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 *Риженко Дениса Сергійовича*

академічної групи *281м-21з-5 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	Сорокіна Н.Г.			
розділів:				

Рецензент:				

Нормоконтролер:	Вишневська О.В.			

Дніпро
2022

РЕФЕРАТ

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

66 с., 79 джерел.

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 Україні.

У першому розділі досліджуються теоретико-правові засади інформаційної безпеки в Україні.

Другий розділ присвячено аналізу сучасного стану забезпечення інформаційної безпеки України. Розглянуто зарубіжний досвід забезпечення інформаційної безпеки

У третьому розділі надані шляхи удосконалення адміністративно-правового забезпечення інформаційної безпеки в Україні.

Сфера практичного застосування результатів роботи – 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»

66 pages, 79 sources.

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

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

The subject of the study is the administrative and legal provision of information security in Ukraine.

The purpose of the study is to determine ways to improve the administrative and legal provision of information security in Ukraine.

The first chapter examines the theoretical and legal foundations of information security in Ukraine.

The second section is devoted to the analysis of the current state of information security in Ukraine. The foreign experience of ensuring information security is considered

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

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

Революція гідності, засуджуючи злочинність попередньої влади, відкрила перед Україною можливості для побудови нової системи відносин між громадянином, суспільством і державою на основі цінностей свободи і демократії, і в цьому безперервному демократичному процесі важлива роль надається забезпеченню інформаційної безпеки засобами адміністративно-правового впливу.

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: Г. В. Атаманчука, О. М. Бандурку, О. Б. Тацишина, Р. С. Свистовича, та інших. Серед зарубіжних вчених значний

внесок у розгляд цієї проблеми внесли С. Алексєєв, І. Бачило, В. Лопатін, Л. Серов, Т. Рона та інші.

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 інформаційної сфери та його роль в забезпеченні інформаційної безпеки;

– проаналізувати сучасний стан інформаційної безпеки в Україні;

– вивчити зарубіжний досвід забезпечення інформаційної безпеки;

– розкрити основні шляхи удосконалення інформаційної безпеки;

– окреслити засоби адміністративно-правового регулювання та державного управління забезпеченням 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.

Практичне значення одержаних результатів полягає в тому, що 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.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

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 [1].

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 [2 – 12] 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 [11], 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 [5] та Законі України «Про основи національної безпеки» [7] 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 роки» [8] та в Законі України «Про телекомунікації» [9].

У першому Законі [8] 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 [9] 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» [4], який є базовим щодо нормативного закріплення інформаційної сфери держави, визначення інформаційної безпеки немає, а в Законі України «Про основи національної безпеки України» [7], 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» [3], 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» [5] проголошує, що «інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки». Воєнна доктрина України [6] 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 [42]. 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 [29. 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 [71].

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 [41].

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 [48]. 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

Сьогодні Україні складно претендувати на інформаційне домінування у світовому інформаційному просторі. Для нашої країни головне не відстати, зберігаючи національну, інтелектуальну, культурну та мовну самобутність. Усе це вимагає замислитися над перспективами використання новітніх інформаційних технологій та розвитку інформаційного суспільства в Україні. Концептуальні засади державної політики України в інформаційній сфері мають формуватися, зважаючи на національні інтереси країни, збалансовуючи інтереси особистості, суспільства і держави.

Тому існуюча політика держави в інформаційній сфері спрямована як на розвиток безпосередньо інформаційної сфери, так і на підвищення ефективності розвитку державності, безпеки, оборони, пріоритетних галузей економіки, фінансової та грошової системи, соціальної сфери, галузей екології та використання природних ресурсів, науки, освіти і культури, міжнародного співробітництва за допомогою інформаційної сфери. Це підтверджується і Концепцією Національної програми інформатизації, в якій інформаційна сфера, інформатизація розглядається як важливий засіб для розвитку України [22].

Виробництво інформаційного продукту, а не продукту матеріального визначає інформаційне суспільство. Інформація та знання стають головними стратегічними ресурсами такого суспільства, в якому інформація проникає у всі сфери суспільства та держави.

Українська дослідниця Ірина Березовська слушно зауважує, що «…в умовах становлення інформаційного суспільства в Україні і світі пріоритетне місце серед різних напрямів державного управління посідає управління інформаційною сферою. Фундаментальною основою його здійснення виступають норми права, які покликані врегулювати та впорядкувати відповідні управлінські процеси, забезпечити їх цілеспрямованість, системність, стабільність і збалансованість. Розглядаючи інформаційну безпеку як одну зі складових національної безпеки, вирішуючи завдання розвитку інформаційної сфери в Україні та проблеми створення умов для побудови

інформаційного суверенітету країни, неможливо обійтись без надійного правового підґрунтя» [39, с. 32].

Сьогодні в національному законодавстві не легалізовано поняття «інформаційна сфера». Вважаємо, що в теперішній час як на побутовому, так і на науковому рівні інформаційна сфера розглядається як сфера, яка формується та розвивається під час інформаційної діяльності. У зв'язку з цим дослідження державного управління в інформаційній сфері виступає актуальним завданням сучасної адміністративно-правової науки.

З огляду державного управління в інформаційній сфері варто загалом, розуміти підзаконну виконавчо-розпорядчу діяльність уповноважених державних органів, їх посадових осіб з реалізації функцій і завдань держави у сфері суспільних інформаційних та інформаційно-інфраструктурних відносин відповідно до інтересів суспільства [33]. Метою державного управління в інформаційній сфері на сучасному історичному етапі є забезпечення задоволення потреб особи і суспільства загалом в інформації як стратегічному ресурсі його розвитку.

Нині в нашій державі управління інформаційною сферою здійснює 5 основних органів державної влади: 2 регуляторних органи – Національна рада України з питань телебачення і радіомовлення та Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, а також 3 органи виконавчої влади – Державний комітет з телебачення та радіомовлення України, Держінформнауки України та Державна служба спеціального зв'язку та захисту інформації України.

Нормативно-правовою основою правового регулювання державного управління інформаційною сферою є саме галузь адміністративного права шляхом визначення завдань і основних напрямів діяльності держави, системи та адміністративно-правового статусу суб'єктів державного управління та керованих ними суб'єктів інформаційних відносин, а також регулювання взаємодії між ними в зазначеній сфері.

