відсутні конкретні визначені заходи національної політики у сфері створення державного інформаційного простору, налагодження і розвитку системи масової інформації, організації інформаційного обміну на міжнародному рівні. Ці фактори також призводять до погіршення ситуації із захистом інформаційних даних, які формують державну таємницю [33].

Таким чином, на рівні законодавства в Україні відсутні достатні гарантії захисту громадян і суспільства від негативних інформаційно-психологічних впливів, в результаті чого може бути зруйнованим єдиний національний інформаційний та духовний простір. Це свідчить про необхідність створення національної системи забезпечення інформаційно-психологічної безпеки, яка має формуватися на основі тісної взаємодії всіх інститутів державної влади та організацій громадськості.

2.2. Шляхи удосконалення механізму протидії сучасним загрозам деструктивного інформаційного впливу в умовах гібридної війни проти України

Удосконалення механізму протидії сучасним загрозам деструктивного інформаційного впливу, на думку сучасних авторів (І. Боднар, О. Власюка, В. Горбуліна, Е. Лібанової, Р. Токсоналієвої та ін.), стане можливим за наступних умов:

- розробка та запровадження комплексу заходів, спрямованих на перешкоджання, нейтралізацію й випередження несприятливих інформаційно-психологічних впливів на громадян, суспільство й державу [38];

- підготовка громадськості до активної інформаційної протидії;

- включення інформаційного поля країни до міжнародного інформаційного простору, удосконалення інформаційно-комунікаційних систем;

- створення системи підготовки кваліфікованих кадрів для реалізації інформаційно-психологічної протидії [1];

- дотримання суспільством однієї соціальної ідентичності;

- досягнення балансу між правами і свободами в інформаційній сфері та можливими обмеженнями в цьому напрямку для забезпечення державної інформаційної безпеки і захисту прав і свобод окремих суб'єктів [6].

З початком гібридної війни проти нашої країни з'явилася необхідність кардинальних трансформацій системи забезпечення національної інформаційної безпеки. Загальний план таких дій було запроваджено рішенням РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [29].

Відповідно до цього рішення, Кабінет Міністрів України повинен був підготувати, опрацювати і внести на розгляд парламенту відповідні законопроекти про зміни в тих нормативно-правових актах, які стосуються протистоянню інформаційній агресії іноземних держав. Наприклад, мали бути сформовані і закріплені механізм протидії несприятливому інформаційно-

психологічному впливу, зокрема, через заборону ретрансляції телевізійних каналів, а також порядок інформування та захисту іноземних журналістів, діяльність яких проходить у місцях збройних конфліктів, здійснення терористичних актів, при знищенні небезпечних злочинних угруповань. До того ж, окремим напрямком було визнано розробку проєкту стратегічного розвитку національного інформаційного простору із застосуванням заходів різнобічного характеру для масштабної реалізації державної політики у сфері інформаційного захисту країни, а також посилення контролю за дотриманням законодавчих вимог щодо інформаційно-психологічної та кібернетичної безпеки. На виконання цього плану заходів були підготовлені Стратегія кібербезпеки [31] та Доктрина інформаційної безпеки України [5].

Прийняття Доктрини інформаційної безпеки мало неоднозначний відгук серед українських експертів та суспільних діячів. Спектр оцінок коливався від визнання її важливості й упевненості, що такий нормативний акт мав бути прийнятим заздалегідь, до звинувачень у її тотожності з аналогічною доктриною інформаційної безпеки Російської Федерації 2016 року [26].

Наприклад, Д. Дубов (Національний інститут стратегічних досліджень) серед головних аспектів Доктрини наголосив на представленому державою розумінні розвитку й функціонування державного інформаційного простору і позиціонуванні Російської Федерації як противника, який веде системну інформаційну війну.

