Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Навчально-науковий інститут державного управління
Кафедра державного управління і місцевого самоврядування

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

Студента *Шаблія Віталія Вікторовича*

академічної групи *281м-22з-4 ІДУ*

спеціальності *281 Публічне управління та адміністрування*

на тему: *«Інформаційна безпека в Україні: адміністративно-правові аспекти»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Квітка С.А.			
розділів:				

Рецензент:				

Нормоконтролер:	Вишневська О.В.			

Дніпро
2023

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи ступеня магістра на тему «Інформаційна безпека в Україні: адміністративно-правові аспекти».

74 с., 64 джерела.

ІНФОРМАЦІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ІНФОРМАЦІЙНА СФЕРА, ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО, ІНФОРМАЦІЙНА ПОЛІТИКА, ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ.

Об’єкт дослідження – суспільні відносини, що виникають в сфері інформаційної безпеки України.

Предмет дослідження – адміністративно-правове забезпечення інформаційної безпеки в Україні.

Мета дослідження – визначення шляхів удосконалення адміністративно-правового забезпечення інформаційної безпеки в умовах цифрової трансформації.

У першому розділі досліджуються теоретико-методологічні засади інформаційної безпеки України в умовах цифрової трансформації.

Другий розділ присвячено аналізу сучасного стану забезпечення інформаційної безпеки в умовах цифровізації інформаційного простору

У третьому розділі надані шляхи удосконалення адміністративно-правового забезпечення інформаційної безпеки в умовах цифрової трансформації.

Сфера практичного застосування результатів дослідження – сформульовані висновки дають можливість удосконалити законодавство в галузі інформаційної безпеки та усунути його недоліки при прогнозуванні можливих небезпек для інформаційного простору держави, інформаційної безпеки особи, держави і суспільства.

ABSTRACT

Explanatory note of the master's degree qualification thesis on the topic «Information security in Ukraine: administrative and legal aspects»

74 pages, 64 sources.

INFORMATION, INFORMATION SECURITY, ADMINISTRATIVE AND LEGAL PROVISION OF INFORMATION SECURITY, INFORMATION SPHERE, INFORMATION SOCIETY, INFORMATION POLICY, INFORMATION SECURITY THREATS.

Object of research is social relations arising in the field of information security of Ukraine.

Subject of research is the administrative and legal provision of information security in Ukraine.

The purpose of research is to determine ways to improve the administrative and legal provision of information security in the conditions of digital transformation.

The first section examines the theoretical and methodological foundations of Ukraine's information security in the context of digital transformation.

The second section is devoted to the analysis of the current state of information security in the conditions of digitalization of the information space

The third section provides ways to improve the administrative and legal provision of information security in the conditions of digital transformation.

The scope of practical application of the results of the work – the formulated conclusions provide an opportunity to improve the legislation in the field of information security and eliminate its shortcomings when forecasting possible dangers for the information space of the state, information security of the individual, the state and society.

ЗМІСТ

ВСТУП

Нові досягнення у сфері інформаційно-комунікаційних технологій, посилення ролі масової комунікації та розвиток когнітивних технологій збільшили можливості деструктивного інформаційного впливу на людину та суспільство. Поряд з унікальними можливостями для соціального прогресу цифрове середовище породило нові виклики та загрози для національної безпеки, які потребують адекватного реагування. Це зумовило виділення інформаційної безпеки як однієї з підсистем національної безпеки, значимість якої у міру розвитку науково-технічного прогресу інформаційно-комунікаційних технологій продовжує зростати. Це передбачає необхідність проведення фундаментальних досліджень адміністративно-правового забезпечення інформаційної безпеки та системного реформування правового регулювання відносин у цій сфері.

У сучасних умовах на тлі повномасштабної війни з росією пріоритетна роль забезпечення стабільного функціонування інформаційної сфери належить державі. Саме на державу як основний регулятор суспільних процесів покладено важливу місію, що цілеспрямовує та стимулює розвиток інформаційної сфери, не допускає негативних проявів цього розвитку, а навпаки – прискорює перехід України до якісно нової стадії розвитку – інформаційного суспільства. За цих обставин сформувалася залежність національної безпеки держави від забезпечення її інформаційної складової, що зростає в силу розвитку інформаційних технологій і сучасних глобалізаційних процесів. Тому, в умовах військового стану, а також соціально-економічної та суспільно-політичної кризи, що спостерігається в Україні, особливої актуальності набувають питання інформаційної безпеки в системі національної безпеки. При цьому, аналіз шляхів ефективності адміністративно-правового забезпечення інформаційної безпеки здійснюється з урахуванням міжгалузевого характеру адміністративних правовідносин. У цьому контексті постає необхідність приведення національного законодавства України до

міжнародних стандартів згідно задекларованим зовнішньополітичним пріоритетам.

Серед сучасних вітчизняних авторів загальнотеоретичних наукових праць у галузі адміністративного та інших галузей права, які заклали фундамент для дослідження цієї теми варто зазначити: О. А. Баранов, А. Ю. Геворкян, Н. Р. Нижник, В. Ю. Степанов, Т. Ю. Ткачук, та інших. Однак, незважаючи на значну кількість наукових праць, опублікованих останніми роками, враховуючи нещодавні зміни чинного законодавства в сфері інформаційної безпеки, можна стверджувати про відсутність у вітчизняній юридичній науці та науці державного управління комплексного дослідження щодо формування концептуальних теоретико-правових засад адміністративно-правового забезпечення інформаційної безпеки в Україні.

Окреслене визначає актуальність роботи і створює умови для формування нової адміністративно-правової парадигми забезпечення інформаційної безпеки з урахуванням вітчизняного та зарубіжного досвіду. Удосконалення правових, організаційних аспектів забезпечення інформаційної безпеки має стати пріоритетним напрямком державної політики України.

Об’єктом дослідження є суспільні відносини, що виникають в сфері інформаційної безпеки України.

Предметом дослідження є адміністративно-правове забезпечення інформаційної безпеки в Україні.

Метою магістерського дослідження є визначення шляхів удосконалення адміністративно-правового забезпечення інформаційної безпеки в Україні.

Відповідно до мети необхідно вирішити наступні завдання:

– з’ясувати сутність та основні характеристики інформаційної безпеки в Україні;

– розглянути правове регулювання забезпечення інформаційної безпеки в умовах цифрової трансформації;

– проаналізувати сучасний стан адміністративно-правових засобів та механізмів забезпечення інформаційної безпеки в умовах цифровізації;

– вивчити зарубіжний досвід забезпечення інформаційної безпеки;

– визначити пріоритетні напрями вдосконалення законодавства у сфері забезпечення інформаційної безпеки в умовах цифрової трансформації;

– обґрунтувати необхідність формування культури інформаційної безпеки.

Методологічною основою дослідження є сукупність загальнонаукових і спеціально методів пізнання, зумовлених метою й особливостями досліджуваної проблематики. Діалектичний метод пізнання правових явищ дав можливість вирішити поставлені завдання щодо аналізу сутності адміністративно-правового забезпечення інформаційної безпеки в Україні. За допомогою системного підходу в процесі аналізу явища інформаційної безпеки розглянуто правове регулювання інформаційної сфери та її роль в забезпеченні інформаційної безпеки метод порівняльного аналізу використаний при вивченні новітніх досліджень вітчизняної та зарубіжної науки адміністративного права, нормативно-правових актів з досліджуваної проблеми.

Наукова новизна дослідження визначається постановкою та рішенням актуальної та багатоаспектної наукової проблеми адміністративно-правового забезпечення інформаційної безпеки. У роботі автор вперше досліджує адміністративно-правове забезпечення інформаційної безпеки в організаційно-правовому аспекті у межах Стратегії інформаційної безпеки України щодо захисту національного інформаційного простору в умовах повномасштабній війни з росією.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

1.1. Сутність та основні характеристики інформаційної безпеки в Україні

Суттєвий прогрес і поширення інформаційних технологій, глобальний характер систем масової комунікації призвели до утворення глобального інформаційного простору, який змушує світову спільноту, кожну державу швидко орієнтуватися та адаптуватися у сучасному інформаційному середовищі. Світове співтовариство в цих умовах усвідомило, що міжнародна інформаційна безпека є проблемою, розв'язання якої суттєво впливає на існування людства. Тобто з розвитком і поширенням інформаційно-комунікаційних технологій у всі сфери життєдіяльності надзвичайної значимості набувають питання забезпечення інформаційної безпеки, визнаної в нашій країні однією з найважливіших складових національної безпеки, як багаторівневої проблеми державної інформаційної політики. Відзначимо, що у загальних засадах Конституції України, а саме ст. 17, наголошено, що інформаційна безпека є найважливішою функцією держави, справою всього Українського народу [14].

Науковці, використовуючи міждисциплінарний комплексний підхід при розробці різних аспектів проблеми безпеки, позитивний світовий і вітчизняний досвід її забезпечення, у своїх роботах розширили дослідне поле, запропонували рекомендації щодо зміцнення безпеки країни. Оскільки питання національної безпеки України є предметом окремих досліджень, то у даній роботі наша увага буде зосереджена на розгляді інформаційної безпеки як складової державної інформаційної політики.

Аналіз законодавства України [29; 34; 38; 39; 41; 42; 43; 50; 27; 28; 37] показав, що до основних проблем забезпечення інформаційної безпеки належать проблеми загальносистемного характеру, пов'язані з відсутністю наукового обґрунтування і практичної апробації політики і методології інформаційної безпеки в контексті державної інформаційної політики.

Так, згідно Доктрини інформаційної безпеки [28], інформаційна безпека України, як невід'ємна складова сфери національної безпеки, є комплекс соціально-економічних, морально-політичних, духовно-ідеологічних і військово-стратегічних ініціатив, що підкоряються жорсткій логіці державних інтересів. У Концепції національної безпеки України [39] та Законі України «Про основи національної безпеки» [42] розглядаються основні напрямки забезпечення безпеки в інформаційній сфері, під якою часто розуміють інформаційну безпеку як складову національної безпеки України. Слід зазначити, що ці поняття не є тотожні за змістом. Під інформаційною сферою на змістовному рівні слід розуміти безпосередньо інформацію та сферу її обігу. Тобто, безпека інформаційної сфери – це стан захищеності інформації та сфер її створення, накопичення, зберігання, оброблення, розповсюдження і використання. Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

На жаль, у процесі побудови теоретичних моделей інформатизації в Україні та інформаційного суспільства питання інформаційної безпеки часто відтісняються на другий план. Можливо тому, що в національному законодавстві є два різні за своєю суттю визначення поняття «інформаційна безпека» – в Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.» [43] та в Законі України «Про телекомунікації» [50].

У першому Законі [43] законодавче визначення цього поняття ототожнюється з поняттям «інформаційна безпека України», а саме: «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».

У другому Законі [50] визначення інформаційної безпеки стосується не так інформаційної безпеки України, як безпеки узагальненої технічної системи, якою є телекомунікаційна мережа, а саме: «інформаційна безпека телекомунікаційних мереж – це здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації».

У Законі України «Про інформацію» [38], який є базовим щодо нормативного закріплення інформаційної сфери держави, визначення інформаційної безпеки немає, а в Законі України «Про основи національної безпеки України» [42], який є основним орієнтиром забезпечення безпеки нашої держави, системну сутність інформаційної безпеки подано як невід'ємну складову національної безпеки України без точного визначення цього поняття. Крім того, в цьому законі замість поняття «інформаційна безпека України» використовується поняття «національна безпека України в інформаційній сфері». У Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» [34], який є одним із основних для забезпечення інформаційної безпеки держави у сфері інформатизації та телекомунікацій, поняття інформаційної безпеки також не визначено, хоча широко вжито та визначено в різних відтінках поняття «захист інформації».

Поняття «інформаційна безпека України» широко застосовується в Конституції України [1] та низці інших нормативно-правових актів, підготовлених та затверджених Верховною Радою, Президентом України, Кабінетом Міністрів, центральними органами виконавчої влади. Так, Закон України «Про Концепцію Національної програми інформатизації» [39] проголошує, що «інформаційна безпека є невід'ємною частиною політичної,

економічної, оборонної та інших складових національної безпеки». Воєнна доктрина України [41] прямо вказує, що «здійснення заходів щодо забезпечення інформаційної безпеки» є одним із основних завдань Збройних сил України в мирний час.

Таким чином, розвиток і вдосконалення системи гарантування інформаційного суверенітету та інформаційної безпеки держави, запобігання злочинам у сфері інформаційних технологій, забезпечення реалізації конституційних прав громадян на свободу слова та інформації, розвиток державного інформаційного ресурсу, захист інформаційної безпеки та національних інтересів в інформаційній сфері наголошується державою як пріоритетні завдання державної інформаційної політики. Але усвідомлюючи всю серйозність нових потенційних загроз національних інтересів в інформаційній сфері, на нашу думку, для вирішення завдань XXI ст. слід багато в чому переглянути концептуальні норми щодо інформаційної безпеки в контексті державної інформаційної політики, розпочати нову розробку довгострокових державних програм, спрямованих на забезпечення інформаційної безпеки держави, передусім її важливих інфраструктур, визначити організаційні засади.

Отже, організація сучасної інформаційної безпеки держави є, безперечно, складним, системним, багаторівневим феноменом, на стан, динаміку й перспективи розвитку якого безпосередньо впливають багато зовнішніх і внутрішніх чинників, найважливішими з яких є: політична обстановка у світі; наявність потенційних зовнішніх і внутрішніх загроз; стан і рівень інформаційно-комунікаційного розвитку країни; внутрішньополітична ситуація.

Слід відзначити, що на межі третього тисячоліття було сформульовано твердження, що інформаційна безпека виходить на перше місце в системі національної безпеки, у зв’язку з цим стало доцільним розглядати інформаційну безпеку як складову державної інформаційної політики. Разом з

цим, інформаційна безпека є самостійною складовою національної безпеки і в цьому проявляється її подвійний характер. Це обумовлюється наступним:

− прагненням кожної держави реалізувати та захистити власні національні інтереси, що направлені на формування та накопичення національного інформаційного потенціалу в умовах глобалізації світових інформаційних процесів;

− необхідністю не лише розвивати й посилювати національний інформаційний потенціал, але й захищати від широкого спектру існуючих та потенційних інформаційних загроз;

− існуванням реальної потреби в захисті всіх суб'єктів інформаційних стосунків від можливих негативних наслідків упровадження та використання інформаційних технологій;

− наявною можливістю інформаційного тиску на Україну, навіть інформаційної агресії з боку розвинутих країн світу з метою одержання односторонніх переваг в політичній, економічній, військовій та інших сферах, а також інформаційного впливу на свідомість і підсвідомість індивідів, на сім'ю, суспільство й державу, що загрожує національній безпеці країни.

На нашу думку, адекватний з методологічної точки зору підхід до проблем інформаційної безпеки повинен починатися з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційно-комунікаційних технологій. У цьому випадку предметом методології інформаційної безпеки є дослідження способів, методів, засобів і каналів реалізації загроз національним інтересам на інформаційному рівні та їх своєчасного виявлення, запобігання і нейтралізації. Тобто методологічною основою визначення поняття «інформаційна безпека» має бути віднесення категорії «безпека» не до самої інформації, хоча інформаційна безпека і пов'язана з нею, а до суб'єктів інформаційного середовища – фізичних та юридичних осіб, які беруть участь в інформаційному процесі.

Забезпечення безпеки в аспекті врахування інтересів суб'єкта інформаційних відносин є процес створення сприятливих умов діяльності,

цілеспрямоване формування (отримання, знаходження) умов, за яких реалізовувалися б його інтереси, здійснювалися б поставлені ним цілі. При цьому найважливішою підставою цілеспрямованої діяльності в галузі інформаційних відносин є його цінності їх учасників. Забезпечення безпеки суб'єкта є процес оволодіння суб'єктом необхідними умовами власного існування. Це, в свою чергу, означає, що безпека передбачає створення таких умов, в яких суб'єкти, як мінімум, зберігають і відтворюють свої цінності.

Спектр інтересів суб'єктів, пов'язаних з використанням інформаційно-комунікаційних технологій, можна розділити на наступні категорії: забезпечення доступності, цілісності і конфіденційності інформації і підтримуючої інфраструктури. Мета заходів у сфері інформаційної безпеки – захистити інтереси суб'єктів інформаційних відносин [17]. Інтереси ці різноманітні, але всі вони сконцентровані навколо трьох основних аспектів: доступність, цілісність та конфіденційність. У цьому контексті інформаційну безпеку можна трактувати і як відсутність неприпустимого ризику, пов'язаного із заподіянням прямого або непрямого збитку підприємству, установі (фізичній особі), викликаного порушенням конфіденційності, цілісності та доступності інформації [5, с. 28].