Так, у Законі України «Про інформацію» закріплено правові основи одержання, використання, поширення та зберігання інформації, визначено коло

учасників інформаційних відносин, врегульовано режими доступу до інформації, її джерела, види, напрями і способи державної інформаційної політики тощо.

Для якісного управління процесами в інформаційному просторі необхідним є функціонування комплексної керуючої системи, яка складається з наступних підсистем: суб'єктів, (держава, територіальні та інші громади, громадські організації); об'єктів (процеси у внутрішньому, міжнародному і глобальному сегментах інформаційного простору та їх похідні); механізму здійснення керуючого впливу (державний апарат, інститути держави і суспільства, громадський сектор, ЗМІ).

Інформаційна держава повинна орієнтуватися у першу чергу на інтереси інформаційного суспільства. Для цього держава повинна розробити відповідну інформаційну політику, ефективна реалізація якої, тобто ефективне державне управління інформаційною сферою повинно враховувати можливості міжнародного співробітництва у сфері інформаційних технологій, продуктів і послуг, реальні можливості вітчизняної інформаційної індустрії.

Природним еволюційним етапом цивілізаційного розвитку є входження до інформаційної ери, де основними стратегічними ресурсами є знання та інформація. Саме ці компоненти стають основою нового – інформаційного суспільства. Забезпечення інформаційної безпеки, реалізація державної інформаційної політики є неможливим у разі несформованості інформаційного суспільства.

У такому відношенні варто констатувати, що побудова інформаційного суспільства є стратегічною метою провідних держав світу – США, Японії, Канади, а також країн-членів Європейського Союзу. Актуальність та важливість розвитку інформаційно-технічної сфери є запорукою конкурентоспроможності країни.

У цьому сенсі, інформаційне суспільство можна розглядати як суспільство, в якому основним предметом праці переважної більшості людей стають інформація й знання, тобто інформаційні ресурси, знаряддям праці – комп'ютерна техніка, засобами – інформаційні технології. У розвинутих

країнах вже сьогодні існуючі суспільні відносини багато в чому визначаються саме цією обставиною. Відповідно, і економіка повинна орієнтуватися на виробництво продуктів інформаційної, інтелектуальної діяльності, що пов'язані із виробленням нової інформації і нових знань, з перетворенням їх у стан, зручний для використання іншими людьми, та продажем цих продуктів як товару [17].

Термін «інформаційне суспільство» було запропоноване японським дослідником К. Каямою, на основі якого в Японії була прийнята програма «План інформаційного суспільства: національна мета 2000 року». Кр. Мей у праці «Інформаційне суспільство: скептичний погляд» виділяє три періоди цієї проблеми: дослідження, що мали місце з початку 1960-х рр. і до середини 1970-х р. і стосувалися винятково США; дослідження кінця 1970-х рр. і початку 1990-х рр., коли інформаційно-комунікативні технології активно впроваджувалися у розвинутих країнах світу; дослідження, коли виникнення і поширення Інтернету сприяло масовій зацікавленості ідеями глобального інформаційного суспільства.

У 1993 р. сутність інформаційного суспільства була розкрита Комісією ЄС: «Інформаційне суспільство – це суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій та технологій зв'язку» [19, с. 187].

Українські вчені приділяють значну увагу проблемам становлення інформаційного суспільства як такого, особливостей процесів, що в ньому відбуваються, формування глобального інформаційного простору, суперечностей у світі, зумовлених інформатизацією та глобалізацією. Зокрема, у працях вітчизняних дослідників аналізуються відповідні концепції відомих зарубіжних дослідників: Д. Белла, А. Турена, О. Тоффлера, Т. Стоуньєра, Дж. Нейсбіта, Л. Квортруна, Ф. Феррароттi, Й. Масуди, В. Феркіса. Особлива увага привертається до наукового аналізу техніко-технологічних і соціальних змін, що відбувалися в розвинених країнах у результаті науково-технічної революції, як на основі такого аналізу, зрештою, виникло і дістало визнання поняття «інформаційне суспільство».

Виходячи з концепцій названих авторів, інформаційно-технологічні процеси характеризуються як передумова виникнення і чинник інформаційного суспільства, з'ясовуються перспективи соціально-економічних змін такого суспільства і можливих змін самої людини в ньому. Можна відзначити, що нинішнє інформаційне суспільство торує шлях до майбутніх перетворень, тому що його економічна необхідність набуває інших форм, раціоналізація соціально-економічних відносин здійснюється на інших підвалинах, внаслідок чого виникають можливості для нового типу поведінки і виробничої діяльності людини. У зв'язку з цим відповідні соціально-економічні перетворення неможливі без зміни існуючої системи цінностей, пріоритетів, світоглядних принципів. Як наслідок, актуалізується проблематика, пов'язана зі створенням етики відповідальності, яка могла б нейтралізувати негативні наслідки сучасного науково-технічного розвитку. Відповідно, як зазначає український філософ В. Лях, має змінитися орієнтація людини на безконтрольне право перетворювати природу, навколишнє середовище і соціальний життєпорядок, і саме тут виникає проблема, якими мають бути стосунки між природою і людиною, чи здатна людина піднестися над своїми вузькоегоїстичними цілями і вийти на рівень світоглядних парадигм глобального масштабу [61, с. 78].

Безперечно, інформаційне суспільство – це суспільство, в якому на першому місці іде розвиток нових інформаційних технологій, найважливішим продуктом для більшості людей стає інформація, безперечною умовою є доступ до неї всіх бажаючих, вирішальним у цьому суспільстві стає здатність мислити, аналізувати і використовувати інформацію. Інформаційне суспільство – надзвичайно динамічне. Варто зазначити, що життя у цьому суспільстві для кожної окремої особистості постає різним, оскільки воно залежить від того, наскільки людина, соціум зможуть пристосуватися до нових умов [20, с. 117].

При цьому, основними характеристиками інформаційного суспільства є: зростання ролі інформації і знань у житті суспільства; зростання кількості людей, зайнятих інформаційними технологіями, комунікаціями і виробництвом інформаційних продуктів та послуг, зростання їх частки у валовому внутрішньому продукті; індустрія інформаційних послуг, сучасні

інтелектуальні інформаційні технології та технології зв’язку, значний потенціал науки, створення глобального інформаційного простору, який забезпечує ефективну інформаційну взаємодію людей, їх доступ до світових інформаційних ресурсів і задоволення їхніх потреб щодо інформаційних продуктів та послуг.