В свою чергу, Т. Попова (громадське об’єднання «Інформаційна безпека») охарактеризувала вітчизняну Доктрину як помітний крок уперед на шляху діяльності нашої країни, спрямованій на протидію агресії інформаційного характеру з боку Росії. З її точки зору, головним досягненням Доктрини вважається спроба визначити, збалансувати та гармонізувати повноваження владних органів держави та силових структур стосовно їхньої діяльності, спрямованої на захист суспільних і державних інтересів в інформаційній сфері, національного інформаційного простору [34].

На сучасному етапі розвитку нормативно-правового регулювання забезпечення інформаційної безпеки існують певні ризики в реалізації положень Доктрини, зокрема:

- несумісність рівня нормативно-правового регулювання конкретних напрямів діяльності державних органів та реальних заходів, спрямованих на виконання ними положень нормативних документів. Доктрина – нормативний документ непрямої дії, в ній лише окреслені стратегічні питання, а деталізація та конкретизація її вимог повинна здійснюватися в інших нормативно-правових актах з боку центральних органів виконавчої влади, структур сектору безпеки та оборони;

- відсутність дійсних функціонуючих механізмів координації та узгодження діяльності в напрямку інформаційного захисту. Існуючі позитивні приклади горизонтальної взаємодії владних органів, різноманітні волонтерські акції, проєкти у вигляді «ручного управління», скоріше за все, представляють собою лише виняток із правил, що підтверджує доцільність офіційного керування і узгодження дій з боку держави. В Доктрині наголошено на важливості централізації діяльності та наявності дієвих алгоритмів координації і контролю, проте відсутні реальні механізми реалізації цих заходів [36].

Узагальнюючи наведені недоліки нормативно-правового регулювання інформаційного захисту країни та існуючі ризики інформаційній безпеці в умовах гібридної війни проти України, доцільно запропонувати два пріоритетні напрями державної політики у цьому напрямку:

1. Захист життєво важливих особистісних, суспільних і державних інтересів від загроз внутрішнього і зовнішнього характеру. В сучасних умовах цей напрям має бути спрямований, в першу чергу, на протидію загрозам, які пов'язані із використанням інформаційних технологій з військово-політичною метою, у тому числі для проведення ворожих дій і актів агресії, націлених на порушення суверенітету або знищення територіальної цілісності України. Цей напрям державної політики може передбачати наступні заходи:

- формування та впровадження ефективних механізмів прогнозування, визначення та оцінювання інформаційних загроз;

- удосконалення сил і засобів інформаційного протистояння для нейтралізації (мінімізації) інформаційно-психологічного впливу та посилення актуальної системи забезпечення інформаційної безпеки Збройних Сил України та інших військових формувань;

- підготовка та формування єдиної державної інформаційної політики для її реалізації на тимчасово окупованих територіях;

- розвиток інформаційної культури особистості, зокрема, сучасної молоді, а також профілактика правопорушень в сфері інформаційної безпеки.

2. Охорона суверенітету, збереження територіальної цілісності країни та забезпечення її стабільності в політичній і соціальній сферах. Цей напрям передбачає такі організаційні заходи:

- протидія застосуванню інформаційних технологій, спрямованих на пропаганду екстремістської ідеології, розповсюдження ксенофобії, поглядів, що провокують виникнення національної ворожнечі;

- гарантування захисту державної таємниці або будь-яких інших інформаційних даних з обмеженим доступом, в першу чергу, комерційної таємниці військово-промислових підприємств та інших, які відіграють ключову роль в національній економіці;

- нейтралізація або мінімізація інформаційного впливу, націленого на знищення духовно-моральних цінностей, звичайних для українського народу;

- розробка та запровадження державних освітніх програм для підготовки висококваліфікованих кадрів з протидії інформаційним загрозам [37].

Таким чином, в умовах гібридної війни проти України державна політика у сфері забезпечення інформаційної безпеки має бути спрямована, в першу чергу, на реалізацію комплексу запобіжних заходів із наданням гарантій захисту життєво важливих особистісних, суспільних і державних інтересів та спроможності мінімізувати дію внутрішніх і зовнішніх імовірних або вже наявних загроз національній безпеці України.