Отже, інтереси особистості в інформаційній сфері полягають в реалізації конституційних прав людини і громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку, а також у захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають у захисті життєво важливих інтересів особистості в цій сфері, забезпеченні реалізації конституційних прав і свобод людини та громадянина в інтересах зміцнення демократії, створенні правової соціальної держави, досягненні і підтримці суспільної злагоди, в духовному оновленні України, досягненні і підтримці громадської згоди, підвищенні творчої активності населення [58].

Інтереси держави в інформаційній сфері визначаються створенням умов для гармонійного розвитку української інформаційної інфраструктури, для реалізації конституційних прав і свобод людини та громадянина у сфері отримання інформації, користування нею з метою забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності України, встановлення політичної, економічної та соціальної стабільності, в безумовному забезпеченні законності і правопорядку, розвитку рівноправного і взаємовигідного міжнародного співробітництва на основі партнерства [15].

Відзначимо, при забезпечення інформаційної безпеки на основі врахування національних інтересів України в інформаційній сфері необхідно формувати стратегічні та поточні завдання внутрішньої і зовнішньої політики держави [21]. Як показує аналіз стану інформаційної безпеки України, її рівень, значною мірою, не відповідає потребам особистості, суспільства і держави. Очевидно, що державна інформаційна політика в аспекті інформаційної безпеки багато в чому буде залежати як від правильного вибору пріоритетів у наукових дослідженнях, так і від розробки адекватних наукових моделей і підходів до вирішення зазначених проблем.

Підходи до дослідження інформаційної безпеки в складі державної інформаційної політики та визначення поняття «інформаційна безпека» дають змогу розглядати дану проблему комплексно та системно. До цієї точки зору, найприйнятнішим є інтегральний підхід, який дає можливість зробити висновок, що інформаційна безпека не може розглядатися лише в якості окремого стану. Безперечно, вона є і властивістю, і атрибутом інформаційного суспільства, і діяльністю, і результатом діяльності людини, спрямованої на забезпечення певного рівня безпеки в інформаційній сфері.

Держава є визначальним і провідним суб’єктом політики. Вона має монополію на насильство як засіб політичного панування і володіє значним набором засобів впливу на поведінку всіх членів суспільства, а також матеріальними, технічними і кадровими ресурсами для реалізації своєї

політики. У зв'язку з цим усі органи держави тією чи іншою мірою беруть участь в діяльності щодо забезпечення інформаційної безпеки.

1.2. Правове регулювання забезпечення інформаційної безпеки в умовах цифрової трансформації

Стимульовані інформаційними технологіями економічні та соціальні перетворення, загальна інформатизація, використання інформації як одного з ефективних засобів впливу на суспільну свідомість та технологічний прогрес, поява нових форм відносин в умовах активного інформаційного обміну призводять до необхідності перегляду принципів взаємодії в системі держава-суспільство-особа.

Настання інформаційного суспільства трансформує звичні моделі економічної, соціальної, політичної діяльності, що тягне перебудову державно-правової діяльності з урахуванням нових умов інформаційної відкритості та необхідності вирішення проблем забезпечення інформаційної безпеки.

Розвиток інформаційно-комунікаційних технологій та процесів цифрової трансформації ставить завдання реформування системи правового регулювання суспільних відносин у різних сферах. Це особливо актуально стосовно нових викликів цифрового середовища, кількість та небезпека яких стрімко зростають.

З початку нового тисячоліття процес нормативного регулювання інформаційної безпеки значно активізувався, особливо у зв'язку з ухваленням Окінавської хартії глобального інформаційного суспільства та Доктрини інформаційної безпеки України (2009 р.) [22]. Загалом, за останні двадцять років було проведено значну роботу, спрямовану на розвиток правового забезпечення інформаційної безпеки.

Спроба детальної правової регламентації базових аспектів забезпечення інформаційної безпеки здійснювалася у законопроєкті «Про засади інформаційної безпеки України» [52]. У проєкті закону було визначено

принципи забезпечення інформаційної безпеки, основні завдання державної політики у сфері забезпечення інформаційної безпеки, функції державної системи забезпечення інформаційної безпеки.

Поняття «забезпечення безпеки» належить до базових категорій у теорії безпеки. Термін «забезпечення», що лежить в основі, орієнтує на активну діяльність певних суб'єктів, спрямовану на досягнення стану захищеності об'єктів безпеки. Змістом діяльності є реалізація уповноваженими суб'єктами політичних, правових, військових, соціально-економічних, інформаційних, організаційних та інших заходів, спрямованих на протидію загрозам національній безпеці.

У Стратегії інформаційної безпеки України забезпечення інформаційної безпеки визначається як здійснення комплексу взаємопов'язаних організаційних, правових та інших заходів щодо прогнозування, виявлення, стримування, запобігання, відображення інформаційних загроз та ліквідації їх негативних наслідків.

У Законі України «Про основи національної безпеки України», так само як і в законі, що прийшов йому на зміну «Про національну безпеку України», у забезпеченні безпеки виділено два рівні: державна політика у сфері забезпечення безпеки; діяльність із забезпечення безпеки [40; 42].

Такий підхід підтримується в науковій літературі. Суть такого розмежування зводиться до того, що на першому рівні здійснюється стратегічне планування забезпечення безпеки (постановка цілей, завдань, напрямів, визначення суб'єктів, форм і методів реалізації), на другому – безпосередня реалізація системи заходів забезпечення безпеки відповідно до виробленого плану.

Під забезпеченням інформаційної безпеки розуміємо діяльність державних інститутів, інститутів громадянського суспільства щодо вироблення та реалізації системи правових, організаційних, інформаційних і інших заходів, спрямованих на забезпечення захищеності особи, соціальних груп та суспільства від деструктивного інформаційного впливу.

Поряд із протидією інформаційним загрозам до змісту забезпечення інформаційної безпеки додано заходи щодо підвищення стійкості людини, соціальних груп та суспільства до впливу загроз.

Останній напрям має важливе значення через неможливість повного захисту соціальних суб'єктів від негативного психологічного впливу та недостатньою ефективністю систем фільтрації інформації.

Забезпечення інформаційної безпеки становлять заходи щодо впливу на інформаційне середовище, у якому здійснюється деструктивний інформаційний вплив на особистість та соціальні групи. Активізуючи позитивні чинники та нейтралізуючи негативні елементи цифрового середовища, можна підвищувати рівень захищеності об'єктів. Цей напрям укладається в концепцію «інформаційної екології», що передбачає створення певного стану інформаційного середовища, безпечного для фізичного та психічного здоров'я людини, індивідуальної, групової та суспільної психології. Інформаційна екосистема – це система, що складається з людини, інформації, інформаційного середовища та інформаційних технологій [16].

Діяльність із забезпечення інформаційної безпеки охоплює чотири основні елементи: протидія джерелам загроз інформаційної безпеки; нівелювання чи зменшення деструктивного впливу загроз на об'єкти інформаційної безпеки; збільшення стійкості об'єктів щодо деструктивного інформаційного впливу; надання впливу на елементи цифрового середовища.

Заходи забезпечення інформаційної безпеки охоплюють: регулювання, зокрема обмеження інформаційних потоків; організація інформаційних потоків, зокрема ініціювання поширення певної інформації; поширення способів й засобів обробки та оцінки інформації; формування групового і індивідуального психологічного захисту.

Важливу роль у механізмі забезпечення інформаційної безпеки відіграє правове забезпечення, оскільки саме право встановлює цілі, завдання та напрями забезпечення, регламентує форми, засоби та методи діяльності уповноважених суб'єктів щодо протидії загрозам інформаційної безпеки.

Ґрунтовний аналіз поняття правового забезпечення інформаційної сфери провів О. А. Баранов. Вчений зіставляє його з більш розробленими в теорії права категоріями «правове регулювання» та «правовий вплив». Зрештою, учений дійшов висновку, що правове забезпечення охоплює правове регулювання та елементи правового впливу. До останніх відносить правосвідомість, правову культуру, правові принципи. О. А. Баранов у контексті правового забезпечення забезпечувальних заходів, фрагментарно звертає увагу на заходи матеріально-технічного, організаційно-управлінського, кадрового, ідеологічного характеру [1].

Правове забезпечення інформаційної безпеки доцільно розглядати як діяльність із розробки та реалізації системи правових засобів, спрямованих на забезпечення захищеності особи, соціальних груп та суспільства від деструктивного інформаційного впливу.

У науці та документах стратегічного планування в галузі національної безпеки перед постановкою цілей та завдань забезпечення безпеки прийнято визначати національні інтереси.

У Стратегії національної безпеки України вони визначені як об’єктивно значущі потреби особистості, суспільства та держави у безпечному та сталому розвитку. Щодо інформаційної сфери національні інтереси визначаються тією роллю, яку відіграє інформація, інформаційна інфраструктура в забезпеченні сталого розвитку нації в конкретних історичних умовах.

Стратегія державної безпеки України закріплює національні інтереси України на сучасному етапі як захист конституційного ладу, суверенітету, незалежності, державної та територіальної цілісності України, зміцнення оборони країни; підтримання громадянського миру та згоди в країні; розвиток безпечного інформаційного простору; захист суспільства від деструктивного інформаційного впливу; зміцнення традиційних духовно-моральних цінностей, збереження культурної та історичної спадщини народу України.

Захист від деструктивного інформаційного впливу вперше виділено як один із національних інтересів у базовому документі стратегічного планування.

У цьому плані необхідне внесення низки змін та доповнень до чинної Стратегії інформаційної безпеки України, у якій захист від деструктивного інформаційного впливу безпосередньо не відображено.

З урахуванням вище зазначеного вважаємо за можливе сформулювати перелік національних інтересів України в інформаційній сфері, що стосуються забезпечення інформаційної безпеки: забезпечення та захист конституційних прав і свобод людини та громадянина, охоплюючи право на свободу, недоторканість приватного життя, захист честі та доброго імені, свободу думки та слова, право на інформацію та свободу масової інформації; формування середовища довіри в цифровому середовищі; забезпечення доступу до інформації, що сприяє розвитку особистості та суспільства; захист особи, соціальних груп та суспільства від деструктивного інформаційного впливу; гарантування психічного здоров'я та благополуччя громадян; збереження традиційних духовно-моральних цінностей та національної ідентичності суспільства, підвищення культурного потенціалу країни; зміцнення національної згоди, політичної та соціальної стабільності; забезпечення інформаційного суверенітету України у контексті асоціації України і Європейського Союзу; покращення іміджу України та підвищення авторитету на міжнародній арені, посилення політичного та культурного впливу України у світі; сприяння формуванню системи інформаційної безпеки, спрямованої на протидію загрозам деструктивного інформаційного впливу на особистість, соціальні групи та суспільство, заснованої на стандартах Північноатлантичного альянсу (НАТО) та Європейського Союзу; входження у Європейський інформаційний простір.

У Стратегії національної безпеки України безпосередньо мета забезпечення інформаційної безпеки не визначена. Узагальнення інформаційних положень та зміцнення суверенітету в інформаційному просторі і є метою забезпечення інформаційної безпеки [46].

У Стратегії інформаційної безпеки України загальну стратегічну мету забезпечення інформаційної безпеки визначено як посилення спроможностей

щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина [47].

Стратегічною метою забезпечення інформаційної безпеки є підтримка стану захищеності особистості, соціальних груп та суспільства від деструктивного інформаційного впливу, що забезпечує гарантовану реалізацію національних інтересів України.

На наступному рівні визначення цілі необхідно дати характеристику завдань та функцій забезпечення інформаційної безпеки. Щодо завдань і функцій забезпечення інформаційної безпеки, то загальноприйнятого уявлення про завдання та функції забезпечення безпеки немає.

У Законопроєкті «Про засади інформаційної безпеки України» було розмежовано завдання та функції забезпечення інформаційної безпеки.

У Стратегії інформаційної безпеки України завдання забезпечення інформаційної безпеки не виділено, а його основні напрями визначено стосовно окремих сфер державного управління: інформаційний вплив російської федерації як держави-агресора на населення України; інформаційне домінування російської федерації як держави-агресора на тимчасово окупованих територіях України; обмежені можливості реагування на дезінформаційні кампанії; несформованість системи стратегічних комунікацій; недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів; спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України; доступ до інформації на місцевому рівні; недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам [47].

Позитивно вирізняється в цьому плані Стратегія державної безпеки України, де чітко окреслено основні завдання забезпечення інформаційної

безпеки. Так, до сфери інформаційної безпеки належать:

– формування безпечного середовища обороту достовірної інформації в цифровому середовищі;

– розвиток системи прогнозування, виявлення та попередження загроз інформаційній безпеці України, визначення їх джерел, оперативної ліквідації наслідків реалізації таких загроз;

– створення умов для ефективного попередження, виявлення та припинення правопорушень, скоєних з використанням інформаційно-комунікаційних технологій;

– протидія використанню інформаційної інфраструктури терористичними організаціями, спеціальними службами та пропагандистськими структурами іноземних держав для здійснення деструктивного інформаційного впливу на громадян та суспільство.

Крім основного тематичного підрозділу, Стратегія державної безпеки України, положення про забезпечення інформаційної безпеки наявні в інших розділах документа, присвячених обороні країни, державній та громадській безпеці, захисту традиційних духовно-моральних цінностей, культури та історичної пам’яті, стратегічній стабільності та взаємовигідному міжнародному співробітництву.

Аналіз Стратегії державної безпеки України дозволяє виділити додаткові завдання забезпечення інформаційної безпеки: підтримання морально-політичного та психологічного стану особового складу Збройних сил України та інших військових формувань, військово-патріотичне виховання; недопущення втручання у внутрішні справи України, припинення розвідувальної та іншої діяльності іноземних держав та окремих осіб проти національних інтересів України; попередження та нейтралізація соціальних, міжконфесійних та міжнаціональних конфліктів, деструктивних релігійних течій; реалізація державної інформаційної політики щодо зміцнення сприйняття суспільством євроатлантичних пріоритетів та європейських культурно-історичних цінностей, неприйняття громадянами деструктивних ідей,

стереотипів; зміцнення культурного суверенітету України та збереження єдиного культурного простору, захист суспільства від зовнішнього деструктивного інформаційного впливу.

Узагальнюючи вищевикладене, до завдань забезпечення інформаційної безпеки слід зарахувати: прогнозування, виявлення, аналіз та оцінку загроз інформаційній безпеці, у тому числі щодо Законів України «Про боротьбу з тероризмом», «Про запобігання корупції» [25; 32]; аналіз та оцінку вразливості особи, соціальних груп і суспільства від деструктивного інформаційного впливу; стратегічне планування у сфері забезпечення інформаційної безпеки; правове регулювання у сфері забезпечення інформаційної безпеки; застосування комплексу оперативних та довготривалих заходів щодо превенції, припинення та усунення загроз інформаційній безпеці, мінімізації та ліквідації наслідків впливу; застосування комплексу оперативних і довготривалих заходів щодо підвищення здатності особи, соціальних груп та суспільства протистояти деструктивному інформаційному впливу; організацію діяльності системи забезпечення інформаційної безпеки; кадрове, інформаційне, матеріально-технічне та фінансове забезпечення діяльності суб’єктів забезпечення інформаційної безпеки; співробітництво у сфері забезпечення інформаційної безпеки з країнами Європейського Союзу та Організації Північноатлантичного Союзу.

За умов розвитку глобального інформаційного суспільства значущою теоретичною проблемою інформаційного права стає відокремлення функцій держави щодо забезпечення інформаційної безпеки. Виділення напрямів забезпечення інформаційної безпеки є важливим не тільки для визначення предметного змісту діяльності уповноважених суб’єктів, але вказівки на основні вектори формування та розвитку законодавства в цій сфері.

При визначенні напрямів забезпечення безпеки недоцільно змішувати діяльність щодо вирішення основних та забезпечувальних завдань. Для визначення основних завдань напрями діяльності державних органів відштовхуються від загроз безпеки та сфер прояву (наприклад, протидія

діяльності російських та іноземних спецслужб щодо деструктивного інформаційного впливу).

У кожному з напрямів діяльності необхідне вирішення однотипних забезпечувальних завдань у межах вироблення та реалізації державної політики забезпечення інформаційної безпеки (стратегічне планування, правове регулювання, матеріально-технічне забезпечення, підготовка кадрів).

Напрями діяльності щодо забезпечення інформаційної безпеки доцільно розглядати з позиції системного підходу, що використовується у правовій інформатиці. Діапазон проблем, що досліджуються та розв'язуються правовою інформатикою, від опрацювання правових даних до отримання нових знань і ухвалення управлінських рішень в інтересах громадян, суспільства, законодавчої, виконавчої та судової влади.