Основна мета формування інформаційного суспільства – це загальне прагнення та рішучість його учасників побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток суспільство. Найважливішою ознакою інформаційного суспільства визначено можливість кожного створити інформацію і знання, мати до них доступ, користуватися та обмінюватися ними. Основна мета інформаційного суспільства – дати окремим особам, громадянам і народам можливість повною мірою реалізувати свій потенціал, сприяючи постійному розвитку та підвищенню рівня свого життя на основі цілей і принципів Статуту Організації Об’єднаних Націй, у повному обсязі дотримуючись і підтримуючи Загальну декларацію прав людини [63, с. 189].

Експерти Організації Об’єднаних Націй з промислового розвитку дійшли висновку: якщо раніше провідна роль в зростанні економіки держави належала природним ресурсам, які надавали тій чи іншій країні переваги в системі світових господарських зв’язків, то зараз на передній план виступає рівень розвитку людських ресурсів – кваліфікація, майстерність, вміння як основа інтелектуального потенціалу нації [65, с. 9].

Обсяги українського ринку інформаційних продуктів та послуг не можна порівняти із ринками розвинених західних країн. Необхідна його структурна реорганізація та модернізація, що потребує значних інвестицій.

Найбільшого успіху на шляху до інформаційного суспільства досягають країни, у яких держава формує і активно проводить у життя відповідну цілеспрямовану політику. Роль держави постає у створенні сприятливих умов для розвитку цього процесу, до яких можна віднести:

– максимальне залучення ресурсів (кадрових, фінансових, матеріальних) до інформаційного виробництва;

- нормативно-правове та нормативно-технічне регулювання;
- розвиток міжнародного інформаційного обміну та співробітництва.

Питання інтеграції України у глобальні інформаційні процеси прямо залежить від темпів інформатизації в Україні. Ключовим нормативно-правовим актом в цій сфері є Національна програма інформатизації України [74]. Головною метою цієї програми є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави.

Якщо розглядати інформаційну безпеку як певні умови, параметри і характеристики інформаційних процесів, що відбуваються в інформаційній сфері держави, то саме держава має можливість за допомогою нормативно-правового регулювання визначати єдині, загальнообов'язкові стандарти інформаційних процесів, що відповідають уявленням про безпеку тих сил, які здійснюють політичну владу в цій державі [43, с. 248].

Отже, для створення цілісної моделі інформаційного суспільства та індустрії інтелектуальних інформаційних технологій Україні необхідно розбудовувати телекомунікаційну інфраструктуру шляхом залучення зовнішніх та внутрішніх інвестицій; мобілізувати науку, освіту, промисловість, гуманітарну, медійну сфери і бізнес на пріоритетних напрямах розвитку інформаційного суспільства, побудованого на знаннях.

Крім того, процес становлення інформаційного суспільства в Україні є довготривалим, багатоетапним, складним, але він є необхідним з огляду на світові тенденції та обрану зовнішньополітичну стратегію.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНОГО СТАНУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Сучасний стан інформаційної безпеки в Україні

В умовах мінливості і суперечливого глобального простору, проникливості кордонів і формування нової політичної географії виникли нові суперечності різного типу між окремими державами і регіонами. До низки гострих конфліктів призвели політичні, економічні, конфесійні, етнічні й інші протиріччя, намагання переглянути вже існуючі кордони, перерозподілити сфери впливу. У суперечностях між державами для досягнення успіху широко використовуються засоби і можливості інформаційної війни, тобто використання й управління інформацією з метою набуття конкурентоздатної переваги над супротивником. В умовах повномасштабної російсько-української війни й окупації Криму, Донецької, Луганської, Запорізької та частково Херсонської областей засоби такої війни широко використовувалися та використовуються росією в Україні. Тому для України важливим завданням постало забезпечення інформаційної безпеки.

Інформаційна безпека є одним із видів національної безпеки. Відповідно до законодавства України, інформаційна безпека має таке визначення: «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 поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [32].

Інформаційна безпека означає:

- законодавче формування державної інформаційної політики;
- створення відповідно до законів України можливостей досягнення

інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об’єднаннями громадян, іншими суб’єктами права в Україні;

− гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України;

− всебічний розвиток інформаційної структури;

− підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей духовно-культурного життя народу України;

− створення і впровадження безпечних інформаційних технологій;

− захист права власності всіх учасників інформаційної діяльності в національному просторі України;

− збереження права власності держави на стратегічні об’єкти інформаційної інфраструктури України;

− охорону державної таємниці, а також інформації з обмеженим доступом, що є об’єктом права власності або об’єктом лише володіння, користування чи розпорядження державою;

− створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом;

− захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції;

− встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядок використання цих ресурсів на основі договорів із іноземними державами;

− законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України [40].

Державна політика інформаційної безпеки визначається пріоритетністю національних інтересів, системою небезпек і загроз та здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм в інформаційній сфері відповідно до чинного законодавства.

У Законі України «Про основи національної безпеки України» визначено основні напрямки державної політики з питань національної безпеки в інформаційній сфері. До них належать:

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- активне залучення засобів масової інформації до боротьби з корупцією, зловживання службовим становищем, іншими явищами, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [7].

Для формування збалансованої державної політики та ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів в інформаційній сфері створення розвиненого і захищеного інформаційного середовища слугує організацією функціонування системи інформаційної безпеки, складовими компонентами якої є національні інтереси в інформаційній сфері, загрози та небезпеки цим інтересам, сама інформаційна безпека як інструмент зі створення сприятливих умов для їх реалізації, які в сукупності становлять об’єкт управління органами державного управління, систему забезпечення інформаційної безпеки, тобто суб’єкт управління, більше

того, основні напрямки політики національної безпеки в інформаційній сфері, а також внутрішнє та зовнішнє середовище. Інформаційна безпека забезпечується комплексом заходів системи забезпечення національної безпеки України, що включає сукупність державних органів, громадських організацій, посадових осіб та окремих громадян [42].

Правову основу забезпечення інформаційної безпеки України становлять Конституція України, закони України «Про основи національної безпеки України», «Про інформаційну безпеку України», «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [8], «Про доступ до публічної інформації» [2], інші закони та інформативно-правові акти, а також ратифіковані або парафовані Україною Договір про безпеку і співробітництво в Європі, Договір «Відкрите небо», Угода про партнерство і співробітництво між європейським співтовариством і Україною, Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства, які зобов'язують країни-учасниці здійснювати багатосторонній обмін інформацією, потребують створення загальнодержавних механізмів зберігання та споживання отриманої інформації в національних інтересах.