ВИСНОВКИ ДО ДРУГОГО РОЗДІЛУ

У другому розділі магістерської роботи проаналізовані сучасні виклики інформаційній безпеці України та охарактеризовані механізми протидії несприятливим інформаційно-психологічним впливам.

При дослідженні державної політики України у сфері інформаційної безпеки було визначено, що її головне призначення полягає в забезпеченні збалансованої та узгодженої реалізації особистісних, суспільних та державних інтересів в інформаційній сфері. Ефективність державної політики України в сфері інформаційного захисту визначається впливом цілої низки факторів, серед яких: світові тенденції розвитку інформаційного простору; специфічні геополітичні та економічні особливості держави; специфічні характеристики і ступінь розвитку суспільної свідомості; відповідність інформаційного законодавства вимогам сучасного суспільства.

Аналіз механізму протидії сучасним загрозам негативного інформаційного впливу в сучасних умовах гібридної війни проти України дозволив виявити, що при забезпеченні безпеки в інформаційно-психологічному напрямку розробляється переважно технічний аспект, а психологічному відведена другорядна роль. В сучасних суспільно-політичних умовах це може зумовити посилення інформаційної агресії з боку Російської Федерації. Події останніх років свідчать про використання іноземними суб’єктами засобів масової інформації та соціальних мереж для дестабілізації українського інформаційного простору з метою певного впливу на хід подій, що може спричинити заподіяння Україні відчутної суспільно-політичної шкоди й економічних збитків. Це обумовлює необхідність подальшого вдосконалення нормативно-правового забезпечення для подальшого запобігання й нейтралізації потенційних та реальних загроз національній безпеці в інформаційній сфері України.

ВИСНОВКИ

В результаті проведеного дослідження у магістерській роботі охарактеризовано правові та організаційні основи протидії деструктивному інформаційному впливу в Україні та запропоновані пропозиції по удосконаленню захисту національного інформаційного простору.

1. Охарактеризовано розвиток і організацію нормативно-правового регулювання інформаційної безпеки України. Система правового регулювання інформаційного захисту країни представляє собою масив юридичних норм, які регулюють взаємовідносини в цьому напрямку, безпосередньо правові відносини, які формуються при використанні цих норм, та відповідні акти правозастосування. Нормативним підґрунтям забезпечення інформаційної безпеки є Конституція України, Закони України «Про інформацію», «Про основи національної безпеки України» та інші нормативно-правові акти. Сьогодні відсутні чітко обґрунтовані і взаємообумовлені підходи до забезпечення інформаційного захисту країни, тому ефективну систему протидії злочинності в інформаційній сфері може забезпечити запровадження і реалізація аргументованої державної політики в цьому напрямку.

2. Досліджено класифікацію загроз інформаційній безпеці України. Такі загрози представляють собою комплекс умов та чинників, які становлять небезпеку життєво необхідним державним, суспільним та особистісним інтересам у зв’язку з імовірністю негативної впливової дії інформації на свідомість та поведінку громадськості, а також на інформаційні ресурси країни та відповідну інфраструктуру. В сфері інформаційного захисту країни можуть визначатися зовнішні та внутрішні, потенційні або реальні та інші види загроз відповідно до джерел утворення, якими можуть бути людина, технічні або програмні засоби, технологічні схеми обробки, зовнішнє оточення тощо.

3. Визначено суб’єктів забезпечення інформаційної безпеки України. Суб’єктний склад системи подолання інформаційних загроз сформований з

урахуванням комплексного характеру останніх і відповідної специфіки функціональних завдань кожного з суб'єктів:

— профільна діяльність яких полягає у забезпеченні безпеки (Рада національної безпеки і оборони України, правоохоронні органи, інші державні виконавчі органи спеціального спрямування);

— для яких ця діяльність є переважною, проте не єдиною.

— які здійснюють інформаційний захист за межами своєї основної діяльності (різноманітні державні та громадські організації).