Основні напрями забезпечення інформаційної безпеки: прогнозування, виявлення, аналіз та оцінка загроз інформаційній безпеці; протидія поширенню негативної інформації у засобах масової інформації та мережі Інтернет; протидія терористичній та сепаратистській пропаганді та вербувальній діяльності, розпалюванню національної чи соціальної ненависті та ворожнечі; протидія деструктивному інформаційному впливу з боку державних органів та спеціальних служб росії та іноземних держав, російських неурядових організацій; забезпечення інформаційно-психологічної безпеки дітей та молоді; захист честі, гідності та ділової репутації громадянина, ділової репутації юридичної особи; захист органів публічної влади, посадових осіб від деструктивного інформаційного впливу; протидія фальсифікації історії України, у тому числі щодо єдності українського і російського народів; протидія поширенню деструктивних субкультур та інших форм негативного інформаційного впливу у духовній сфері у контексті пропаганди «русского мира и единства россии и Украины»; протидія кримінальним та адміністративним правопорушенням, пов'язаним з наданням деструктивного інформаційного впливу; інформування української та зарубіжної громадськості про внутрішню та зовнішню політику України, офіційну позицію щодо

соціально значущих подій в Україні та міжнародному житті; ведення контрпропаганди в Україні та за кордоном; формування цифрової грамотності громадян та культури інформаційної безпеки.

У Стратегії інформаційної безпеки України закріплено, що забезпечення інформаційної безпеки здійснюється на основі поєднання законодавчої, правозастосовної, правоохоронної, судової, контрольної та інших форм діяльності державних органів у взаємодії з органами місцевого самоврядування, фізичними та юридичними особами.

Ця діяльність здійснюється у звичайних і в особливих умовах спеціальних правових режимів. У Стратегії інформаційної безпеки України спеціально виділено низку напрямів забезпечення інформаційної безпеки в надзвичайних ситуаціях, що має суттєве значення в умовах воєнного стану.

Система правового регулювання забезпечення інформаційної безпеки в Україні характеризується ієрархічністю структури. Елементами цієї системи виступають правові норми, суб'єкти правовідносин, правові засоби, методи та принципи регулювання. Цей висновок ґрунтується на представленні досліджуваного об'єкту у вигляді системи, яка охоплює цілісність об'єкту з урахуванням усіх внутрішніх і зовнішніх взаємозв'язків і чинників, що характеризують правові відносини в інформаційній сфері.

З урахуванням викладеного, систему правового забезпечення інформаційної безпеки щодо деструктивного інформаційного впливу можна визначити як упорядкований комплекс правових засобів, які використовуються для підтримки стану захищеності особи, соціальних груп і суспільства від деструктивного інформаційного впливу.

Фундаментом правової основи забезпечення інформаційної безпеки стали Закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист суспільної моралі», «Про електронні комунікації» [38; 34; 35; 31].

Водночас в умовах воєнного стану, поєднаного з цифровою трансформацією, з метою прискореного розвитку економіки України, що

позначено у Законі України «Про стимулювання розвитку цифрової економіки в Україні», забезпечення інформаційної безпеки охоплює усі напрями: інформаційну безпеку особи, інформаційну безпеку суспільства, інформаційну безпеку держави [49].

Системи правового забезпечення інформаційної безпеки подана як сукупність наукових знань, що становлять зміст теорії систем права та теорії інформаційного права, що розвиваються.

Система правового забезпечення інформаційної безпеки розвивається на методологічній базі адекватного проблемно орієнтованого варіанта системного інформаційно-кібернетичного підходу на основі синергетики з розподілом на кібербезпеку та інформаційну безпеку особи, суспільства та держави.

Для переходу до цифрової економіки державі необхідно створити інформаційну інфраструктуру, у якій відкритість та прозорість даних поєднуються з рівністю можливостей окремих осіб в економіці (інклюзивна економіка) та ефективною системою інформаційної безпеки, яка захистить інтереси особи, суспільства і держави.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНОГО СТАНУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ ІНФОРМАЦІЙНОГО ПРОСТОРУ

2.1. Адміністративно-правові засоби та механізми забезпечення інформаційної безпеки в умовах цифровізації

Правове регулювання використання інформаційно-комунікаційних технологій і систем створення та використання інформаційної інфраструктури в Україні безпосередньо пов’язане з правовим забезпечення інформаційної безпеки та кібербезпеки всіх учасників таких відносин. Цифровізація інформаційної сфери безпосередньо пов’язана із зусиллями та ресурсами, що виділяються органами публічного сектору для виконання нормативних документів у момент впровадження та з часом. Критичну роль відіграє переплетення макро- та мікроінституціональних і технічних умов. Правова та інституційна основа цифровізації інформаційної сфери – це основа, у якій можуть відбуватися зміни, що насамперед торкаються інформаційної безпеки.

Використання інформаційної інфраструктури з метою забезпечення інформаційної безпеки створює суспільні відносини, регулювання яких має здійснюватися правовими нормами, а розробка, прийняття, застосування та виконання обов’язкових вимог до інформаційних технологій у контексті забезпечення інформаційної безпеки має здійснюватися нормами технічного регулювання.

Активне використання в суспільних відносинах технологій великих даних (англ. BigData), промислового Інтернету породжує необхідність визначення критеріїв і правових засад використовуваних інформаційних технологій та інформаційної інфраструктури; забезпечення інформаційної безпеки щодо інформації, яка збирається та обробляється цими технологіями, у тому числі персональних даних, відомостей, що становлять комерційну таємницю, інших

видів інформації обмеженого доступу, що розміщуються в інформаційній інфраструктурі.

Використання інформаційних технологій у контексті цифрової трансформації потребує зміни підходу до правового регулювання інформаційної безпеки, запровадження інститутів «цифрового права»; формування єдиних стандартів життєвого циклу інформаційних технологій. Предметом ІТ-права є відносини у цифровому середовищі (відносини з приводу створення, зберігання, передачі та захисту інформації в електронному вигляді).

Дослідження механізму правового забезпечення інформаційної безпеки в умовах цифровізації передбачає вивчення правового інструментарію, використовуваного інформаційним та іншими галузями права щодо захисту особи та суспільства від деструктивного інформаційного впливу.

Сьогодні, зазначає О. В. Соскін, спостерігається перехід до комплексних методів у провідних країнах світу, основною метою яких є огляд можливостей цифрової трансформації державного управління і перспектив розвитку інформаційно-комунікаційної інфраструктури на технологічному підґрунті цифрових технологій. Інформаційно-комунікаційне середовище має дві складові: інформаційно-технічну (штучно створену людиною – світ техніки, технологій тощо) та інформаційно-психологічну (світ живої природи, який охоплює й саму людину). Як наслідок, загалом інформаційну безпеку особистості, суспільства (держави) можна презентувати двома складовими частинами: інформаційно-технічною безпекою та інформаційно-психологічною (психофізичною) безпекою [57].

У механізмі правового забезпечення інформаційної безпеки дуже поширене використання правових заборон. Прикладами таких заборон є: заборона зловживання свободою масової інформації; заборона розповсюдження протиправної інформації; заборона недобросовісної та недостовірної реклами; заборона обігу інформаційної продукції, що містить інформацію, заборонену для поширення серед дітей тощо.

Фундаментальне значення у механізмі правового забезпечення

інформаційної безпеки має закріплена у ст. 28 Закону України «Про інформацію» заборона поширення протиправної інформації [38]. У ньому проявляється міжгалузева природа аналізованого правового інституту та простежуються галузеві взаємозв'язки інформаційного, адміністративного та кримінального права.

Ця правова заборона сформульована двояко: спочатку через перерахування кількох конкретних видів негативного контенту (інформації, спрямованої на пропаганду війни, розпалювання національної, расової чи релігійної ненависті та ворожнечі), поширення якого забороняється, та через вказівку щодо інформації, за поширення якої передбачена кримінальна чи адміністративна відповідальність.

Як інформація, що надає деструктивний вплив на індивідуальну, групову або суспільну свідомість, ідентифіковані: інформація порнографічного характеру; інформація, що пропагує культ насильства та жорстокості, що містить заклики до насильницького повалення конституційного ладу, організації або проведення масових заворушень; інформація, що пропагує війни, соціальну, національну, релігійну та расову ворожнечу; інформація, що охоплює загрозу вчинення акту тероризму.

Будь-який варіант правової регламентації переліку негативної інформації, забороненої для розповсюдження, вимагає подальшої синхронізації з механізмами обмеження доступу до такої інформації.

В Україні з моменту запровадження Закону України «Про санкції» використано досить цікаву схему [48]. Законодавець встановлює процедури блокування таких ресурсів, які містять певні види забороненої інформації у позасудовому порядку. Перелік видів такої інформації поповнюється. Санкції вводяться у дію указами Президента України на підставі рішення Ради національної безпеки і оборони.

За даними аналітичного звіту «Санкції та блокування вебсайтів в Україні», станом на 2021 р. заблоковано 633 інтернет-ресурси [6].

У 2022 р. за допомогою телеграм-ботів кіберполіції вдалося заблокувати

понад 3 тисячі ворожих інтернет-ресурсів. Загальна аудиторія заблокованих ресурсів становила понад 23 млн осіб [9].

Такий алгоритм роботи правового механізму блокування можна вважати прийнятним. Однак очевидна відсутність системності та чітких методологічних принципів функціонування.

Значущими у контексті забезпечення інформаційної безпеки є юридичні обов'язки:

– не допускати використання сервісу з метою вчинення кримінальних діянь, поширення пропаганди тероризму, матеріалів, що пропагують порнографію, культ насильства та жорстокості;

– перевіряти достовірність поширених суспільно значимих відомостей до поширення;

– не допускати використання сервісу з метою приховування або фальсифікації суспільно значимих відомостей, поширення недостовірної суспільно значущої інформації новин під виглядом достовірних повідомлень;

– не допускати поширення інформації з метою знеславити громадянина або окремі категорії громадян за ознаками статі, віку, расової чи національної приналежності, мови, ставлення до релігії, професії, місця проживання та роботи, у зв'язку з політичними переконаннями.

Частина сформульована за типом пасивних обов'язків, тобто обов'язки не допускати, але реалізація передбачає активну діяльність з вивчення, перевірки та оцінки контенту, що поширюється, вживання заходів щодо припинення обігу недостовірного контенту в певних випадках.

О. А. Невельська-Гордєєва та В. О. Нечитайло, досліджуючи «Феномен «fakenews» у контексті забезпечення інформаційної безпеки держави», зазначають, що неправдива інформація – «fakenews» – існує в усіх сферах суспільства. Завдяки розвитку інформаційних технологій вони стали поширюватися ще швидше та охоплюють більшу аудиторію. Загроза пропаганди, дезінформації, бажання похитнути авторитет та викликати агресію приносять величезну кількість проблем у сучасному світі. Інформаційні війна є

однією з таких проблем, з якими зіштовхнулися багато країн, у тому числі й Україна. Психологічні операції є надзвичайно інтерактивними та застосовуються з однією метою – знизити можливі ризики з боку населення та здобути його довіру. Тому першим кроком у бік запобігання дезінформації є медіаобізнаність, власна усвідомленість та глибокий аналіз новин, що поширюються [20, с. 131].

Дозвіл є важливим методом правового забезпечення інформаційної безпеки і його застосування має розширюватися. Вектором такого розширення має стати правова регламентація прав фізичних та юридичних осіб щодо участі у забезпеченні інформаційної безпеки.

Що стосується додаткових способів правового регулювання, до яких належать заохочення та рекомендації, то вони знаходять необґрунтовано мале застосування у механізмі правового забезпечення інформаційної безпеки. Це стосується законодавчого рівня, де таких норм практично немає. Розвиток таких способів регулювання, як пільги та стимули, можна віднести до трансформації правового регулювання інформаційної безпеки.

У нормативних документах Європейського Союзу активно застосовуються заохочувальні та рекомендаційні норми, присвячені забезпеченню інформаційної безпеки.

Проте держава недостатньо чітко сформулювала зацікавленість у реалізації таких ініціатив громадянського суспільства та інтернет-галузі. Зробити це можна було б за допомогою заохочувальних та рекомендаційних правових норм. Позитивним у цьому плані є розробка проєкту Концепції та плану заходів з розвитку цифрових прав дітей [54].

У Концепції закріплено комплекс заохочувальних та рекомендаційних норм, спрямованих на стимулювання участі інститутів громадянського суспільства у забезпеченні інформаційної безпеки дітей та поширення наявного позитивного досвіду в цій сфері.

Зокрема, Концепція передбачає: надання державної підтримки соціально значимим проєктам у галузі друкованих та електронних мас-медіа для дітей та

молоді, узагальнення кращих форм з підтримки регіональних виробників інформаційної продукції для дітей з подальшим виробленням рекомендацій для органів місцевого самоврядування; організацію та проведення конкурсу соціальної реклами пропаганди здорового способу життя, спрямованого на формування у підлітків та молоді негативного ставлення до незаконного споживання наркотиків та ін.

Такі механізми охоплюють певні правові засоби та методи чи їх комплекс. Проведений аналіз інформаційного законодавства дозволив вирізнити такі:

1. Встановлення правових заборон та інших обмежень поширення певних видів негативної інформації – означає правове закріплення заборон поширення негативного контенту, обмежень інших видів.

Правові обмеження можуть виражатися у зменшенні кількості можливих форм здійснення права чи свободи, у фіксації чи звуженні просторових та тимчасових кордонів реалізації права чи свободи, кола осіб, які мають можливість користуватися правом (свободою), у виключенні юридичної можливості здійснення права чи свободи у певних випадках, в ускладненні порядку здійснення права або свободи, а також у знищенні, вилученні або применшенні блага, що лежить в основі конституційного права або свободи.

Основне значення має норма ст. 28 Закону України «Про інформацію», яка встановлює заборону розповсюдження протиправної інформації.

2. Закріплення спеціальних правил обігу інформаційної продукції певних видів – означає встановлення правовими нормами спеціальних умов виробництва та поширення негативної інформації. Такі умови можуть охоплювати просторові та тимчасові обмеження розповсюдження контенту, додаткові вимоги до обігу інформаційної продукції. Усі вони знайшли відображення у Законі України «Про захист суспільної моралі».

У законодавстві встановлено низку додаткових вимог поширення певних видів інформаційної продукції. Наприклад, продукція сексуального чи еротичного характеру може розповсюджуватися лише за умови герметичної

упаковки, спеціального маркування і за наявності повідомлення «продукція сексуального характеру, продаж дітям заборонено». Це передбачено Законом України «Про внесення змін до Закону України «Про захист суспільної моралі» щодо захисту прав та найкращих інтересів дитини» [26].

3. Закріплення обов'язків суб'єктів інформаційних правовідносин щодо забезпечення інформаційної безпеки означає встановлення правовими нормами зобов'язань учасників правовідносин щодо забезпечення інформаційної безпеки. Такий правовий механізм використовує законодавець стосовно ключових інформаційних посередників у мережі Інтернет. Важливим стало закріплення обов'язків соціальних мереж здійснювати моніторинг з метою виявлення протиправного контенту та вживати заходів щодо обмеження доступу.

4. Вікова класифікація та маркування інформаційної продукції – передбачає проведення класифікації інформаційної продукції щодо прийнятності інформації для людей певних вікових категорій з наступним нанесенням на таку продукцію присвоєного знака вікової категорії.

Сам правовий механізм вікової класифікації та маркування використовується подвійним чином. З одного боку, вона є основою для встановлення правових режимів обігу інформаційної продукції певних вікових категорій, а з іншого – має самостійну значущість як спосіб оповіщення дорослих про вікові обмеження інформаційної продукції для прийняття рішення про доцільність та допустимість показу дітям.

5. Ідентифікація особи абонентів, користувачів мережі Інтернет та цифрових сервісів – означає систему заходів, спрямовану встановлення та перевірку справжності особи користувачів інформаційних сервісів і послуг. Ідентифікація – це інформаційний процес, спрямований на встановлення суб'єктного та об'єктного складу правовідносин на основі ідентифікаторів або їхньої сукупності.

Ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях та/або електронних

даних, у результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи [30].

Значимість ідентифікації в механізмі забезпечення інформаційної безпеки обумовлюється тим, що спрямована на усунення анонімності як одного з важливих факторів, що утворюють загрозу в цифровому середовищі. Анонімністю користуються іноземні спецслужби та злочинці для здійснення шкідливої діяльності в цифровому середовищі, пов'язаному з негативним інформаційним впливом на окремих індивідів або соціальні групи. Фактор анонімності найбільш активно проявляється при використанні мобільного зв'язку та інформаційно-комунікаційних мереж. Останніми роками законодавець вніс до чинного інформаційного законодавства низку норм, спрямованих на усунення чи зниження впливу анонімності в електронних комунікаціях.

Реалізація різних методів ідентифікації за умов цифрової трансформації сприяє вирішенню важливого завдання забезпечення довіри до цифрових комунікацій.

6. Видалення чи обмеження доступу до протиправного контенту – охоплює правові методи та засоби обмеження доступу до забороненої інформації або її видалення.