Проте необхідно зауважити, що досі в Україні не прийнято закону, який би визначав концепцію державної інформаційної політики України. Відповідно, в країні не існує єдиного плану, єдиної державної позиції чи стратегії розвитку інформаційної галузі, а отже, і забезпечення інформаційної безпеки. Хоча протягом 2002-2010 рр. було три спроби ухвалити концепцію державної інформаційної політики – 2002, 2009 та 2010 р. 11 січня 2011 р. черговий проект концепції прийняли у першому читанні за основу закону і направили на доопрацювання Комітету Верховної Ради з питань свободи слова та інформації [35].

Лише після революції Гідності питанням інформаційної безпеки приділяється більше уваги. Указом Президента України було оприлюднено рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики

у сфері інформаційної безпеки України». Було передбачено у місячний термін розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши механізм протидії негативному інформаційно-психологічному впливу, зокрема шляхом заборони ретрансляції телевізійних каналів, а також запровадження для іноземних засобів масової інформації, системи інформування та захисту журналістів, які працюють у зоні збройних конфліктів, вчинення терористичних актів, при ліквідації небезпечних злочинних груп.

У місячний термін також було передбачено за участю Національного інституту та інших органів розробити проект Стратегії розвитку інформаційного простору України і проект стратегії кібернетичної безпеки України, а також розробити комплексні заходи організаційного, інформаційного і роз'яснювального типу щодо всебічного висвітлення заходів із реалізації державної політики у сфері забезпечення інформаційної безпеки, а також посилення контролю за держанням законодавства з питань інформаційно-психологічної та кібернетичної безпеки.

Указом було передбачено у тримісячний термін робити проект нової редакції Доктрини інформаційної безпеки України, проект Закону України про кібернетичну безпеку України, законопроекти про внесення змін до деяких законів України, зокрема до Законів України «Про основи національної безпеки України», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про службу безпеки України», «Про службу спеціального зв'язку та захисту інформації України» та внести їх на розгляд Верховної Ради України [12].

В листопаді 2014 р. було створено Міністерство інформаційної політики. При Міністерстві в процесі спілкування Міністра з представниками громадськості була створена Експертна Рада, метою якої стала розробка Стратегії інформаційної політики України, Концепції інформаційної

безпеки України та Державної програми розвитку інформаційного простору України [26].

До пріоритетних напрямків забезпечення інформаційної безпеки України можна зарахувати:

- створення законодавчої та нормативної бази;
- здійснення моніторингу інформаційної безпеки України;
- стандартизація, сертифікація та ліцензування діяльності у сфері забезпечення інформаційної безпеки України;
- удосконалення та розвиток державної інформаційної інфраструктури з урахуванням вимог інформаційної безпеки України;
- удосконалення системи освіти, навчання та виховання з урахуванням вимог інформаційної безпеки України та Закону України «Про державну мову»;
- розробка міжрегіональних, державних та міждержавних програм розвитку системи інформаційної безпеки України [45].

На сучасному етапі інтеграційних процесів України до Європейського Союзу особливого значення набуває проблема інформаційного забезпечення політики європейської інтеграції. Завданням інформаційної політики постала необхідність забезпечення вирішення двох основних завдань:

1. Забезпечення загальнонаціональної підтримки курсу інтеграції України в Європейський Союз широкими колами громадськості, створення проєвропейської більшості в суспільстві.

2. Донесення до урядів і громадськості країн-членів Європейського Союзу об’єктивної інформації про Україну, її досягнень на шляху реформ, створення позитивного іміджу України.

На шляху до вирішення цих завдань постають такі проблеми, які можна вирішити шляхом:

1. Проведення широкомасштабної інформаційної роз’яснювальної компанії серед населення України.

2. Здійснення іноземного просування України в країнах Європейського Союзу Розроблення структурної програми просування України на

міжнародному рівні в процесі просування України на міжнародному рівні в процесі інтеграції до Європейського Союзу [49].

Проведення планомірного інформування громадськості з питань європейської інтеграції відповідає пріоритетним напрямам Програми інтеграції України до Європейського Союзу. Для забезпечення підтримки політики європейської інтеграції України серед української громадськості необхідно запровадити системи ефективних заходів інформування та освіти суспільства, налагодити механізм співпраці державних органів із засобами масової інформації з метою ефективного використання інформації, яка надходить від центральних органів виконавчої влади, забезпечити прозорість у прийнятті відповідних рішень органів виконавчої влади, налагодити постійний зворотний зв'язок.

Заходи мають охоплювати усі сфери діяльності виконавчої влади. Серед основних заходів, які здійснюються, можна виділити такі освітні заходи:

− розроблення Національної програми перепідготовки й навчання державних службовців центральних, регіональних та місцевих органів влади, спрямованої на поглиблення знань про європейську інтеграцію, забезпечення розуміння цілей інтеграції до Європейського Союзу, його основних інституцій, процесу ухвалення рішень, вміння вести переговори, використовувати європейські інформаційні ресурси, покращення володіння хоча б однією з основних європейських мов;

− інформування молоді з питань інтеграції України до ЄС;

− поширення в Україні освітніх, наукових та культурних європейських програм «Сократ», «Леонардо», «Молодь», «Проект Жана Моне» та інших;

− започаткування у вищих навчальних закладах освітніх програм із інтеграції України до ЄС.

Не менше значення мають видавничі заходи:

− готування та видання енциклопедії, словників, серії довідників про ЄС (його історію, законодавство, про держави-члени ЄС), листівок;

− розроблення методичних та довідкових матеріалів на допомогу

викладачам, працівникам органів виконавчої влади і органів місцевого самоврядування, присвячених питанням європейської інтеграції;

− виготовлення буклетів, інших пропагандистських матеріалів із висвітленням європейської інтеграції.