4. Обґрунтовано основні можливості розвитку правових основ державної політики України у сфері інформаційної безпеки. Державна інформаційна політика на сучасному етапі розвитку українського суспільства має бути спрямована на вирішення завдань по збалансованому забезпеченню інформаційної безпеки громадян, суспільства й держави поряд з паралельним виділенням актуальних пріоритетів в кожний необхідний момент. Такими пріоритетами можуть бути визначені, в залежності від ситуації, необхідність законодавчого оформлення певних стратегічних або програмних цілей і завдань, виявлення і прогнозування потенційних інформаційних загроз, ліквідація наявних загроз із мінімізацією наслідків різного ступеня їхньої сили і складності.

5. Визначено шляхи удосконалення механізму протидії сучасним загрозам деструктивного інформаційного впливу в умовах гібридної війни проти України. Відсутність упорядкованої та усталеної ієрархії при прийнятті та практичній реалізації нормативних документів щодо інформаційного захисту країни призводить до нестабільності та розбалансованості державної політики, зменшує ефективність відповідних управлінських дій з боку держави. Тому пріоритетними напрямками вдосконалення діючого законодавства визнано захист національних і суспільних інтересів, охорону суверенітету, збереження територіальної цілісності країни та її стабільності в політичній і соціальній сферах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Боднар І.Р. Державна політика та інформаційна безпека України: післякризові виклики. *Актуальні проблеми післякризового відновлення економіки України*: зб. матер. наук.-практ. конф. Львів. 2013. С.29-32.

2. Горбулін В.П., Качинський А.П. Засади національної безпеки України: підручник. Київ: Інтертехнологія, 2009. 272с.

3. Данільян О.Г. Національна безпека України: сутність, структура та напрями реалізації. Навчальний посібник. Х: Фоліо, 2002. 285с.

4. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави*. 2015. №2 (18). С.16-22.

5. Доктрина інформаційної безпеки України: затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: http://www.zakon3.rada.gov.ua/laws/show/514/2009 (дата звернення: 01.11.2021).

6. Донбас і Крим: ціна повернення: монографія / за заг. ред. В.П. Горбуліна, О.С. Власюка, Е.М. Лібанової, О.М. Ляшенко. К.: НІСД, 2015. 74с.

7. Жарков Я.М. Інформаційна безпека особистості, суспільства, держави: підручник. Видавничо-поліграфічний цента «Київський університет», 2008. 256с.

8. Зайцев М.М. Суб'єкти забезпечення інформаційної безпеки України. *Форум права*. 2013. №3. С.231-238.

9. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. 2016. №2-1. С.27-32.

10. Конституція України: прийнята Верховною Радою України №254к/96-ВР від 28.06.1996р. URL: https://zakon.rada.gov.ua/laws/show/ 254%D0%BA/ 96-%D0%B2%D1%80. (дата звернення: 03.11.2021).

11. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2007. 471с.

12. Кузьменко А. Проблеми відповідності стратегії та системи забезпечення безпеки України національним потребам. *Юридичний Журнал*. 2016. №10. С.27-32.

13. Левицька М.Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України: дис. … канд. юрид. наук: 12.00.01. Київ, 2002. 206с.

14. Ліпкан В.А. Національна безпека України: навч. посібник. Київ: Кондор, 2009. 280с.

15. Ліпкан В.А., Макименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ: КНТ, 2006. 280с.

16. Лісовська Ю.П. Державна політика забезпечення інформаційної безпеки України: адміністративно-правовий аспект. *Молодий вчений*. 2015. №2 (17). С.177-179.

17. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. … канд. юрид. наук: 12.00.01. Київ, 2007. 186с.

18. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду. *Ефективність державного управління*: Збірник наукових праць. Випуск 32. 2012. С.20-27.

19. Марутян Р.Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України. *Асоціація розвитку та безпеки*. 2019. №8. URL: http://www.dsaua.org/index. php?option= com_ content&view=article&id =198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90 &lang=uk (дата звернення: 05.11.2021).

20. Менеджмент інформаційної безпеки: підруч.: у 2 ч. / А.К. Гринь та ін.; за заг. ред. Є.Д. Скулиша. К.: НА СБУ, 2013. Ч.2. 604с.