7. Встановлення юридичної відповідальності за правопорушення, що посягають на інформаційну безпеку – означає правове закріплення складів правопорушень та заходів відповідальності за вчинення. Ключове значення тут мають норми кримінального та адміністративно-деліктного законодавства. Безперервне розширення спектра загроз інформаційній безпеці особи, суспільству та державі диктує потребу постійного доповнення складів правопорушень. Формою юридичної відповідальності за правопорушення, що посягають на інформаційну безпеку, є цивільно-правова відповідальність, що регламентується Цивільним кодексом України.

8. Правове регулювання заходів контрпропаганди – означає правову регламентацію заходів контрпропаганди, змістом якої є надання зустрічного

інформаційного впливу з метою нейтралізації деструктивної інформаційної активності противника (джерела загрози). В інформаційному законодавстві брак норм, які комплексно регулюють цей напрям діяльності. Фрагментарне правове регулювання з цього питання є у Законі України «Про боротьбу з тероризмом» та в інших законодавчих актах, які стосуються сфери адміністративного права.

9. Правове стимулювання розвитку цифрової грамотності та формування культури інформаційної безпеки – охоплює правові засоби, спрямовані на стимулювання підвищення поінформованості громадян про наявні загрози інформаційній безпеці, джерела та форми прояву, правила безпечної поведінки в інформаційному середовищі.

Проєкт Концепції виховання дітей та молоді в цифровому просторі серед пріоритетних завдань забезпечення інформаційної безпеки закріпив формування у дітей навичок самостійного та відповідального споживання інформаційної продукції та підвищення рівня медіаграмотності [53].

Оскільки основна роль у підвищенні цифрової грамотності та формуванні культури інформаційної безпеки відводиться системі освіти та інститутам громадянського суспільства, головними завданнями держави є стимулювання та підтримка таких ініціатив.

Заходи щодо формування культури інформаційної безпеки знайшли відображення у Пріоритетних напрямах та завданнях (проєктах) цифрової трансформації на період до 2023 р. [7].

В умовах цифрової трансформації зміни зазнає сфера правового регулювання, у якій формуються відносини, що охоплює безпосередню участь громадян, у тому числі у сфері інформаційної безпеки. Багато нових відносин не можуть бути врегульовані своєчасно через відсутність відповідних цифрових технологій та можливостей здійснення контролю реалізації. Правова практика потребує оптимального поєднання юридичних та цифрових технологій величезного спектра відносин, які підпадають під сферу правового регулювання, що визначаються об’єктивними умовами життя.

У національній правовій системі формуються суспільні відносини, які раніше не вимагали правової регламентації. Їх учасниками є анонімні цифрові суб'єкти у віртуальному просторі. Регулювання подібних відносин передбачає заміну багатьох юридичних процедур у чинному праві, пов'язаних, перш за все, з ідентифікацією особи як суб'єкта права, з реалізацією прав людини у цифровому просторі, з використанням баз даних, що впливає на забезпечення інформаційної безпеки.

В інформаційному праві та на практиці склався комплекс юридичних засобів, які при системному застосуванні дозволяють забезпечувати інформаційну безпеку. Системне та впорядковане застосування юридичних засобів дозволяє виявити існування забезпечувального механізму. Як основний підхід до аналізу сутності названого механізму використовувався інституціоналізм, що передбачає охоплення названим механізмом та вивчення окремих адміністративно-правових норм або інститутів адміністративного та інформаційного права та практику застосування за допомогою діяльності держави, органів публічної адміністрації, інститутів громадянського суспільства, судових та квазісудових органів. За такого підходу інституційний механізм забезпечення інформаційної безпеки є комплексним правовим явищем. Забезпечення інформаційної безпеки потребує активного впровадження інновацій, поступового переходу до механізмів, передбачених нормативними актами НАТО та Європейського Союзу.

Наразі триває подальший розвиток законодавства щодо удосконалення адміністративно-правових засобів та механізмів забезпечення інформаційної безпеки. Передбачувані зміни можуть торкнутися спектру питань, важливими з яких в аспекті проблем адміністративно-правового регулювання є посилення державного контролю за раціональним використанням ресурсів та вдосконалення взаємодії органів публічної влади та інститутів громадянського суспільства в досліджуваній сфері. Це пов'язано з великим обсягом чинних нормативно-правових актів, що регламентують складову діяльність у сфері інформаційної безпеки. Щодо видання локальних нормативно-правових актів

адміністративно-правового регулювання, то вони можуть здійснюватися незалежно один від одного компетентними органами.

Аналіз дозволив зробити висновок про те, що адміністративно-правові засоби та механізми забезпечення інформаційної безпеки в умовах проведення цифровізації в Україні становлять досить складне поєднання політико-правових та адміністративно-правових норм, які відповідають за певну сферу діяльності органів публічної влади та суб'єктів господарювання.

Органи публічної влади у сфері інформаційної безпеки повинні демонструвати систему горизонтально та вертикально взаємно збалансованих та взаємопов'язаних публічно-правових утворень, до завдань яких належить координація з метою недопущення виникнення загроз інформаційній безпеці особи, суспільства та держави.

2.2. Зарубіжний досвід забезпечення інформаційної безпеки

Сучасні підходи до забезпечення інформаційної безпеки, прийняті у країнах Східної Європи, не є уніфікованими, що зумовлено геополітичною специфікою відповідних країн, одні з яких входять до Північноатлантичного Альянсу (НАТО) та Європейського Союзу (ЄС), інші – прямують до членства у вказаних організаціях, а деякі – входять до євразійських міждержавних утворень. Обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфері [24, с. 18].

Втім, не менш важливим є і досвід інших країн Східної Європи, які проходять аналогічний шлях у процесі становлення та розвитку інформаційного суспільства. Тож дослідження, оцінка та імплементація позитивного досвіду східноєвропейських країн мають важливе значення при розбудові системи забезпечення інформаційної безпеки в Україні, оскільки події останніх років в нашій державі показали, що наша країна поки що не

готова протистояти інформаційним війнам, а її політика у сфері забезпечення інформаційної безпеки та інформаційна політика в цілому потребує вдосконалення [63, с. 179].

З точки зору забезпечення інформаційної безпеки у Східній Європі доцільно буде визначити репрезентативними країни різних геостратегічних спрямувань, тому пропонуємо зосередитись на огляді питань забезпечення інформаційної безпеки у Румунії, Болгарії, Молдові та Білорусі.

Передусім зауважимо, що Румунія та Болгарія є членами Північноатлантичного Альянсу та Європейського Союзу. Відповідно, на них поширюються стандарти цих міжнародних організацій щодо інформаційної політики та забезпечення інформаційної безпеки. Це, зокрема, стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору (НАТО)», офіційна політика НАТО у сфері кіберзахисту [64], стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського саміту й уточнена за результатами Варшавського саміту тощо. Також Румунія та Болгарія, як країни-члени ЄС, втілюють у національній політиці забезпечення інформаційної безпеки стандарти ЄС, в тому числі передбачені «Європейськими критеріями безпеки інформаційних технологій» (1991 р.), «Єдиними критеріями безпеки інформаційних технологій» (1996 р.), документом «Мережева та інформаційна безпека: європейський політичний підхід» (2001 р.), документом «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» (2007 р.) [59] тощо.

Відповідно, основними напрямами забезпечення інформаційної безпеки у вказаних країнах є: підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами; створення європейської системи попередження та інформування про нові загрози; забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації; правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності; зміцнення інформаційної безпеки на державному

рівні шляхом впровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних он-лайн послуг тощо; розвиток міжнародного співробітництва з питань інформаційної безпеки. Основними викликами інформаційній безпеці Румунії та Болгарії, як країн ЄС, є некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів; відсутність на європейському рівні партнерства між державним та приватним секторами; обмежені можливості щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем; відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури [59].

Одним з найбільш важливих питань політики інформаційної безпеки Румунії та Болгарії, як країн-членів ЄС, є захист персональних даних, в якому вони керуються положеннями Директиви 95/46/ЄС «Про захист фізичних осіб у зв'язку з обробкою персональних даних і вільного обігу таких даних». У цьому документі одночасно декларується прагнення до вільного переміщення інформації між країнами-членами ЄС та надаються гарантії захисту основних прав громадян, до яких входить право на недоторканність особистих даних і їх захист від третіх осіб [36]. Крім того, з 2018 р. для Румунії та Болгарії, як і інших країн-членів ЄС, набудуть чинності нові правила захисту персональних даних (GDPR), які схвалено 14 квітня 2016 р.. Ці правила буде поширено не тільки на європейські компанії, але й на компанії з інших країн, які пропонують товари й послуги в ЄС. У відповідному документі переглянуті цивільні права користувачів, відповідальність за схоронність даних, а також уведені деякі обмеження переміщення даних між різними країнами. Також важливим нововведенням є введення більш суворого покарання за несвоєчасне повідомлення інформації про виток даних. Компаніям, що порушили

положення нової директиви та не доповіли про факт витоку або злому протягом 72 годин з моменту виявлення інциденту, загрожує штраф до 4 % річного доходу або до 20 млн. євро. Крім того, відповідна Директива передбачає необхідність отримання згоди користувачів на обробку їх персональних даних, причому на обробку даних з різними цілями потрібні будуть окремі згоди. Згода повинна бути вільною, свідомою і конкретною, а також може бути відкликана в будь-який момент. Згода не буде вважатися вільною, якщо користувач змушений дати таку згоду, щоб одержати доступ до сайту, програми або додатка. Виключенням є випадки, коли персональні дані користувача потрібні для виконання угоди. У випадках, коли персональні дані збираються й обробляються для маркетингових цілей, користувач повинен мати можливість не погоджуватися зі збором і обробкою його даних. Компанії, що працюють із персональними даними, також повинні будуть вести облік операцій з персональними даними (тип даних і цілі, для яких вони обробляються), мінімізувати використання персональних даних відповідно до принципу data protection by design, а також проводити внутрішній аудит.

Не менш гостро, ніж проблема захисту персональних даних, у Румунії та Болгарії усвідомлюється небезпечність загроз, що виходять з кіберпростору.

Так, у Румунії на сьогоднішній день активно триває процес розбудови системи кібернетичної безпеки держави як на законодавчому, так і на організаційному рівнях. При цьому ключова роль у забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації, у структурі якої створено національний центр кібербезпеки [12, с. 79–80]. Головною функцією цього центру є поєднання систем технічного захисту із можливостями спецслужби з метою отримання інформації, необхідної для попередження, припинення та подолання наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави [59]. Законопроект «Про кібербезпеку», який у грудні 2014 р. був схвалений сенатом Румунії, також передбачає створення Національної системи кібернетичної безпеки Румунії, технічну координацію

якої покладено на Румунську службу інформації як головного суб'єкта кібербезпеки держави [59].

Національна стратегія забезпечення кібербезпеки Румунії (2013 р.) при цьому передбачає, що Румунія забезпечує функціонування динамічного інформаційного середовища на основі функціональної сумісності й послуг, характерних для інформаційного суспільства, а також забезпечення відповідності основних прав і свобод громадян та інтересів національної безпеки у відповідних правових рамках. Важливим для цього є розвиток культури кібербезпеки користувачів комп'ютерів і телекомунікаційних систем, їх поінформованість щодо потенційних ризиків, а також про можливості їх мінімізації. Збільшення поінформованості щодо ризиків і загроз, пов'язаних з діяльністю, здійснюваною в кіберпросторі, а також способів запобігання та протидії їм вимагають ефективної комунікації й співробітництва між всіма учасниками діяльності у цій сфері, тож Румунська держава бере на себе роль координатора заходів, здійснюваних на національному рівні, забезпечуючи кібербезпеку відповідно до визначених під керівництвом ЄС і НАТО підходів.

З метою забезпечення кібербезпеки Румунії Стратегія визначає наступні цілі: адаптація нормативного й інституціонального підґрунтя до динаміки конкретних загроз у кіберпросторі; встановлення й застосування мінімальних профілів і вимог безпеки для національних кіберсистем, що забезпечують правильну роботу критичної інфраструктури; забезпечення стійкості кіберінфраструктури; забезпечення безпеки шляхом усвідомлення й запобігання уразливостям та ризикам, а також протидії загрозам кібербезпеці Румунії; використання можливостей кіберпростору для просування інтересів, цінностей та національних цілей в кіберпросторі; сприяння та розвиток співробітництва між державним і приватним секторами на національному рівні, а також міжнародне співробітництво у сфері кібербезпеки; розвиток культури безпеки населення шляхом усвідомлення уразливостей, ризиків і загроз з кіберпростору та необхідності захисту власних інформаційних систем; активна участь в ініціативах міжнародних організацій, учасницею яких є Румунія, в

рамках реалізації комплексу заходів щодо зміцнення довіри до міжнародного використання кіберпростору. Особливу увагу Стратегія приділяє розвитку національних можливостей щодо управління ризиками у сфері кібернетичної безпеки.

На думку Консультативної ради з питань національної безпеки Болгарії, кібербезпека і стабільність мають стратегічне значення для розвитку електронного урядування в Болгарії й досягнення оперативної сумісності в роботі адміністрації в цифровому середовищі шляхом введення загальних стандартів. Відповідно, необхідно прискорене впровадження комплексу заходів щодо забезпечення безпеки електронної ідентичності громадян, а також щодо забезпечення захищеної й оптимізованої сумісності електронної ідентичності з такими компонентами, як електронний підпис. Тож у квітні 2016 р. Консультативна рада представила Парламенту Болгарії проект Національної стратегії кібербезпеки під назвою «Стійка до кібератак Болгарія 2020», яка передбачає реалізацію наступних заходів: ініціювання законодавчих змін з метою остаточного прийняття й транспонування Директиви ЄС і Європейського Парламенту про заходи щодо забезпечення високого загального рівня мережної й інформаційної безпеки в ЄС, а також для захисту політичних і виборчих прав громадян і в кіберпросторі; забезпечення цільових ресурсів, необхідних для створення належного потенціалу для кібербезпеки та удосконалення ІТ-інфраструктури, а також реалізації мережної моделі обміну інформацією й координації між організаціями, відповідальними за кібербезпеку у Болгарії; забезпечення Міністерства внутрішніх справ, Агентства національної безпеки, Міністерства оборони, Міністерства транспорту й Державного агентства розвідки необхідними фінансовими ресурсами з поступовим збільшенням числа експертів з питань кібербезпеки для запобігання й боротьби з кіберзагрозами; організація й проведення національних навчань з кіберстійкості з тестуванням ключових елементів Національної стратегії кібербезпеки й ефективності чинних контрзаходів; зміцнення співробітництва з ЄС і НАТО щодо забезпечення кібербезпеки;

покладання на державні установи обов'язку щодо вчасного інформування компетентних служб щодо фактів здійснених на них кібератак. Національна стратегія була прийнята Радою міністрів Республіки Болгарії 13 липня 2016 р..

Відповідно до п. 4.7.1 Національної стратегії, провідну роль у забезпеченні кіберзахисту країни відіграє Міністерство оборони Болгарії. Ефективне забезпечення кібербезпеки при цьому передбачає розбудову існуючих та створення нових розширених можливостей для кіберзахисту, сумісних з вимогами НАТО і ЄС, а також проведення адекватних структурних і організаційних реформ, зокрема: розробку політики у сфері забезпечення кібербезпеки, розробку відповідної концепції й методичних документів, що передбачають захист національної безпеки шляхом активної протидії кібер- і гібридним загрозам у кіберпросторі; реалізацію інвестиційних проектів для кіберзахисту у рамках спільних ініціатив, у тому числі ініціативи НАТО/ЄС «Smart Defense» та «об'єднання й спільного використання», а також створення можливостей для кібероборони в рамках загального процесу планування у сфері оборони; створення Оперативного центру кіберзахисту відповідно до плану розвитку Збройних сил Болгарії до 2020 р. за допомогою центру NCIRC НАТО із забезпеченням безперервного моніторингу і повної оперативної інтеграції в національну мережу NKOMKS, розвиток колективного потенціалу реагування на кібер- і гібридні загрози на національному й міжнародному рівні; погоджений обмін інформацією про кіберінциденти за допомогою державних установ, НАТО і ЄС, а також співробітництво з діловими й науковими колами; накопичення досвіду у сфері кіберзахисту й підвищення професійної підготовки персоналу шляхом періодичної підготовки й участі в навчаннях, розширення участі у роботі центру кіберзахисту НАТО та інших партнерських центрів; удосконалювання й розвиток взаємодії із промисловістю й науково-дослідними організаціями на основі «кластерної кібероборони»; активну участь у міжнародних програмах НАТО і ЄС у рамках науково-дослідних проектів; адаптація й впровадження моделі ES75 щодо спільного використання ресурсів на національному рівні для професіоналів, інші форми залучення експертів з

кіберпромисловості та наукових кіл. Пункт 7.3 Стратегії передбачає створення механізмів і технічних ресурсів для постійного моніторингу можливих загроз кібербезпеці з точки зору масштабів, джерел і природи (кібер-, гібридні), тенденцій у геополітичному контексті й аналізу національної картини кібербезпеки, а також розвитку здатності застосовувати адекватні форми протидії, в т.ч. підтримувати створення джерел контр-інформаційних впливів [59].