Належне місце в інформаційній політиці з питань європейської інтеграції займали комунікативні заходи:

− проведення зустрічей членів Уряду з політиками, представниками центральних, регіональних ЗМІ, громадськістю;

− організація семінарів, брифінгів для представників засобів масової інформації;

− забезпечення виступів керівників у регіонах з окремих питань інтеграції України до Європейського Союзу;

− проведення інтерв'ю, прес-конференцій з питань євроінтеграції;

− організація культурних масових заходів: проведення виставок, конференцій, акцій, форумів, показ високоякісної європейської продукції;

− створення інформаційних центрів із надання населенню інформаційних та консультативних послуг із питань євроінтеграції;

Важливі завдання реалізації інформаційної політики з питань євроінтеграції стоять перед ЗМІ, зокрема:

− підготовлення низки телевізійних проектів, програм, передач, репортажів із країн-членів ЄС та держав-кандидатів на вступ до ЄС про досвід європейської інтеграції, про нові можливості, перспективи, наслідки;

− залучення українських мас-медіа як друкованих, так і електронних, телебачення, радіо, інформаційних агентств до висвітлення різних аспектів української політики та внутрішнього життя через призму інтеграції до ЄС;

− розповсюдження через ЗМІ презентаційних та довідкових матеріалів із питань європейської інтеграції України;

− забезпечення участі керівників міністерств, інших центральних органів виконавчої влади в теле- і радіопередачах із метою роз'яснення політики України з питань європейської інтеграції;

– створення веб-сторінок органів виконавчої влади, присвячених питанням європейської інтеграції, та забезпечення розміщення в Інтернеті повідомлень у рамках європейських процесів;

– проведення Інтернет-конференцій із залученням зацікавлених міністерств, інших центральних органів виконавчої влади.

Виконання цих заходів дасть змогу поліпшити знання суспільства про сутність європейської інтеграції, специфіку функціонування ЄС, подолати психологічний пострадянський бар'єр суспільної думки стосовно нової системи європейських координат й інтеграційних перспектив, забезпечити всебічну підтримку Уряду українським суспільством. За цього важливого значення набувають знання про ЄС та виховання молодих людей у дусі спільних європейських цінностей та ідеалів. Звичайно, виконання цих усіх заходів потребує значних фінансових затрат [49].

Високою буде ефективність від організації просування України в країнах Європейського Союзу та від розроблення структурної програми просування України на міжнародному рівні в процесі інтеграції до ЄС. Український імідж за кордоном має суттєвий вплив на реалізацію цілей української зовнішньої політики у напрямку інтеграції до ЄС. Дуже важливим є формування позитивного національного іміджу, зокрема в країнах-членах Європейського Союзу. Україна має переконати європейську громадськість, насамперед чиновників Європейської Комісії, що вона гідна посісти чільне місце в стабільній демократичній Європі. Україна зацікавлена в лібералізації зовнішньоекономічних зв'язків з іншими країнами-членами ЄС. Для того, щоб співпрацювати з ними та формувати зону вільної торгівлі, що сприятиме інтенсифікації господарських взаємовідносин, активному обміну капіталом, товарами, послугами, робочою силою, необхідно вирішити багато проблем, одна з яких – забезпечити європейську громадськість повною та вичерпною інформацією про інтеграційну політику України. Від кращого розуміння європейським співтовариством української політики, соціальної сфери, культури тощо залежить місце та роль України. Від кращого розуміння

європейським співтовариством української політики, соціальної сфери, культури тощо залежить місце та роль України на світовій арені. Успіх переговорів з Європейським Союзом, рівень прийняття європейською громадськістю намірів України щодо входження в ЄС залежить також від результативної діяльності у напрямку просування України серед країн-членів. Для цього теж повинні слугувати відповідні заходи та повинні бути визначені індикатори їх результативності [49].

В умовах, коли Україна відстоює свій євроінтеграційний курс, проти України ведеться війна з боку російської федерації. Складовою частиною цієї війни є контрпропаганда, яка ведеться проти України – справжня інформаційна війна. Ворог намагається створити розкол між силовими структурами України та волонтерами, між силовими структурами і населення, скеровуються зусилля на зрив мобілізації тощо [27].

У зв’язку з посиленням негативного зовнішнього впливу на інформаційний простір України, що загрожує розмиванню суспільних цінностей і національної ідентичності, недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту. Наближається до критичного стан безпеки інформаційно-комп’ютерних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій.

Забезпечення сприятливих зовнішніх умов для розвитку та безпеки держави передбачає забезпечення інформаційної безпеки при інтеграції до структур глобального інформаційного суспільства.

Ефективна реалізація стратегічних пріоритетів, основних принципів і завдань державної політики інформаційної безпеки потребує вдосконалення правових та організаційних механізмів управління інформаційною безпекою, його відповідного інтелектуально-кадрового і ресурсного забезпечення, зокрема вдосконалення законодавства з питань національної безпеки, насамперед шляхом:

− розвитку правових засад управління національною безпекою через

розробку відповідних законів, концепцій, доктрин, стратегій і програм, зокрема антикорупційного законодавства, Національної програми протидії тероризму та екстремізму, Концепції розвитку Воєнної організації держави, Національної стратегії формування інформаційного суспільства, Доктрини інноваційного та науково-технологічного розвитку тощо;

− розробка та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами, зокрема з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність;

− приведення законодавства з питань охорони державної таємниці до європейських стандартів;

− розробка та впровадження загальнодержавної системи визначення та моніторингу порогових значень показників (індикаторів), що характеризують рівень захищеності національних інтересів у різних сферах життєдіяльності та виникнення реальних загроз національній безпеці.

Отже, у сучасних умовах важливою складовою національної безпеки є інформаційна безпека України, що є станом захищеності національних інтересів у інформаційній сфері.

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 [64, 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 [77, 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 [78], 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.) [76] 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 [76].

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 [67]. Крім того, з 2018 року для Румунії та Болгарії, як і

інших країн-членів ЄС, набудуть чинності нові правила захисту персональних даних (GDPR), які схвалено 14 квітня 2016 року. 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 [25]. 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 [60].

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 [36, 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 [76]. Законопроект «Про кібербезпеку», який у грудні 2014 року 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 [76].

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 року 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 року.

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 року 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 [76].