21. Новицька Н.Б. Правове забезпечення інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави*. 2009. №1. С.44-47.

22. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Право і суспільство*. 2018. №2. С.132-137.

23. Олійник О.В. Структура суб'єктів забезпечення інформаційної безпеки в Україні. *Актуальні проблеми держави і права*. URL: http://www.apdp.in.ua/v69/18.pdf (дата звернення: 02.11.2021).

24. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. URL: http://www.justinian.com.ua/ article.php?id=3222 (дата звернення: 07.11.2021).

25. Пилипчук В.Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми. *Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти*: матеріали наук.-практ. конф. (06 жовтня 2016 р.). Київ: НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка», 2016. С.24-28.

26. Пилипчук В.Г. Інформаційна сфера як складова гібридної війни. *Актуальні проблеми управління інформаційною безпекою держави*: зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018р.). Київ: Нац. акад. СБУ, 2018. 408с.

27. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. *Науковий вісник Ужгородського національного університету: серія «Право»*. Випуск 43, том 1. 2017. С.34- 39

28. Почепцов Г. Сучасні інформаційні війни. Київ: Видавн. дім «Києво-Могилянська академія», 2015. 497с.

29. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Рішення Ради національної безпеки і оборони України від 28 квітня 2014р., введено в дію Указом Президента №449/2014 від 01.05.2014р. URL: http://www.zakon5.rada. gov.ua/ laws/show/n0004525-14 (дата звернення: 02.11.2021).

30. Про основи національної безпеки України: Закон України від 19.06.2003р. №964-IV. URL: http://uadocs.exdat.com/docs/index-208817.html (дата звернення: 02.11.2021).

31. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016р. №96/2016. URL: www.president.gov.ua/documents/ 962016-19836 (дата звернення: 02.11.2021).

32. Прозоров А.Ю. Ціннісні основи інформаційної безпеки особи, суспільства та держави. *Інформаційна безпека людини, суспільства, держави*. 2016. №1 (20). С.29-37.

33. Руденко Ю.Ю. Плюралізм в Україні як складова інформаційної політики у контексті забезпечення національної безпеки. *Актуальні проблеми управління інформаційною безпекою держави*: зб. матер. наук.-практ. конф. К. : Наук-вид. відділ НА СБ України, 2012. С.96-97.

34. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. URL: http://nbuviap.gov.ua/index.php?option=com_ content&view =article&id=2760:doktrina-informatsijnoji-bezpeki-yak-zasib-protidiji-informatsijn im-zagrozam2&catid=63&Itemid=393 (дата звернення: 07.12.2021).

35. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія. Заг. ред. Р.А. Калюжний. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196с.

36. Ткачук Т.Ю. Інформаційний чинник у гібридній війні. *Кібербезпека у системі нацбезпеки України: пріоритетні напрями розвитку*: мат. наук. круглого столу (Маріуполь, 26.04.18). МДУ, 2018. С.39-42.

37. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. … докт. юрид. наук. Ужгород, 2019. 487с.

38. Токсоналиева Р.М. Государственная политика Кыргызской республики в сфере информационно-психологической безопасности. *Вестник КРСУ*. 2015. Том 15. №5. С.35-38.

39. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об’єктів інформаційної діяльності. *Сучасний захист інформації*. 2016. №4. С.65-70.

40. Цивілізаційний вибір України: парадигма осмислення і стратегія дії: національна доповідь. Ред. кол.: С. Пирожков, О. Майборода, Ю. Шайгородський [та ін.]. Інститут політичних і етнонаціональних досліджень ім. І.Ф. Кураса НАН України. Київ: НАН України, 2016. 284с.

41. Черниш Р.Ф., Ігнатюк М.В., Заріцький О.Ю. Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти. *Юридичний науковий електронний журнал*. №11. 2021. URL: http://www.lsej.org.ua/index.php/arkhiv-nomeriv?id=146.

42. Шаповал Р.В., Клочко В.О. Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. *Наше право*. 2014. №6. С.5-9.