Незважаючи на критику політики забезпечення інформаційної безпеки у наукових колах [55, с. 63], у Молдові діє відносно надійна система протидії кіберзлочинності. Так, ще у 2009 р. Парламентом була ратифікована Конвенція Ради Європи про кіберзлочинність [13]. Крім того, влада Молдови підписала Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах у березні 2012 р. [8]. Парламентом також був прийнятий Закон «Про попередження та боротьбу зі злочинністю у сфері комп'ютерної інформації» у січні 2010 р. [59]. Згідно із цим Законом генпрокуратура Молдови наділена повноваженнями координувати й здійснювати кримінальне переслідування осіб, що вчинили кіберзлочини. Метою Закону є вдосконалення регламентації правовідносин за такими напрямками: запобігання та боротьба з кіберзлочинністю, сприяння провайдерам і користувачам інформаційних систем, співробітництво державних служб із неурядовими організаціями та іншими представниками громадянського суспільства, а також міжнародне співробітництво з організаціями й країнами, що мають досвід у відповідних питаннях. Генеральною прокуратурою з метою сприяння розслідуванням був відкритий Центр розслідування кіберзлочинів, один з відділів якого уповноважений реагувати на випадки загроз безпеці в урядових структурах, бізнесі й громадському секторі.

Також у Молдові здійснено низку інших заходів щодо зміцнення інформаційної безпеки. Так, у результаті ратифікації Факультативного протоколу до Конвенції ООН про права дитини, що стосується торгівлі дітьми,

дитячої проституції й порнографії [44], Конвенції Ради Європи про кіберзлочинність [13] й Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства [33], Молдова стала активним учасником процесу застосування загальної кримінальної політики у сфері боротьби з інформаційною злочинністю, у тому числі злочинами, пов'язаними із онлайн-експлуатацією дітей.

Важливим кроком на національному рівні стало також затвердження Закону Молдови «Про електронний підпис та електронний документ» від 29 травня 2014 р., розробленого з метою підвищення рівня безпеки електронних підписів та приведення у відповідність із міжнародними стандартами й рекомендаціями щодо інфраструктури відкритих ключів [4]. В цілому слід зауважити, що у Молдові розпочато процес приведення чинного законодавства у відповідність до положень Директиви 2006/24/ЄС «Про зберігання інформації, створеної або обробленої при наданні послуг зв'язку загального користування або мереж зв'язку загального користування й внесення змін у Директиву ЄС 2002/58/ЄС» від 15 березня 2006 р. щодо захисту персональних даних [59] тощо.

З метою забезпечення системного підходу й формування державної політики у сфері забезпечення інформаційної безпеки, яка об'єднала б правові, організаційні, технічні, технологічні й фізичні заходи щодо захисту кіберпростору Молдови, а також чіткої регламентації функцій і повноважень підвідомчих структур, Уряд Республіки Молдова Постановою від 31 жовтня 2013 р. № 857 затвердив Національну стратегію розвитку інформаційного суспільства «Moldova digitala 2020» (Цифрова Молдова 2020) і План дій з її впровадження, розроблений Міністерством інформаційних технологій та зв'язку. У Стратегії вперше розглядається проблема створення умов для підвищення ступеня безпеки й довіри до кіберпростору, а ключові дії щодо створення цих умов становлять окрему главу вищезгаданого Плану дій. Стратегія визначає, що використання нових технологій породжує численні можливості розвитку, але й численні ризики й уразливості, що вимагають

підвищеної уваги держави й зацікавлених учасників. Ці ризики характеризуються асиметрією, вираженою динамікою й глобальним характером, що ускладнює їхнє виявлення й протидію за допомогою заходів, пропорційних до ефекту їхньої матеріалізації. То ж попередження і боротьба з кібератаками, у тому числі зі злочинністю в цій сфері є одним із пріоритетів міжнародних організацій, а їх бурхливий ріст на світовому рівні на 600 % з 2005 р. вказує на нагальну необхідність вжиття заходів щодо страхування інформаційної інфраструктури Республіки Молдова від можливих ризиків, пов'язаних з незаконною діяльністю у цій сфері. Важливість цієї проблеми була відзначена у Концепції національної безпеки й Стратегії національної безпеки Республіки Молдова, у яких були встановлені цілі системи забезпечення національної безпеки та загрози у інформаційній сфері [19].

Проект Концепції інформаційної безпеки, схвалений Парламентом Молдови в першому читанні 23 червня 2017 р., викликав у суспільстві неоднозначну реакцію. На думку експертів, останні ініціативи щодо регламентації інформаційного простору містять цілу низку серйозних прогалин, які можуть призвести до зловживань. Зокрема, Концепцію інформаційної безпеки доцільно узгодити із новою Стратегією національної безпеки, однак останній проект Стратегії національної безпеки в червні 2017 р. був відкликаний з Парламенту Президентом, а новий проект досі не розроблений. Крім того, проект Концепції припускає занадто суворий контроль Інтернету з боку деяких держустанов, зокрема Служби інформації та безпеки Республіки Молдова, які зможуть втручатися в діяльність провайдерів, а також контролювати інформаційний простір, включаючи соціальні мережі.

Однак, з урахуванням того, що населення дедалі активніше користується Інтернетом, і на цьому тлі влада починає втрачати контроль над інформацією, це не єдина законодавча ініціатива у сфері інформаційної безпеки, захисту інформації, протистояння кіберзлочинності й боротьби зі зловживаннями в Інтернеті – серед таких ініціатив слід згадати, зокрема, законопроект № 161, більш відомий як «Великий брат», і законопроект № 281, що одержав назву

«Мандат безпеки», який уточнює правила проведення спеціальних розшукових заходів в інформаційному просторі й припускає розширення повноважень спеціальних служб у цій сфері. За оцінками фахівців, спроби держави встановити контроль над інформаційними мережами у спосіб, який передбачається цими законопроектами, не стільки забезпечать ефект безпеки інформаційного простору, скільки вдарить по громадянському суспільству, політичних партіях, простих громадянах, яким обмежать можливості висловлювати свою думку й критичні зауваження на адресу влади [59].

У Білорусі нагляд за інформаційним простором та система обмежень наразі є ключовими елементами державної політики забезпечення інформаційної безпеки, зокрема, державні органи відстежують протестні настрої за допомогою складного російського устаткування для моніторингу, впровадженого телекомунікаційними компаніями. З 2010 до 2015 р. у країні діяла Постанова Оперативно-аналітичного центру при Президентові Республіки Білорусь і Міністерства зв'язку та інформатизації Республіки Білорусь «Про затвердження Положення про порядок обмеження доступу користувачів Інтернет-послуг до інформації, забороненої до поширення відповідно законодавчих актів» від 29.06.10 р. № 4/11, за змістом якої провайдери мали фільтрувати Інтернет-контент відповідно до двох чорних списків url-адрес, один з яких перебував у публічному доступі, а інший – був доступний тільки провайдерам (закритий список містив приблизно 80 url-адрес, доступ до яких було обмежено у державних, культурних і урядових закладах, і включав популярні опозиційні сайти на кшталт Charter97.org і Belaruspartisan.org).

У березні 2010 р. від білоруських провайдерів зажадали більш тісного співробітництва з державними системами спостереження (СОРМ), які здійснює повний он-лайн-нагляд у всій країні, що регламентується значною кількістю нормативно – правових актів. Як і в росії та сусідніх країнах, СОРМ Білорусі дає виконавчим органам і органам національної безпеки можливість здійснювати перехоплення повідомлень з будь-яких комунікаційних каналів з метою боротьби зі злочинністю. Провайдери Інтернет-послуг і оператори

зв’язку зобов’язані встановлювати відповідне устаткування й надавати державним органам цілодобовий доступ до нього. Відповідно до Указу Президента Республіки Беларусь «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет» від 01.02.10 р. № 60, провайдери повинні вести облік IP-адрес, а держава може витребувати інформацію щодо Інтернет-діяльності будь-якого громадянина. З 2007 р. до Інтернет-кафе пред’являється вимога зберігати історію Інтернет-активності користувачів протягом одного року й інформувати виконавчі органі про підозрілі дії.

У Білорусі немає спеціальних законів, присвячених протидії кіберзлочинності, але деякі аспекти регулюються Кримінальним кодексом і законами, що стосуються регламентації діяльності глобальної інформаційної мережі Інтернет. Білорусь також подавала заявку на приєднання до Конвенції про кіберзлочинність, прийнятої в Будапешті в 2012 р. [13], що й визначило необхідність дотримуватись відповідних міжнародних стандартів. Це був доволі неочікуваний для Білорусі крок, особливо у контексті тісних зв’язків з росією, адже Китай і росія виступили проти конвенції й висловилися на захист альтернативної концепції боротьби з кіберзлочинністю, у рамках якої держава одержувала значно більше повноважень, ніж це передбачалося Будапештською конвенцією.

За розслідування комп’ютерних злочинів у Білорусі відповідає спеціальне управління Міністерства внутрішніх справ, яке координує роботу з іншими виконавчими органами в Білорусі й аналогічними міжнародними організаціями в США, Євросоюзі, країнах СНД і в інших державах. У суспільстві висловлюються непоодинокі підозри, що це управління має справу здебільшого з переслідуванням порушників кримінального кодексу й не займається розробкою законодавства з питань кібербезпеки, а також бере участь у переслідуванні та он-лайн-відстеженні політичних активістів [10].

Наразі країни Східної Європи вважають вирішення проблеми забезпечення інформаційної безпеки особи, суспільства, держави, їх захисту від

внутрішніх та зовнішніх, у тому числі гібридних загроз, одним з найбільш важливих стратегічних пріоритетів забезпечення національної безпеки.

Україна має співпрацювати з іншими країнами Східної Європи у розбудові систем регіональної та міжнародної інформаційної безпеки з метою протидії загрозам стратегічній стабільності, таким, як кібертероризм та кіберзлочинність, орієнтуючись при цьому на стандарти ЄС та НАТО.

В цьому контексті для України є важливим досвід країн Східної Європи щодо приведення національного законодавства у відповідність до вимог вказаних міжнародних організацій, передусім – щодо забезпечення балансу між свободою й безпекою в інформаційній сфері на законодавчому рівні.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

3.1. Пріоритетні напрями удосконалення законодавства у сфері забезпечення інформаційної безпеки в умовах цифрової трансформації

Формування принципово нового технологічного середовища з урахуванням цифрових технологій істотно впливає на економіку, політику та соціальні процеси сучасного світу. Вплив цифрової революції поширився на систему права на національному та на міжнародному рівні. Передові цифрові технології, що застосовуються в різноманітних галузях діяльності, які охоплюють Інтернет речей (Internet of things), штучний інтелект і машинне навчання (Artificial intelligence & Deep learning), технології на принципах розподіленого реєстру (Blockchain), хмарні комп'ютерні сервіси та обчислення (Cloud computing), розумні комплекси та пристрої (Smart everything), великі дані (Big Data), віртуальна та доповнена реальність (Augmented & additive reality), сучасні біоінженерні технології (Biotech), системи кібербезпеки (Cybersecurity), соціальні мережі (Facebook, *Instagram,* Twitter), цифрові двійники (Digital twins), цифрові технологічні платформи (агрегатори) та пов'язані з ними інші технології, створили технологічний базис для формування принципово нового середовища адміністративно-правового та інформаційно-правового регулювання.

Застосування цифрових технологій у зв'язку зі стратегічною спрямованістю європейського та національного розвитку цифрової економіки, цифровізації різноманітних сфер діяльності зумовили зростаючий науковий інтерес до теоретичних та науково-практичних досліджень, у тому числі в галузі правового регулювання забезпечення інформаційної безпеки. Перспективи розвитку інформаційного права багато в чому пов'язані з

використанням цифрових технологій у сфері забезпечення інформаційної безпеки.

Питання про значення інформаційної безпеки в житті суспільства та кожного з нас не потребує додаткового обґрунтування, але, безсумнівно, потребує пильної уваги. В інформаційному суспільстві, заснованому на знаннях, роль інформаційної безпеки визначається потребою реалізації права людини на інформацію, позбавлення деструктивного інформаційного впливу, необхідністю забезпечення системи стратегічного планування та розвитку національного інформаційного середовища.

Розробка методологічних, організаційних і нормативно-правових засад побудови системи інформаційної безпеки розпочалася у 90-ті роки минулого століття, але не втратила актуальності сьогодні для забезпечення інтересів особи, суспільства та держави.

Сукупність національних документів стратегічного планування, охоплюючи ухвалені стратегії та доктрини, сьогодні значною мірою характеризує основні цілі, завдання та напрями розвитку інформаційної безпеки. Серед інших важливих завдань Стратегія інформаційної безпеки України передбачає розвиток механізмів електронної взаємодії між органами державного управління України, місцевими органами державної влади з державними позабюджетними фондами, фізичними та юридичними особами в межах концепції електронного уряду.

В умовах динаміки інформаційного суспільства інформаційна безпека набуває характеру стратегічного ресурсу в системі цифровізації управління, оскільки цифрові технології, перебуваючи у постійному розвитку та розширюючи доступ до інформації на основі електронної взаємодії різних суб’єктів, створюють умови для переходу державного управління на новий рівень та підвищення якості життя населення, що потребує наукового осмислення з позиції інформаційного права та подальшого вдосконалення правового регулювання відносин в інформаційній сфері.

Велику роль в умовах цифровізації мають питання реалізації

конституційного права на інформацію, забезпечення права на достовірну інформацію, що охоплює інформаційна безпеки.

Юридичні ознаки забезпечення інформаційної безпеки вказують на первинну публічно-правову природу та самостійність, що дозволило визначити зазначений інститут у двох аспектах: вузькому та широкому. У широкому аспекті забезпечення інформаційної безпеки – правовий елемент інформаційної діяльності держави, спрямований на реалізацію державної політики у соціально-інформаційній та економічній сфері шляхом створення умов захисту інформації, інформаційних систем і ресурсів та захисту від деструктивного інформаційного впливу. У вузькому аспекті забезпечення інформаційної безпеки є самостійним елементом в структурі інформаційного права, створеним та регульованим спеціальними нормативно-правовими актами.

У документальному аспекті інформаційна безпека охоплює сукупність нормативно-правових актів та ненормативно-правових актів, довідкові, нормативно-технічні документи, документи стратегічного планування, програмно-цільові документи, ненормативні правові акти, правові знання, правова статистика, акти правозастосовної практики, акти тлумачення законодавства, правові коментарі тощо.

Нормативно-правові документи, інформаційні ресурси є складовою інформаційної системи і належать до інформаційної інфраструктури, входять до системи забезпечення інформаційної безпеки України.

Право на достовірну інформацію багато в чому пов’язане з тим, що Стратегія інформаційної безпеки Україні закріплює поступовий перехід від інформаційного суспільства до суспільства знань, у якому переважне значення з урахуванням національних пріоритетів мають отримання, збереження, виробництво та розповсюдження. достовірної інформації, що забезпечується заходами та засобами інформаційної безпеки [47].

Під нормативною базою інформаційної безпеки у широкому сенсі слід розуміти всю сукупність правових знань, що охоплюють не лише нормативно-правові акти, а й документи стратегічного планування, програмно-цільові

документи, акти правозастосовної практики, акти тлумачення законодавства, коментарі до законів.

У вузькому значенні під нормативною базою інформаційної безпеки слід розуміти масив нормативно-правових актів та тісно пов'язаних з ними актів та документів правового змісту – акти тлумачення, довідкові матеріали, нормативно-технічні документи тощо.

Оскільки у формуванні системи нормативно-правових актів беруть участь місцеві органи влади та органи місцевого самоврядування, необхідно на основі досягнень цифровізації та системного підходу виявити однорідні та суттєво взаємопов'язані компоненти наявної нормативної бази інформаційної безпеки для об'єднання їх у систему нормативного забезпечення інформаційної безпеки.

Зазначена система є впорядкованою багаторівневою сукупністю інформаційних ресурсів нормативно-правового характеру на базі сучасних інформаційних технологій, єдиного програмно-апаратного середовища, що надає функціонально повний набір інформаційно-технологічних сервісів, які забезпечують збирання, обробку, зберігання, надання та передачу інформації з метою підвищення інформаційної безпеки та безпеки критичної інформаційної інфраструктури.

Охоплення інформаційних технологій системою інформаційної безпеки, формування, розвиток та подальше вдосконалення державної системи інформаційної безпеки є важливими складовими національної безпеки держави що має суттєве значення в умовах збройної агресії росії щодо України.