Незважаючи на критику політики забезпечення інформаційної безпеки у наукових колах [69, с. 63], у Молдові діє відносно надійна система протидії кіберзлочинності. Так, ще у 2009 році Парламентом була ратифікована Конвенція Ради Європи про кіберзлочинність [37]. Крім того, влада Молдови підписала Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах у березні 2012 року [31]. Парламентом також був прийнятий Закон «Про попередження та боротьбу зі злочинністю у сфері комп'ютерної інформації» у січні 2010 року [76]. 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 [68], Конвенції Ради Європи про кіберзлочинність [37] й Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства [66], 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 року, розробленого з метою підвищення рівня безпеки електронних підписів та приведення у відповідність із міжнародними стандартами й рекомендаціями щодо інфраструктури відкритих ключів [28]. 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 року щодо захисту персональних даних [76], Директиву 2008/114/ЄС «Про ідентифікацію й призначення європейських критичних інфраструктур і заходах з їх захисту» від 8 грудня 2008 року [50] 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 року № 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 року 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 [47].

Проект Концепції інформаційної безпеки, схвалений Парламентом Молдови в першому читанні 23 червня 2017 року, 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 року 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 [76].

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 року 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) [23]. Наразі ж відповідні обмеження реалізуються відповідно до Указу Президента Республіки Білорусь «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет» від 01.02.10 р. № 60, Декрету Президента Республіки Білорусь «Про невідкладні заходи з протидії незаконному обігу наркотиків» від 28.12.14 р. та Закону Республіки Білорусь «Про засоби масової інформації» від 17.07.08 р. [52].

У березні 2010 року 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 [51], провайдери повинні вести облік IP-адрес, а держава може витребувати інформацію щодо Інтернет-діяльності будь-якого громадянина. З 2007 року до Інтернет-кафе пред'являється вимога зберігати історію Інтернет-активності користувачів протягом одного року й інформувати виконавчі органі про підозрілі дії [23]. СОРМ працює, головним чином, відповідно до Закону «Про оперативно-розшукову діяльність» [53], Закону «Про органи державної безпеки Республіки Білорусь» [54] та Указу «Про затвердження Положення про порядок взаємодії операторів електрозв'язку з органами, що здійснюють оперативно-розшукову діяльність» № 129 [55].

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 році [37], 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 [34].

Що стосується участі Республіки Білорусь у забезпеченні кібербезпеки на регіональному рівні, слід зауважити, що Рада голів держав Співдружності Незалежних Держав (СНД) у 2013 році прийняла Концепцію співробітництва держав-членів СНД у боротьбі зі злочинами, що вчиняються з використанням інформаційних технологій [23]. Відповідно до цього документу країни-члени СНД обмінюються робочою, статистичною й методологічною інформацією та ведуть єдину базу даних щодо кіберзлочинців. На підставі цієї Концепції з 2015 року здійснюється розробка програми співробітництва між країнами СНД у боротьбі з кіберзлочинністю, яка підлягає затвердженню Радою Міністрів країн СНД. Також у 2017 р. розпочато підписання нової Угоди про

співробітництво держав-членів СНД у боротьбі зі злочинами у сфері інформаційних технологій [75].

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 УКРАЇНІ

3.1. Шляхи удосконалення інформаційної безпеки

Динаміка відносин в інформаційній сфері постійно випереджає розвиток суспільної правосвідомості, встановлені норми суспільних відносин, ускладнює створення стабільної правової регламентації. Недосконаліть нормативно-правової бази дозволяє окремим суб’єктам реалізовувати свої протиправні наміри в інформаційній сфері як щодо життєво важливих інтересів інших суб'єктів, так і об’єктів національної безпеки.

Питання забезпечення інформаційної безпеки є вкрай важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо. Окрім цього, стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, що вимагає удосконалення нормативно-правової бази забезпечення інформаційної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам в інформаційній сфері.

Зазначене вище знаходить відображення у прийнятій Стратегії Національної безпеки України [15]. У своїх положеннях вона визначила пріоритети державної політики національної безпеки, вказавши на основні її цілі, а саме: мінімізацію загроз державному суверенітету та створення умов для відновлення територіальної цілісності України у межах міжнародно-визнаного державного кордону України, гарантування мирного майбутнього України як суверенної і незалежної, демократичної, соціальної, правової держави; утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку, забезпечення інтеграції

України до Європейського Союзу та формування умов для вступу в НАТО. Крім того, Стратегія визначила як основні загрози інформаційній безпеці: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа- культури суспільства. Фактором, що послаблює здатність держави нейтралізувати загрози, є посилення взаємозалежності країн та їх відкритість до зовнішніх впливів. Здебільшого держава перестає бути монополістом на власній території, її інформаційна політика все більш обмежується, корегується, нівелюється діями інших держав, міжнародних та недержавних організацій, неформальних об'єднань негативної спрямованості, кримінальних угруповань тощо. Слабка ідеологічно, інституційно, економічно держава не здатна скористатися технологічними, економічними, соціокультурними перевагами глобалізації, проте активно переймає її негативні риси [56].

Розвиток глобальних процесів на основі всеосяжної інформатизації створює широку різноманітність інформаційних загроз – від витіснення на внутрішньому інформаційному ринку вітчизняних продуктів більш конкурентоспроможними аж до ведення цілеспрямованих інформаційних війн. Згідно з доповіддю Національної ради з розвідки США, інформаційні війни будуть домінантним фактором у нинішньому столітті. Вони вестимуться на всіх рівнях соціальної структури людства між блоками держав включно. Сучасна інформаційна революція розгортається на фоні інформаційних війн, які своєю головною метою ставлять підрив національної безпеки держав. З урахуванням таких підходів безпекова інформаційна функція держави в усіх регіонах світу набуває особливої важливості [58].

Наявна ситуація в світовому інформаційному просторі обумовлена наступним:

− більшість країн світу зіштовхнулася з проблемами кібертероризму, кіберзлочинності та іншими проблемами інформаційної безпеки;

− протягом останніх десятиліть спостерігається тенденція до поширення інформаційної агресії і насилля;

− набувають поширення агресивна реклама, спроби маніпуляції свідомістю людини, періодично проводяться інформаційно-психологічні операції;

− майже у 120 країнах світу (за оцінками американських експертів) ведуться розробки інформаційної зброї або її елементів (для порівняння – розробки зброї масового знищення здійснюються у близько 20 країнах);

− наслідки використання сучасної інформаційної зброї (згідно з висновками вчених та експертів європейських країн, України, рф і США) можуть бути зіставленими із застосуванням зброї масового ураження;

− новітні виклики і загрози в інформаційній сфері становлять реальну загрозу безпеці людства та міжнародному правопорядку [62, с. 3 – 7].