Управління процесами забезпечення інформаційної безпеки має перебувати у підпорядкуванні держави, яка згідно з Конституцією України зобов'язана забезпечити права, свободи та законні інтереси фізичних і юридичних осіб на основі достовірної та актуальної інформації, захисту від інформаційного деструктивного впливу. Для цього потрібний науково-технічний потенціал та використання цифрових технологій для забезпечення інформаційної безпеки, що відповідає всім необхідним сучасним параметрам безпеки.

На основі розвитку правової культури інформаційного суспільства та правосвідомості вимагають уваги такі визнані інститути правового регулювання у сфері забезпечення інформаційної безпеки, як юридична техніка, експертиза нормативно-правових актів, застосування цифрових технологій у юридичній діяльності, правового моніторингу, використання різноманітних форм контролю та оцінки якості законодавства та ефективності застосування права.

Аналіз чинного законодавства показав наявність розвиненої системи правового забезпечення інформаційної безпеки. Водночас є прогалини у правовому регулюванні. У зв'язку з надзвичайно високою динамічністю розвитку інформаційної сфери в умовах цифрової трансформації необхідно виробляти правові рішення, що дозволяють успішно підготуватися до появи нових інформаційних загроз.

Одна з прогалин у чинному інформаційному законодавстві полягає в тому, що за наявності широкого переліку правових механізмів забезпечення інформаційної безпеки у базових джерелах інформаційного права є брак основоположних положень та засад інформаційної безпеки.

Для іншого ключового елемента інформаційної безпеки – захисту інформації такі основні норми закріплені у Законі України «Про захист інформації у інформаційно-комунікаційних системах».

Стаття 1 «Визначення термінів» і 9 «Забезпечення захисту інформації в системі» закону закріплює правову дефініцію захисту інформації, визначає методи та зміст державного регулювання відносин у цій сфері, встановлює низку правових обов'язків та вимог щодо захисту інформації.

Причина очевидна – назва цього закону адекватно відображає його предмет регулювання, але блок інформаційної безпеки виходить за межі захисту інформації.

Має місце, коли передові вітчизняні розробки у сфері правового регулювання отримують підтримку, але не знаходять втілення у законодавстві. Закріплення блоку норм про поняття, правові принципи та засоби забезпечення

інформаційної безпеки дуже важливе.

Надання інформаційної безпеки статусу стратегічного національного пріоритету у Стратегії інформаційної безпеки України вимагає зміни ситуації, що склалася, та повноцінної правової регламентації основ забезпечення інформаційної безпеки на рівні закону.

Тому доцільною є пропозиції про доповнення змісту Закону України «Про інформацію» нормами щодо забезпечення інформаційної безпеки. Пропозиція полягає у внесенні до закону окремої статті щодо забезпечення інформаційної безпеки (Захист інформації охоплює захист від неправомірного доступу, знищення, блокування, копіювання, надання, розповсюдження від інших неправомірних дій, від деструктивного інформаційного впливу, що завдає шкоди здоров'ю).

Таке рішення забезпечить побудову логічної та цілісної системи правового регулювання інформаційної безпеки, що охоплює спочатку базові відправні засади забезпечення, а потім правові норми щодо двох фундаментальних напрямів забезпечення – захисту інформації та інформаційної безпеки.

Однак таке широке коло питань забезпечення інформаційної безпеки доцільно нормативно закріпити в документі стратегічного планування. Механізм практичного використання може бути різним – як використання основи для розробки офіційного документа стратегічного планування з такою назвою, так і застосування під час оновлення Стратегії інформаційної безпеки України. Кожне з рішень має переваги та недоліки.

Наприклад, основним аргументом на користь варіанта єдиного документа є тісний взаємозв'язок інформаційно-психологічних та інформаційно-технічних загроз, так само як діяльність державних органів щодо протидії. Щодо законодавства у сфері забезпечення інформаційної безпеки, то оптимальною стратегією розвитку є закріплення правових засад забезпечення інформаційної безпеки у Законі України «Про інформацію» у поєднанні з регламентацією окремих напрямів та аспектів забезпечення інформаційної безпеки у

самостійних законодавчих актах.

У цифровій сфері важливе значення мають інформаційні системи та офіційні сайти органів публічного управління, надання адміністративних послуг органами публічного управління, що здійснюється на основі інформаційних систем.

Інформаційні системи, що містять правову інформацію, яка застосовується у сфері публічного управління та судової системи, є базою інформаційно-правового забезпечення організаційно-управлінської діяльності органів публічної влади, судової діяльності у сфері інформаційної безпеки, що дозволяє розвивати державні інформаційні системи у різних галузях діяльності із забезпеченням вимог інформаційної безпеки.

У базовому нормативному акті щодо державних інформаційних ресурсів Закон України «Про публічні електронні реєстри» безпосередньо не згадується інформаційна безпека. Водночас зазначений закон доцільно доповнити словами: «Вимоги про захист інформації, які містяться в реєстрах, встановлюються центральним органом виконавчої влади зі спеціальним статусом у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв’язку» [45].

Аналіз європейського досвіду свідчить про успішність переведення органів публічної влади на сервісні моделі споживання хмарних сервісів, центрів обробки даних з метою підвищення стабільності роботи інформаційно-комунікаційних систем, підвищення безпеки інформації, що міститься в інформаційних ресурсах, зменшення витрат на розвиток інформаційно-комунікаційної інфраструктури, охоплюючи хмарні сервіси.

12 березня 2022 р. Кабінет Міністрів України дозволив українським державним установам у воєнний час користуватися хмарними технологіями з розміщенням даних у закордонних дата-центрах. Реалізація розміщення даних у закордонних дата-центрах вимагає внесення доповнень до закону України, що регулює надання хмарних послуг.

Доцільно доповнити статтю 14 «Захист інформації при наданні хмарних

послуг та/або послуг центру обробки даних» Закону України «Про хмарні послуги» частиною 3 у редакції:

«Державний нагляд за дотриманням вимог з інформаційної безпеки хмарних послуг здійснюється центральним органом виконавчої влади зі спеціальним статусом у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку. Предметом державного нагляду за дотриманням вимог з інформаційної безпеки є дотримання фізичними особами-підприємцями та юридичними особами обов'язкових вимог, встановлених цим законом, іншими законами та прийнятими відповідно до нормативно-правових актів у сфері інформаційної безпеки» [51].

З метою підвищення ефективності інфраструктури електронного уряду в Україні впроваджується єдина платформа цифрової взаємодії, що охоплює єдине програмно-апаратне середовище та методологію, яке підтримує взаємовідносини громадян, державних органів та юридичних осіб на базі сучасних інформаційних технологій. Розроблена концептуальна модель єдиної платформи цифрової взаємодії передбачає поетапний перехід державних інформаційних систем на вказану платформу та впровадження сервісної моделі надання інформаційних послуг в електронній формі, що посилить інформаційну безпеку у певному секторі інформаційного простору країни [2].

В опрацюванні правових актів у сфері інформаційної безпеки беруть участь державні органи та органи місцевого самоврядування. В умовах інформаційного суспільства та цифровізації ключове значення набуває трансформація зазначеної системи в загальнонаціональну систему інформаційної безпеки відповідно до принципів державно-приватного партнерства, що дозволить перейти на наступний рівень правової інформатизації на основі цифрових технологій з метою формування єдиного цифрового інформаційно-правового простору України.

Запровадження нових цифрових технологій, цифрової взаємодії потребує пошуку нових концептуальних підходів і правових методів, механізмів публічного управління за обов'язкового дотримання вимог забезпечення

інформаційної безпеки.

Цифрова трансформація впливає на механізми інформаційно-правової та електронної взаємодії між державою та суспільством, іншими суб'єктами інформаційного обміну, що відповідно вимагає адекватного забезпечення інформаційної безпеки.

Запит на розвиток інформаційної інфраструктури національної системи забезпечення інформаційної безпеки виходить із підвищення правової поінформованості та культури фізичних і юридичних осіб, а також необхідності забезпечення інформаційних потоків різних рівнів лінгвістичними, інформаційними засобами та інструментами, що забезпечують взаємодію громадян із державними інформаційними ресурсами.

Створення єдиного цифрового простору на платформній основі є перспективним, і в рамках реалізації зазначеного підходу можливий розвиток національної системи інформаційної безпеки на основі платформних рішень.

Водночас потрібні відповідні зміни у законодавстві та інтеграція сукупності публічних інформаційних ресурсів та сучасних цифрових технологій, спрямованих на забезпечення взаємодії всіх суб'єктів інформаційного обміну, інтеграція нормативного масиву інформаційної безпеки, що забезпечить її актуальний стан.

У сучасних умовах інформаційна безпека в інформаційному суспільстві набуває характеру стратегічного ресурсу; трансформуючись у систему цифровізації та публічного управління, вона дозволить публічним інформаційним системам перейти на платформне забезпечення та запровадити сучасні сервісні моделі інформаційних послуг на підставі нових правових і технологічних рішень у сфері забезпечення інформаційної безпеки.

Національна система інформаційної безпеки має розвиватися та набути офіційного статусу, бути інтегрованою, багаторівневою та відкритою для взаємодії з іншими інформаційними системами, а її інформаційно-правове забезпечення будуватися на базі конвергентних інформаційних технологій та платформних рішень.

У зазначеному контексті важливо виділити необхідність забезпечення інформаційної безпеки особи та суспільства від деструктивного інформаційного впливу. Провідну роль у структурі цього інституту мають норми інформаційного права. Водночас усталені правові механізми безпеки вимагають подальшого розвитку та адаптації до нових загроз та викликів в умовах цифрової трансформації.

Аналіз інформаційного та іншого галузевого законодавства дозволив виділити такі основні правові механізми забезпечення інформаційної безпеки від деструктивного інформаційного впливу:

– встановлення правових заборон та інших обмежень на поширення певних видів негативної інформації;

– встановлення спеціальних правил обороту інформаційної продукції певних видів;

– закріплення обов’язків суб’єктів інформаційних правовідносин щодо забезпечення інформаційно-психологічної безпеки;

– вікова класифікація та маркування інформаційної продукції;

– експертиза інформаційної продукції;

– ідентифікація особи абонентів, користувачів мережі Інтернет та цифрових сервісів;

– видалення чи обмеження доступу до протиправного контенту;

– встановлення юридичної відповідальності за правопорушення, що посягають на інформаційно-психологічну безпеку;

– правове закріплення заходів контрпропаганди;

– правове стимулювання розвитку цифрової грамотності та формування культури інформаційної безпеки.

Важливу роль у механізмі правового забезпечення інформаційної безпеки відіграють заходи юридичної відповідальності за скоєння правопорушень у цій галузі, які закріплені кримінальним, адміністративно-деліктним і цивільним законодавством. Водночас розширено практику нормативного закріплення санкцій за правопорушення у сфері захисту від деструктивного інформаційного

впливу безпосередньо інформаційним законодавством.

Зазначені правові механізми демонструють доцільність розробки та прийняття окремого Закону України «Про захист від деструктивного інформаційного впливу на населення України».

3.2. Формування культури інформаційної безпеки

З кожним роком зростає потреба у забезпеченні інформаційної безпеки особи, держави та суспільства. Збільшення обсягів використання мережі Інтернет розширює масштаби інформаційних загроз, пов'язаних із діяльністю представників кіберзлочинності, розв'язуванням інформаційних воєн, комп'ютерними атаками хакерів на державні та приватні інформаційні ресурси, які є критично важливими для існування держави та суспільства.

Інша важлива небезпека використання мережі Інтернет у тому, що потужність формованого інформаційного потоку значно перевищує можливості освоєння та застосування інформації людьми. У сприйнятті світу зміщується акцент із наукового, освітнього та культурного на розважально-довідковий. Це формує кліпове мислення, що характеризується поверхневим сприйняттям інформації, падінням здібностей до аналізу, спрощенням поглядів та переваг людей, що сприяє формуванню нав'язаних моделей поведінки.

Необхідно брати до уваги, що при сучасних темпах розвитку інформаційних технологій та інформаційного простору жоден управлінський апарат не в силах вчасно встановлювати необхідні механізми та адаптувати державне регулювання зазначеної сфери до обставин, що постійно змінюються. Цей факт призводить до необхідності забезпечення інформаційної безпеки.

При розгляді основних напрямів забезпечення інформаційної безпеки у різних галузях переважає необхідність забезпечення безпеки держави та суспільства. Інтереси особи та забезпечення інформаційної безпеки окремих громадян розглядаються локально, причому як напрям забезпечення інформаційної безпеки в галузі науки, технологій та освіти, фігурує

забезпечення захищеності громадян від інформаційних загроз, у тому числі шляхом формування культури особистої інформаційної безпеки.

В умовах посилення цифрової трансформації зростає значення адаптації громадян до нових реалій в умовах цифрового середовища, підвищення поінформованості та набуття навичок протистояння інформаційним загрозам та ризикам. Водночас в умовах інформаційної війни, яку проводить російська федерація, основна увага в державній політиці надається боротьбі з загрозами інформаційної безпеки. Це правильно, оскільки завдання держави полягає в тому, щоб максимально захистити особу та соціум від деструктивного впливу інформаційних ризиків.

Однак донині в експертній спільноті склалося розуміння того, що в інформаційному середовищі не можна уникнути будь-яких факторів, що утворюють загрози. Це зумовлено багатьма причинами: складністю виявлення загроз інформаційній безпеці, латентним характером дії, чисельністю джерел загроз інформаційній безпеці, обмеженою ефективністю методів припинення поширення деструктивної інформації.

Не можна забувати про те, що в правовій демократичній державі ступінь втручання в суспільне життя, у тому числі в духовну сферу, має бути лімітованим.

Спроби державного директивного нав’язування поглядів та цінностей, припинення будь-якого інакомислення несумісні з принципами демократичного устрою. Ці ідеї знайшли відображення в Конституції України, що закріплює принципи ідеологічного та політичного плюралізму, свободу думки, слова та інформації, гарантованість свободи масової інформації та допускає суворо лімітоване обмеження прав та свобод.

Слід наголосити, що поняття «культура особистої інформаційної безпеки» може мати широке тлумачення, яке не несе певної конкретики, оскільки його розшифрування в нормативних документах не відображено.

Культура особистої інформаційної безпеки - одна із складових загальної культури людини та її інформаційної культури. Культура охоплює сукупність

інформаційного світогляду та системи спеціальних знань, що забезпечують самостійну діяльність із задоволення індивідуальних інформаційних потреб з використанням інформаційно-комунікаційних технологій та автоматизованих систем на принципах захищеності особистої інформації та підтримувальної інфраструктури від випадкових чи навмисних впливів природного чи штучного характеру, які можуть завдати збитків особі.

Для того, щоб сформувати культуру особистої інформаційної безпеки, необхідно коригувати систему формування світогляду, знань та умінь, пов'язаних із виробництвом, перетворенням, використанням та зберіганням інформації. Для формування культури особистої інформаційної безпеки доцільно:

– проводити заходи у галузі духовно-морального виховання громадян;

– формувати та розвивати правосвідомість громадян та відповідальне ставлення до використання інформаційних технологій, у тому числі споживчу та користувальницьку культуру;

– забезпечити створення та розвиток систем нормативно-правової, інформаційно-консультативної, технологічної та технічної допомоги у виявленні, попередженні, запобіганні та відображенні загроз інформаційній безпеці громадян та ліквідації наслідків прояву;

– удосконалювати механізми обмеження доступу до інформації, поширення якої в Україні заборонено законом, та її видалення;

– удосконалювати механізми законодавчого регулювання діяльності традиційних і нових засобів масової інформації (Інтернет, телебачення, соціальні мережі, вебсайти в мережі Інтернет, месенджери);

– забезпечити використання сучасних інформаційних платформ для поширення достовірної та якісної інформації, наповнення національного інформаційного простору доступними, якісними та легальними медіапродуктами та сервісами.

Зазначені заходи, які проводяться за допомогою апарату публічного управління, можуть допомогти сформувати культуру особистої інформаційної

безпеки. Робота з її формування має вестися на всіх рівнях.

У зв'язку з цим потрібне посилення іншого магістрального спрямування забезпечення інформаційної безпеки – підвищення життєстійкості об'єктів інформаційної безпеки, їх здатність самостійно блокувати або знижувати до прийнятних значень деструктивний вплив загроз інформаційної безпеки. Це завдання можна позначити як формування інформаційного імунітету особистості та суспільства.

А. Ю. Геворкян запропонував комплексний проєкт формування сталої культури інформаційної безпеки українського суспільства, у якому зібрані всі основні аспекти та елементи системи інформаційної безпеки та наведено їх взаємозв'язок із головним завданням держави – зміцненням національної безпеки. Це три взаємопов'язані блоки для досягнення максимального ефекту від запровадження та реалізації:

– теоретико-правові основи формування культури інформаційної безпеки суспільства;

– визначення основних викликів і загроз інформаційній безпеці;

– визначення короткострокових і стратегічних завдань державної політики в галузі формування культури інформаційної безпеки суспільства [3, с. 176].

У правових актах та науковій літературі цей напрям забезпечення безпеки зазвичай позначається як формування інформаційної грамотності та цифрової компетентності, культури інформаційної безпеки.

Проведення політики держави щодо підвищення цифрової та інформаційної грамотності населення є важливим інструментом формування довіри суспільства до цифрових технологій.

Відповідні положення закріплені в документах стратегічного планування. У Стратегії інформаційної безпеки України та Національній економічній стратегії на період до 2030 р. окреслено завдання формування культури особистої інформаційної безпеки.

Національна економічна стратегія на період до 2030 р. закріплює, що для

створення інформаційного простору знань потрібні розвиток правосвідомості громадян та відповідальне використання інформаційно- комунікаційних технологій.

У Концепції виховання дітей та молоді в цифровому просторі як базові засади державної політики названо: необхідність формування в дітей вміння орієнтуватися в сучасному інформаційному середовищі, виховання навичок самостійного та критичного мислення та навчання медіаграмотності [53].

У 2002 р. Генеральна асамблея ООН ухвалила резолюцію, присвячену створенню глобальної культури кібербезпеки «Утворення глобальної культури кібербезпеки». У преамбулі зазначається, що забезпечення кібербезпеки залежить не тільки від роботи правоохоронних структур, а й від превентивних заходів, обізнаності та відповідальності власників та користувачів інформаційно-комунікаційних технологій. Останні два аспекти закріплені серед елементів глобальної культури кібербезпеки у додатку до резолюції.

Ще до активного розвитку Інтернету, у європейських країнах за активної підтримки ЮНЕСКО сформувався специфічний напрям «медіа освіта» (media education), покликаний допомогти школярам та студентам краще адаптуватися у світі медіакультури та спрямований на досягнення медіаграмотності (media literacy).

Медіаграмотність – це комплекс знань, навичок і вмінь, що дозволяють розуміти, аналізувати та критично оцінювати медіа та їхні сюжети та статті, визначається як грамотне використання інструментів, що забезпечують доступ до інформації, розвиток критичного аналізу змісту інформації та прищеплення комунікативних навичок [18].

З появою та зростанням популярності Інтернету дослідники почали говорити про «цифрову грамотність» як здатність критично розуміти та використовувати інформацію, одержувану за допомогою комп’ютера в різних форматах із широкого діапазону джерел. Цифрова грамотність – це наявність навичок, необхідних для життя, навчання і роботи в суспільстві, де спілкування і доступ до інформації здійснюється за допомогою цифрових технологій

(інтернет-платформи, соціальні мережі, мобільні пристрої тощо).

Істотне зростання можливостей Інтернету та входження у повсякденне життя людини привели дослідників до акцентування уваги на понятті цифрової компетентності. Цифрова компетентність – здатність впевнено, ефективно, критично та безпечно обирати та застосовувати інформаційно-комунікаційні технології у різних сферах життєдіяльності (інформаційне середовище, комунікації, споживання, технічна сфера), готовність до такої діяльності.

За останні десятиліття в країні підготовлено комплекс наукових та методичних праць, присвячених формуванню інформаційної (медійної, цифрової) грамотності та культури інформаційної безпеки.

Виділяють чотири різновиди цифрової компетентності: інформаційна та медіакомпетентність, комунікативна, технічна та споживча компетентність. Методологічним підходом до формування культури інформаційної безпеки є цифрова (кібер) гігієна.

Як зазначається на вебсайті Міністерства та Комітету цифрової трансформації , цифрова гігієна – це грамотне споживання інформації, а також дотримання базових правил кібербезпеки: не використовувати один і той самий пароль на всіх акаунтах, застосовувати двохфакторну ідентифікацію, регулярно здійснювати резервне копіювання та оновлення [61]. Експерти сформулювали правила кібергігієни, що охоплює безпечне зберігання паролів, використання багатофакторної автентифікації.

Для інформаційної безпеки більше значення мають правила цифрової гігієни: не видавати особистої інформації; не вірити та не довіряти незнайомцям; не викладати нічого важливого у хмару; бути уважним та усвідомленим; пам’ятати та дбати про майбутнє; розпізнавати маніпуляцію та маніпуляторів; дотримуватися розумної помірності; бути джерелом знань.

Аналізуючи зв’язок цифрової компетентності та зіткнення з онлайн ризиками, дослідники дійшли висновку про наявність прямої кореляції між ними. Чим частіше користувач зіштовхувався з онлайнризиками, тим вищий у нього рівень цифрової компетентності. Однак такий спосіб формування

цифрової компетентності є небезпечним, оскільки може спричинити неприйнятну шкоду. Головне завдання полягає в навчанні дітей, батьків, вчителів та інших категорій громадян навичок та вмінь, які складають зміст цифрової грамотності (компетентності).

У цьому напрямі в Україні за останнє десятиліття виконано певну роботу. Проводяться виміри рівня цифрової обізнаності, запущено портал цифрової грамотності, у закладах освіти проводяться уроки кібербезпеки.

Міністерством цифрової трансформації України відповідно до Концепції розвитку цифрових компетентностей та плану заходів щодо її реалізації розроблені Рамки цифрової компетенції для громадян України [23]. Це інструмент щодо покращення цифрової компетенції українців, спрямованих на підвищення цифрової грамотності та практичного використання сервісів ІТ технологій конкретними групами населення.

Якщо говорити безпосередньо про Україну, то 53% громадян володіли цифровою грамотністю нижче за базовий рівень, за даними дослідження 2019 р.. У 28% громадян вище за базовий рівень. Лише 11% українців можуть розпізнати неправдиву інформацію в Інтернеті [62].

В. Є. Іонан, заступник Міністра цифрової трансформації України з питань євроінтеграції, вказує, що багато хто, як і раніше, має недостатні знання та навички у сфері цифрових технологій. Цифрова грамотність населення у першій половині 2021 р. оцінюється: ситуація з комунікацією та взаємодією у цифровому суспільстві: 27% на високому рівні, 69% на середньому рівні; з розв’язанням проблем у цифровій середовищі та навчанням протягом життя: 20% на високому рівні, 77% на середньому рівні. Навички безпеки у цифровій середовищі: лише 14% на високому рівні, 82% на середньому рівні. Ще гірша ситуація зі створенням цифрового контенту: лише 10% на високому рівні, 83% на середньому рівні [11].

Важливим напрямом роботи з формування культури інформаційної безпеки є стимулювання проєктів підвищення медійної та цифрової грамотності громадян. Робота в цій галузі ведеться різними громадськими організаціями

національного та місцевого рівнів, причому нерідко з власної ініціативи. Потрібне подальше посилення державної підтримки цього напряму громадської активності.

Наказом Міністерства освіти і науки України затверджено Типову програму підвищення кваліфікації педагогічних працівників із розвитку цифрової компетентності, яка розроблена відповідно до сучасних вимог суспільства [60].

У 2019 р. було запущено тематичний інтернет-портал «Цифрова грамотність». На місцевому рівні діють численні проєкти підвищення медійної та цифрової грамотності.

Крім освіти як основної форми підвищення цифрової грамотності та культури інформаційної безпеки, важливе значення має інформаційно-просвітницька робота. Вона спрямована на розвиток критичного мислення, підвищення поінформованості про загрози інформаційній безпеці (хибні новини, маніпуляцію свідомістю, шахрайство та ін.) та правила реагування на них. Формами ведення інформаційно-просвітницької роботи є створення та поширення тематичних інформаційних матеріалів (плакатів, пам’яток, роликів), інтернет-ресурсів, проведення навчальних занять та інших профілактичних заходів.

Запит на здобуття знань про правила безпеки в цифровому середовищі є в суспільстві. Дослідження аналітичного центру Разумкова показало, що громадяни переймаються власною інформаційною безпекою. Більше половини опитаних хотіли б дізнатися про те, як краще захиститися від цифрових загроз та розвинути навички безпечного використання цифрових пристроїв та технологій, про інструменти особистої цифрової безпеки, люди відчувають інформаційний дефіцит [56]. Потрібна подальша активізація інформаційно-просвітницької роботи інститутів громадянського суспільства в розглянутій сфері за державної підтримки.

На сучасному етапі розвитку України немає можливості повністю позбавити людину інформаційних загроз або зменшити потік новин. Отже,

необхідно вживати заходів забезпечення інформаційної безпеки. Використовувати варто не лише технічні методи, а й соціальні технології. Особливу увагу слід звернути на необхідність удосконалення освітньої системи, яка сьогодні не повною мірою відповідає вимогам інформаційного суспільства та захисту від деструктивного інформаційного впливу російського медіасередовища.

Виховання критичного мислення шляхом вивчення питань інформаційної безпеки дозволить уникнути руйнівних психологічних наслідків інформаційних воєн для особистості та дозволить уникнути маніпулятивних технологій російських політичних шахраїв, які активно ведуть діяльність у мережі Інтернет. Грамотний підхід до освіти дітей і молоді з питань інформаційної безпеки дозволить сформувати правильне ставлення до необхідності збереження цілісності, достовірності та доступності інформації, зробить внесок у формування культури особистої інформаційної безпеки, що дозволить успішно посісти своє місце в інформаційному суспільстві.

У правовій системі України забезпечення інформаційної безпеки багато в чому забезпечує стабілізацію та ефективний розвиток національного інформаційного простору в умовах цифрової трансформації, що дає змогу забезпечити перехід від інформаційного суспільства до суспільства знань, в основі якого лежить забезпечення безпеки всіх інформаційних процесів.

Щодо цифрових технологій інформаційна безпека набуває особливого значення, є обов’язковою умовою забезпечення стану захищеності в цифровому середовищі, у різних інформаційних просторах, заснованих на цифрових даних; достовірності інформації, пов’язаної з функціонуванням системи органів публічної влади на різних цифрових платформах, наданням на їх основі адміністративних послуг.

Нормативно-правові акти, якими здійснюється регулювання інформаційної безпеки є специфічними техніко-юридичними правовими актами, але ця специфіка не береться до уваги суб’єктами нормотворчості.

Аналіз дозволив виділити низку напрямів розвитку законодавства у сфері

забезпечення інформаційної безпеки: закріплення базових положень про інформаційну безпеку, у тому числі принципів інформаційної безпеки, прав та обов'язків, пов'язаних із забезпеченням інформаційної безпеки та інституту юридичної відповідальності; регулювання питань у сфері поширення відомостей, заборонених законодавством, регулювання забезпечення інформаційної безпеки у масових комунікаціях; забезпечення інформаційної безпеки в державних інформаційних системах та реєстрах; регулювання протидії поширенню фейкової інформації та дезінформації.

Удосконалення законодавства у сфері забезпечення інформаційної безпеки є юридичною діяльністю, спрямованою на покращення ефективності засобів і заходів інформаційної безпеки, що здійснюється різними способами в залежності від того аспекту, у якому напрямі інформаційного простору безпека є об'єктом удосконалення.

Для забезпечення інформаційної безпеки людини та суспільства недостатньо соціально-владного, службово-розпорядчого, охоронно-захисного та техніко-технологічного інструменталізму, а необхідне розуміння гуманітарного характеру цієї проблеми, що досягається узгодженням балансу інформаційних інтересів людини як особистості та громадянина, і інформаційних інтересів суспільства та держави, що відображається в культурі інформаційної безпеки. Культура інформаційної безпеки повинна бути зорієнтована на забезпечення інформаційної безпеки, яка становить серцевину державної інформаційної політики, є визначальним фактором забезпечення інформаційного суверенітету України та інформаційної підтримки територіальної цілісності та суверенітету, захисту особи та суспільства від деструктивного інформаційного впливу.

Проблема формування культури інформаційної безпеки особи та суспільства в умовах системних перетворень національної економіки, захисті територіальної цілісності як адекватної відповіді на виклики зовнішнього та внутрішнього інформаційного середовища набула безпосередньо практичного значення та гранично актуалізує суб'єктно-особистісний вимір. Адекватна

відповідь на виклик інформаційного середовища залежить від стилю правового мислення громадянина, його ціннісних орієнтацій.

Аналіз динамічного розвитку загроз у сфері деструктивного інформаційно-психологічного впливу на особу та суспільство вимагає нових засобів забезпечення інформаційної безпеки, у зв'язку з чим існує об'єктивна необхідність продовження досліджень різних аспектів формування культури інформаційної безпеки як основного засобу протидії деструктивним впливам.

Планомірне, систематичне та послідовне удосконалення діяльності щодо розвитку культури інформаційної безпеки на засадах національних інтересів потребує упорядкування нормативної бази цього важливого самостійного постійного напряму діяльності, яка сьогодні є хаотичною та суперечливою. Цей процес набув характеру гострої проблеми, яка вимагає невідкладного вирішення.

ВИСНОВКИ

Проведене досліджене дозволяє зробити наступні узагальнюючі висновки:

1. Інформаційна безпека виходить на перше місце в системі національної безпеки, у зв'язку з цим стало доцільним розглядати інформаційну безпеку як складову державної інформаційної політики. Разом з цим, інформаційна безпека є самостійною складовою національної безпеки і в цьому проявляється її подвійний характер. Підходи до дослідження інформаційної безпеки в складі державної інформаційної політики та визначення поняття «інформаційна безпека» дають змогу розглядати дану проблему комплексно та системно. Ми вважаємо, що найприйнятнішим є інтегральний підхід, який дає можливість зробити висновок, що інформаційна безпека не може розглядатися лише в якості окремого стану, вона є і властивістю, і атрибутом інформаційного суспільства, і діяльністю, і результатом діяльності людини, спрямованої на забезпечення певного рівня безпеки в інформаційній сфері.

2. Характеризуючи систему правового забезпечення інформаційної безпеки в умовах цифрової трансформації, доцільно зазначити міжгалузевий характер і складну внутрішню структуру (охоплює конституційно-правові, адміністративно-правові, інформаційно-правові, цивільно-правові, кримінально-правові, міжнародно-правові елементи та взаємозв'язки між ними), що перебуває в динамічному розвитку. Взаємопов'язаними вимірами правового регулювання забезпечення інформаційної безпеки є ціннісний, нормативно-правовий, функціональний та інституційний. Ціннісний вимір забезпечення інформаційної безпеки вказує, що зазначений правовий феномен перебуває у складних системних зв'язках із конституційними цінностями та слугує забезпеченню суспільно корисних цілей – гарантованості й захищеності людини, суспільства та держави. Нормативно-правовий вимір передбачає фіксацію на законодавчому рівні адміністративно-правових засобів і механізмів, їх основних видів, підстав і особливостей застосування.

Функціональний вимір вказує, що нормативне закріплення інформаційної безпеки сприяє реалізації низки суспільно важливих функцій: поновлення права, компенсаторної, правоохоронної, каральної, виховної.

3. Адміністративно-правове забезпечення інформаційної безпеки – це врегульована нормами адміністративного права державно-управлінська діяльність публічних органів влади та посадових осіб з виявлення деструктивного інформаційного впливу на інформацію у контексті її захисту, особу, суспільство та державу, запобігання розповсюдженню шляхом блокування або видалення, що здійснюється на основі застосування відповідних адміністративно-правових заходів. Адміністративно-правові засоби запобігання інформаційної безпеки – це способи адміністративно-правового впливу держави на осіб, які здійснюють інформаційну діяльність щодо запобігання правопорушенням в інформаційному просторі України. Механізм адміністративно-правового регулювання у сфері забезпечення інформаційної безпеки – юридично закріплена, організована система адміністративноправових засобів, що становить нормативно-правову, інституційну та інструментальну основу для досягнення відповідно до певних юридичних процедур цілей у галузі забезпечення стану захищеності інформації, особи, суспільства та держави та національних інтересів від можливого деструктивного інформаційного впливу їх наслідків.

Аналіз інформаційного та галузевого законодавства дозволив виділити основні адміністративно-правові механізми забезпечення інформаційної безпеки: встановлення правових заборон та інших обмежень на поширення певних видів негативної інформації; встановлення спеціальних правил обігу інформаційної продукції певних видів; закріплення обов’язків суб’єктів інформаційних правовідносин щодо забезпечення інформаційної безпеки; експертиза інформаційної продукції; ідентифікація особи абонентів, користувачів мережі Інтернет та цифрових сервісів; видалення чи обмеження доступу до протиправного контенту; встановлення юридичної відповідальності за правопорушення, що посягають на інформаційно-психологічну безпеку;

правове закріплення заходів контрпропаганди; правове стимулювання розвитку цифрової грамотності та формування культури інформаційної безпеки.