Аналіз аспектів розвитку інформаційного суспільства, інформаційної глобалізації та інформаційного протистояння в сучасних умовах загалом засвідчив наявність низки проблем організаційно-правового змісту у сфері інформаційної безпеки України, а саме:

− недосконалість державної політики з питань інформаційної безпеки: відсутність стратегічного рівня забезпечення інформаційної безпеки;

− неналежний рівень інформаційного супроводження зовнішньої та внутрішньої політики України;

− відомчу автономність державних органів та установ, на які покладено завдання забезпечення інформаційної безпеки України, дублювання їх повноважень та недостатня якість наявної координаційної складової;

− відсутність дієвих механізмів експертної оцінки інформаційної продукції, поширення якої створює загрозу інформаційній безпеці щодо прав людини, інтересам суспільства та держави;

− відсутність ефективних механізмів залучення громадськості та приватного сектору України до протидії негативним інформаційним впливам, міжнародної співпраці у цій сфері;

− наявність законодавчих та організаційних прогалин у сфері обігу інформації з обмеженим доступом.

При цьому сучасні виклики інформаційній безпеці України зумовлені як внутрішніми, так і зовнішніми чинниками:

− внутрішні – найбільшою мірою пов’язані з відсталістю інформаційних технологій в Україні від провідних країн світу, низьким рівнем інформатизації, розпорошеністю повноважень органів державної влади та законодавства в інформаційній сфері;

− зовнішні – загальносвітові тенденції створення та застосування інформаційних технологій та намаганнями іноземних суб’єктів впливати на світовий та вітчизняний інформаційний простір з метою забезпечення власних інтересів, залежність від іноземного програмного забезпечення.

Відтак, на сучасному етапі Україні слід зосередитись на двох основних напрямах:

− зробити внутрішній український простір сучасним, повноструктурним та конкурентоспроможним;

− забезпечити інформаційну присутність держави в світі та просувати її позитивний імідж.

Забезпечення національної безпеки здійснюється за умови пріоритетності національних інтересів, необхідності своєчасного вжиття заходів, адекватних характеру і масштабам загроз цим інтересам, і ґрунтується на засадах правової демократичної держави. А оскільки інформаційна безпека є частиною національної, то тут теж повинен бути пріоритет національних інтересів в інформаційній сфері.

Незважаючи на те, що на сьогодні науковцями виділяється дві складових забезпечення інформаційної безпеки – активна і пасивна (розвиток і захист) [59], у переважній більшості, система працює на протидію загрозам, тобто на пасивну складову. Проте, аналіз практики країн ЄС свідчить про те, що інформаційна безпека повинна бути побудована на моделі стратегічного мислення: вжиття заходів для захисту цілей, їх утримання й забезпечення безпеки на основі принципів демократії, прав людини, захищеного Інтернету.

Разом з тим, інформаційна безпека є невід'ємним напрямом розбудови інформаційного суспільства, розвиток якого повинен відбуватись не тільки через нарощування технологічних можливостей інформаційного обміну, але й через її глибоке усвідомлення усіма суб'єктами інформаційних відносин. Як наслідок, до проблем інформаційної безпеки на цьому етапі починають долучатися питання інформаційної етики, забезпечення приватності в умовах інформаційного суспільства, захисту від маніпулятивних інформаційних впливів тощо.

Відтак, основними напрямами державної політики з питань національної безпеки України в інформаційній сфері є:

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- активне залучення засобів масової інформації (далі – ЗМІ) до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, захист персональних даних, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність ЗМІ та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [7].

Аналіз антиукраїнських дій в інформаційному просторі вказує на те, що слід зробити акцент на збереженні національної ідентичності та популяризації

національної культури як базису не лише інформаційної безпеки України, але й загалом національної. Захист інформаційного суверенітету України виділяється як один із пріоритетних напрямів забезпечення національної безпеки. Проте законодавство не містить адекватного тлумачення зазначеного поняття, як і конкретних механізмів його забезпечення.

Так, на сьогодні взагалі відсутній механізм ефективного та швидкого блокування (обмеження доступу) ресурсів з протиправним контентом, зокрема розміщених на технічних майданчиках за кордоном, як і власне визначення шкідливого контенту.

Окрім цього, відсутній механізм запобігання та протидії поширенню інформаційної продукції антиукраїнського змісту, шляхом визначення загальних критеріїв її віднесення до заборонених для розповсюдження; визначення суб'єкта, який би виконував функцію експертного оцінювання інформаційної продукції, що містить заклики до порушення конституційного ладу, територіальної цілісності, пропаганду війни, фашизму, національної та релігійної ворожнечі.

Поряд із поняттям «інформаційний суверенітет» широко вживається «цифровий суверенітет», яке тісно пов'язане з поняттям «кібервійна», що є продовженням війни за допомогою інформаційних і комунікаційних систем, проте із двома фундаментальними відмінностями: вона не призводить до фронтального протистояння ворогуючих сторін та прямих жертв [28].

Зважаючи на низку важливих проблем, що заважають створити ефективно діючу національну систему протидії загрозам в кіберпросторі, а саме: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів іноземного виробництва, складнощі із кадровим наповненням відповідних структурних підрозділів актуальним є питання побудови системи кібернетичної безпеки.

Застарілість, складність системи охорони державної таємниці та службової інформації, створення умов для її несанкціонованого

розповсюдження, переважна «паперовість» носіїв такої інформації ставить питання щодо необхідності гармонізації інформаційного законодавства з нормами міжнародного права і правовими актами ЄС, РЄ і НАТО, що перш за все ґрунтується на невід'ємному праві доступу до інформації. І в першу чергу, саме держава має забезпечувати якісний доступ всіх категорій громадян до виробленої нею інформації, як до офіційних матеріалів, так і до роз'яснення змісту своєї власної діяльності.

Окрім цього, аналіз законодавства розвинутих країн вказує на те, що право на доступ до інформації трансформується у право на комунікацію, яке передбачає не лише право на ознайомлення з інформацією, а й право участі у її створенні. Наприклад, замість розуміння публічної інформації як такої, що «надсилається» з політичної організації або державного органу громадянам, у Норвегії її розглядають як спільно вироблену та використану з громадянами, а також групами громадян самостійно, у спосіб активних інноваційних практик відтворення різних видів доступної інформації, урядової чи ні, у нові форми публічної інформації. Водночас доступ до «старої» публічної інформації має бути настільки відкритим, наскільки це можливо, так, щоб нова публічна інформація могла створюватися та використовуватися без державного втручання, наразі «пересічний громадянин» має розглядатися як «дистриб'ютор публічної інформації» [21].