4. Узагальнюючи зарубіжний досвід забезпечення інформаційної безпеки, зазначено, що значна кількість держав світу приділяє особливу увагу інформаційній безпеці, створюють спеціальні органи і підрозділи для боротьби з інформаційними війнами. Основними напрямами забезпечення інформаційної безпеки у країнах Європи є: підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами; створення європейської системи попередження та інформування про нові загрози; забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації; правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності; зміцнення інформаційної безпеки на державному рівні шляхом впровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних он-лайн послуг тощо; розвиток міжнародного співробітництва з питань інформаційної безпеки.

Підкреслено, що в Україні поки що немає можливості протиставити достатню кількість кваліфікованих фахівців, які б могли на належному рівні протидіяти зростаючій інформаційній активності іноземних держав щодо українського інформаційного простору. Саме тому Україна має використовувати досвід розвинутих країн, що мають напрацювання у сфері забезпечення інформаційної безпеки, зокрема досвід Європейського Союзу.

Прогнозовано, що вирішення проблем інформаційної безпеки в межах Європейського Союзу передбачає створення спільної стратегії європейської інформаційної безпеки, протидії кібервійни, інформаційному тероризму і боротьбі з інформаційною злочинністю. Акцентовано, що вступ України до Ради Європи, членство в Європейській телерадіомовній спілці полегшують її входження в європейський і разом з тим світовий масово-комунікаційний простір, надають нових можливостей для укладання міждержавних угод із сусідніми країнами

про транскордонне теле- і радіомовлення, а також змогу поглиблювати кооперацію і співпрацю між європейськими та вітчизняними масово-комунікаційними системами.

5. Правове вдосконалення інституту адміністративно-правового забезпечення інформаційної безпеки в Україні має спиратися на чітку правову основу й новітні доктринально-правові напрацювання; передбачати процесуальне закріплення відповідних матеріальних норм, доповнення їх належними гарантіями та санкціями юридичної відповідальності за порушення; забезпечувати поєднання загальнодержавних, суспільних та індивідуальних інтересів. Належне унормування відповідного кола суспільних відносин покликане сприяти усуненню поширення інформації, яка потенційно може загрожувати державі, суспільству, правам і свободам людини.

Зволікання з вирішенням проблеми належного адміністративно-правового унормування забезпечення інформаційної безпеки не сприятиме оптимальному й ефективному виконанню органами публічної адміністрації зобов'язань із захисту громадян від деструктивного інформаційного впливу.

Важливими напрямами вдосконалення законодавства України щодо адміністративно-правового забезпечення інформаційної безпеки в Україні доцільно вважати: внесення змін до законів України, які регулюють суспільні відносини щодо забезпечення інформаційної безпеки у контексті рішень Європейського Суду з прав людини; законодавчу деталізацію й розмежування порядку виконання рішень щодо блокування або видалення відповідного контенту; запровадження спеціальних процедур ефективного контролю за виконанням рішень уповноважених органів щодо блокування або видалення протиправного контенту.

6. Важливою складовою правового забезпечення інформаційної безпеки особи та суспільства, які значною мірою визначають інформаційну безпеку держави, є необхідність формування культури інформаційної безпеки. Культура інформаційної безпеки – це сукупність певних знань, умінь, навичок та високий рівень правосвідомості особистості в інформаційній сфері. До знань, умінь та

навичок у сфері інформаційної безпеки належать: здатність забезпечувати безпечну реалізацію інтересів в інформаційній сфері, усвідомлення національних інформаційних пріоритетів та інтересів, сформоване вміння визначати загрози інформаційній безпеці, оцінювати ризики, сформовані вміння та навички протистояння можливим загрозам в інформаційній сфері.

З метою формування культури інформаційної безпеки особистості та суспільства за умов цифрової трансформації необхідно розробити документи планування; правове просвітництво, охоплюючи питання відповідальності за правопорушення в інформаційній сфері; визначення викликів і загроз інформаційній безпеці; постановку короткострокових та довгострокових завдань, що охоплють активне залучення до цього процесу установ освіти та культури, інститутів громадянського суспільства; розвиток механізмів саморегулювання користувачів засобів масової комунікації, соціальних мереж та інших можливостей інформаційних технологій та систем.

Законодавче закріплення і застосування засобів забезпечення інформаційної безпеки сприятиме як формуванню, так і ефективному функціонуванню системи забезпечення інформаційної безпеки.

Використання засобів адміністративно-правового регулювання інформаційної безпеки буде сприяти оперативному прийняттю рішень, своєчасному застосуванню запобіжних заходів і засобів адекватних характеру загроз і небезпек національним інтересам України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: монографія. Київ : Едельвейс, 2014. 434 с.

2. В Україні запустили єдину платформу цифрової взаємодії для допомоги в релокації бізнесу. 12 квітня 2022. URL : https://zt.dsp.gov.ua/news/vukraini-zapustyly-iedynu-platformu-tsyfrovoi-vzaiemodii-dlia-dopomohy-vrelokatsii-biznesu/ (дата звернення: 10.09.2023).

3. Геворкян А. Ю. Формування основ культури інформаційної безпеки суспільства як фактор зміцнення національної безпеки. *Вісник Національного університету цивільного захисту України. Серія «Державне управління».* 2021. № 1 (14). С. 168–177.

4. Горовий В. М. Правові перспективи національного розвитку. URL : www.uaforeignaffairs.com/ua/ekspertna-dumka/view/article (дата звернення: 18.10.2023).

5. Губенков А. А. Информационная безопасность. Киев : 2005. 128 с.

6. Дворовий М. Санкції та блокування веб-сайтів в Україні: як непомітно відкрити скриньку Пандори. Аналітичний звіт. Київ : ГО «Лабораторія цифрової безпеки», 2021. 43 с.

7. Деякі питання цифрової трансформації : Розпорядження Кабінету Міністрів України від 17.02.2021 р. № 365-р. URL : https://zakon.rada.gov.ua/laws/show/365-2021-%D1%80#Text (дата звернення: 01.11.2023).

8. Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах від 8 листопада 2001 року. URL : www.zakon.rada.gov.ua/laws/show/994_518 (дата звернення: 17.10.2023).

9. За допомогою Телеграм-ботів кіберполіції вдалося заблокувати понад 3 тисячі ворожих Інтернет-ресурсів, – Ігор Клименко. Національна поліція України, 02 червня 2022 року. URL : https://www.kmu.gov.ua/news/

zadopomogoyu-telegram-botiv-kiberpoliciyi-vdalosya-zablokuvati-ponad-3-tisyachiv orozhih-internet-resursiv-igor-klimenko (дата звернення: 17.11.2023).

10. Інформаційна безпека. Практикум. В. М. Ахрамович., В. В. Козлов ; Націон. акад. статистики, обліку та аудиту. Київ : ДП «Інформ.-аналіт. агентство», 2018. 340 с.

11. Іонан В. Цифрограм 2.0. Цифрова грамотність українців у режимі реального часу. URL : https://ua.interfax.com.ua/news/blog/ 746434.html (дата звернення: 18.11.2023).

12. Климчук О. О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави.* 2015. № 3 (19). С. 75–83.

13. Конвенція про кіберзлочинність від 23 листопада 2001 року. URL : www.zakon5.rada.gov.ua/laws/show/994_575 (дата звернення: 11.09.2023).

14. Конституція України : від 28.06.1996 р. № 254к/96-ВР: Дата оновлення : 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 11.09.2023).

15. Кузьменко Б. В. Захист інформації. Ч. 1. Організаційно-правові засоби забезпечення інформаційної безпеки. Київ : Вид. Відділ КНУКІМ, 2009. 83 с.

16. Куц. О. В. Концепція інформаційної екології у дослідженні бібліотек. Матеріали XX ювілейної міжнародної науково-практичної конференції (Київ, 19-20.05.2021 р.). URL : https://repo.knmu.edu.ua/bitstream/ 123456789/28665/1/%D0%9A%D1%83%D1%86_%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%20%D0%B5%D0%BA%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F.pdf (дата звернення: 17.11.2023).

17. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції. Київ : КНТ, 2006. 280 с.

18. Медіаграмотність. URL : http://media-iq.tilda.ws/medialiteracy (дата звернення: 05.09.2023).

19. Молдова: Национальный ИКТ-профайл. (Информационная безопасность и защита информации). URL : www.digital.report/moldova-informatsionnaya-bezopasnost (дата звернення: 17.10.2023).

20. Невельська-Гордєєва О. П., Нечитайло В. О. Феномен «fakenews» у контексті забезпечення інформаційної безпеки держави. *Вісник Національного юридичного університету імені Ярослава Мудрого.* 2022. № 1 (52). С. 123–135.

21. Нижник Н. Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) ; Укр. Акад. держ. упр. при Президентові України, Акад. держ. податк. служби України. Київ : Преса України, 2000. 304 с.

22. Окінавська хартія глобального інформаційного суспільства. URL : https://zakon.rada.gov.ua/laws/show/998_163#Text (дата звернення: 15.09.2023).

23. Опис рамки цифрової компетентності для громадян України. Київ : Цифрова освіта Дія, 2021. 56 с.

24. Політанський В. С. Інформаційне суспільство в Україні : від зародження до сьогодення. *Науковий вісник Ужгородського національного університету. (Серія «Правоя»).* 2017. Вип. 42. С. 16–22.

25. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. № 638-IV. URL : https://zakon.rada.gov.ua/laws/card/638-15 (дата звернення: 17.10.2023).

26. Про внесення змін до Закону України «Про захист суспільної моралі» щодо захисту прав та найкращих інтересів дитини»: Закон України від 15.02.2022 р. № 2047-IX. URL.https://zakon.rada.gov.ua/laws/show/2047-20#Text (дата звернення: 17.10.2023).

27. Про деякі заходи щодо захисту держави в інформаційній сфері : Указ Президента України від 24.09.2001 р. № 891/2001. URL : www.zakon.rada. gov.ua/laws/show/891/2001 (дата звернення: 10.10.2023).

28. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.2009 р. № 514/2009. URL : www.zakon.rada.gov.ua/ laws/show/514/2009 (дата звернення: 15.09.2023).

29. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI. *Відомості Верховної Ради України.* 2011. № 32. Ст. 314 (дата звернення: 15.09.2023).

30. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. URL : https://zakon.rada.gov.ua/laws/card/2155-19 (дата звернення: 17.11.2023).

31. Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX. URL. https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 17.09.2023).

32. Про запобігання корупції: Закон України від 14.10.2014 р. № 1700-VII. URL : https://zakon.rada.gov.ua/laws/card/1700-18 (дата звернення: 17.10.2023).

33. Про захист дітей від сексуальної експлуатації та сексуального насильства : Конвенція Ради Європи від 25.10.2007 р. URL : www.zakon3.rada.gov.ua/laws/show/ 994_927 (дата звернення: 18.11.2023).

34. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 31.05.2005 р. № 2594. Відомості Верховної Ради України. 2005. № 26. Ст. 347.

35. Про захист суспільної моралі: Закон України від 20.11.2003 р. № 1296-IV. URL : https://zakon.rada.gov.ua/laws/card/1296-15 (дата звернення: 10.09.2023).

36. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : директива 95/46/ЄС Європейського Парламенту і Ради від 24.10.1995 р. URL : www.zakon2.rada.gov.ua/ laws/show/994_242 (дата звернення: 25.10.2023).

37. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Указ Президента України від 28.04.2014 р. URL : www.president.gov.ua/dokument/17588.html (дата звернення: 17.09.2023).

38. Про інформацію : Закон України від 2.10.1992 р. № 2657 : зі змінами згідно Закону України від 13.01.2011 р. № 2938-VI «Про внесення змін до

Закону України «Про інформацію». Відомості Верховної Ради України. 1992. № 48. Ст. 650.

39. Про Концепцію Національної програми інформатизації : Закон України : із змінами, внесеними згідно із Законом № 3421-IV (3421-15) від 09.02.2006 р. URL : www.zakon.rada.gov.ua/laws/show/75/98-вр (дата звернення: 17.09.2023).

40. Про національну безпеку України: Закон України від 21.06.2018 р. № 2496-VIII. URL : https://zakon.rada.gov.ua/laws/card/2469-19 (дата звернення: 08.10.2023).

41. Про оборону України : Закон України від 11.05.2007 р. № 1014-V. URL : www.zakon.rada.gov.ua/laws/show/1932-12 (дата звернення: 17.09.2023).

42. Про основи національної безпеки: Закон України від 19.06.2003 р. № 964-IV. URL : https://zakon.rada.gov.ua/laws/card/964-15 (дата звернення: 08.10.2023)

43. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 9.01.2007 р. № 537-V. *Урядовий кур'єр.* 2007. 14 лют. С. 2–3.

44. Про права дитини, що стосується торгівлі дітьми, дитячої проституції й порнографії : факультативний протокол до Конвенції ООН від 01.01.2000 р. URL : www.zakon3.rada.gov.ua/laws/show/995_b09 (дата звернення: 12.09.2023).

45. Про публічні електронні реєстри: Закон України від 18.11.2021 р. № 1907-IX. URL : https://zakon.rada.gov.ua/laws/show/1907-20/conv#n472 (дата звернення: 07.09.2023).

46. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 р. № 392/2020. URL : https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 07.09.2023).

47. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента

України від 28.12.2021 р. № 685/2021. URL : https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 25.09.2023)

48. Про санкції: Закон України від 14.08.2014 р. № 1644-VII. URL : https://zakon.rada.gov.ua/laws/show/1644-18#Text (дата звернення: 23.09.2023).

49. Про стимулювання розвитку цифрової економіки в Україні: Закон України від 15.07.2021 р. № 1667-IX. URL : https://zakon.rada.gov.ua/laws/show/1667-20#Text (дата звернення: 17.11.2023).

50. Про телекомунікації : Закон України від 01.11.2003 р. № 1280-IV. Відомості Верховної Ради України. 2004. № 12. Ст. 155.

51. Про хмарні послуги: Закон України від 17.02.2022 р. № 2075-IX. URL : https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення: 17.10.2023).

52. Проєкт Закону України «Про засади інформаційної безпеки України». URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123 (дата звернення: 17.10.2023).

53. Проєкт Концепції виховання дітей та молоді в цифровому просторі. Київ : Національна академія педагогічних наук України, 2021. 52 с.

54. Проєкт Концепції та плану заходів з розвитку цифрових прав дітей. URL : https://thedigital.gov.ua/storage/uploads/files/%D0%9F%D1%80%D0%BE%D1%94%D0%BA%D1%82%20%D0%B0%D0%BA%D1%82%D0%B0.pdf (дата звернення: 17.10.2023).

55. Руснак А. К. Молдова и информационная безопасность. SECURITATEA INFORMATIONALĂ 2011 : Conferinţa Internaţională, ediţia a VIII-a, 4 mai 2011. P. 62–63.

56. Смарт-інфраструктура у сталому розвитку міст: світовий досвід та перспективи України. Центр Разумкова. Київ : Видавництво «Заповіт», 2021. 400 с.

57. Соскін О. Цифровізація як нова реальність України. 2022. URL : https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/ (дата звернення: 17.10.2023).

58. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики. *Державне будівництво.* 2016. URL : www.kbuapa. kharkov.ua/e-book/db/2016-2/doc/1/02.pdf (дата звернення: 23.10.2023).

59. Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн східної Європи. *Інформація і право.* 2017. URL : www.ippi.org.ua/tkachuk-tyu-zabezpechennya-informatsiinoi-bezpeki-dosvid-okremikh-krain-skhidnoi- %D1 %94vropi-st-62-72 (дата звернення: 25.10.2023).

60. Ухвалено типову програму підвищення кваліфікації педагогічних працівників із розвитку цифрової компетентності. 13 грудня 2021 року. URL : https://mon.gov.ua/ua/news/uhvaleno-tipovu-programu-pidvishennya-kvalifikaciyipedagogichnih-pracivnikiv-iz-rozvitku-cifrovoyi-kompetentnosti (дата звернення: 11.10.2023).

61. Цифрова гігієна: яких правил варто дотримуватися в Інтернеті? 24 березня 2020. URL : https://thedigital.gov.ua/news/tsifrova-gigiena-yakikh-pravilvarto-dotrimuvatisya-v-interneti (дата звернення: 09.11.2023).

62. Цифрова компетентність. Які навички слід розвивати під час пандемії? 10.06.2021. URL : https://eufordigital.eu/uk/digital-competence-whatskills-do-you-need-to-develop-during-the-pandemic/ (дата звернення: 09.11.2023).

63. Шатун В. Т. Інформаційна безпека – невід’ємна складова національної безпеки України. *Наукові праці. Державне управління.* 2016. Вип. 255. Т. 267. С. 174–180.

64. NATO Bucharest Summit Declaration, 3 April 2008. URL : www.nato.int/docu/pr/2008/p08-049e.html/ (Last accessed: 11.11.2023).