Ідея публічності відтепер реалізується через використання соціальних медіа в процесі обміну інформацією, які стали якісно новим явищем в системі горизонтальних інформаційних зв'язків та створили принципово нову ситуацію в соціальній сфері суспільства, створивши умови для організації віртуальних соціальних утворень, і їх зростаючий вплив на суспільне життя.

Відтак, пріоритетами удосконалення забезпечення інформаційної безпеки є:

– удосконалення правового забезпечення інформаційної безпеки шляхом розробки її концептуальних основ:

– визначення або уточнення завдань, функцій і повноважень суб'єктів

забезпечення інформаційної безпеки України;

− забезпечення інформаційного суверенітету України з метою недопущення інформаційної залежності та інформаційної експансії з боку інших держав чи міжнародних структур;

− сприяння розвитку міжнародного співробітництва в інформаційній сфері в умовах перегляду його принципів і механізмів, посиленню міжнародно-правової відповідальності за використання в інформаційній сфері сил і засобів, які негативно впливають або створюють загрози людині, суспільству, державі;

− зміцнення організаційних основ забезпечення інформаційної безпеки:

− вирішення питання координації діяльності суб'єктів забезпечення інформаційної безпеки, зокрема у сфері протидії інформаційній агресії, забезпечення кібернетичної безпеки України;

− налагодження системи державно-приватного партнерства у сфері забезпечення інформаційної безпеки;

− запровадження системи демократичного контролю за діяльністю державних суб'єктів забезпечення інформаційної безпеки;

− розвиток комунікаційної політики у стосунках «держава-суспільство».

Разом з тим, необхідною є розробка програм освітньо-виховного впливу, спрямованого на формування здатностей забезпечення власної інформаційної безпеки, зокрема підвищення рівня культури використання засобів оброблення інформації, оприлюднення власної інформації та способів її захисту, критичного ставлення до інформації.

Для успішного входження нашої держави в міжнародні інформаційні обміни вона має зосередитись насамперед на таких напрямах у сфері правової діяльності: розробляти систему правових актів, спрямованих на якісне збереження національних інформаційних ресурсів, їх розвиток і ефективне використання в національних інтересах; здійснювати необхідну адаптацію національного інформаційного законодавства до загальновизнаної міжнародної правової бази з метою активізації своєї участі у інформаційних обмінах; брати активну участь у міжнародній правотворчості, що має оперативно

регламентувати нові явища в сфері інформатизації; сформувати правову базу для регламентації участі у міжнародній діяльності по забезпеченню дотримання міжнародного інформаційного законодавства, боротьби з кібертероризмом та ін. видами інформаційної злочинності [30].

В умовах зростаючої активізації глобальних процесів у сучасному світі, що поряд із позитивними аспектами своїх впливів на світову спільноту створили також небезпеки інформаційної агресії, кіберзлочинності, саме загальнонаціональна система інформаційної безпеки, скоординована в своїй діяльності державою, може стати запорукою нейтралізації інформаційних загроз і використання позитивних факторів розвитку інформатизації.

Важливою складовою загальної політики забезпечення інформаційної безпеки України є підвищення участі громадськості у процесах удосконалення зв'язку «суспільство – держава». Подальше зміцнення інформаційної безпеки країни вбачається у спільних, злагоджених діях усіх державних інституцій, громадськості, медіа-спільноти [70].

В сучасних умовах необхідно вирішувати не лише такі важливі завдання, як формування власного інформаційного простору та його захисту від загроз, а й переходити від захисних стратегій до наступальних.

3.2. Засоби адміністративно-правового регулювання та державного управління забезпеченням інформаційної безпеки

Ключові напрями адміністративно-правового забезпечення інформаційної безпеки ґрунтуються на вимогах Конституції України [1], у ст. 17 якої зазначено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Під найважливішою функцією держави потрібно розуміти найважливішу функцію всіх гілок влади: законодавчої, виконавчої, судової. Забезпечення інформаційної безпеки як справи всього українського народу має включати певні види діяльності,

визначені законом, і обов'язки громадських організацій та громадян. Одним із важливих аспектів Конституції України є те (ст. 34), що кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, свободу у сфері інформації та інформаційної діяльності. При цьому встановлено, що здійснення прав і свобод може бути обмежене законом в інтересах національної безпеки та інших чітко визначених цілях.

Про необхідність формування системи забезпечення інформаційної безпеки йдеться майже з перших років незалежності України. Вживаються певні заходи. Повноваження і функції державних органів, інших інституцій країни визначені в правових актах різного рівня: Конституції України, Законах України, Указах Президента України, нормативно-правових актах Уряду України, міністерств, відомств. На подальше вдосконалення державно-управлінської діяльності спрямований кожний черговий етап адміністративної реформи. Водночас, аналіз стану та тенденцій формування і розвитку сфери, що досліджується, інформаційних складових забезпечення національної безпеки (політичної, економічної, соціально-гуманітарної, науково-технологічної, оборони і державної безпеки та інших) свідчить про те, що рівень інформаційної безпеки України наблизився до критичної межі, за якою можлива втрата здатності держави забезпечити захист власних національних інтересів, безпеки особи, суспільства і держави. Сьогодні Україна не в повній мірі готова протистояти таким небезпечним явищам як «інформаційні та інформаційно-психологічні впливи», «кібернетичні атаки», «інформаційні війни» тощо, а також до запровадження заходів інформаційної боротьби з метою протидії та послаблення дії зовнішніх і внутрішніх інформаційних загроз. Значно загострили проблеми інформаційної безпеки глобалізаційні процеси у світі, науково-технічна революція, світова фінансово-економічна криза та інші зовнішні та внутрішні чинники, які викликали докорінний переворот в інформаційному забезпеченні життєдіяльності людства.

Означене вище зумовило необхідність визначити змістовну сутність засобів адміністративно-правового забезпечення інформаційної безпеки.

Як зазначає І. Березовська [57, с. 4] Правовий аспект інформаційної безпеки має у розв'язанні цієї проблеми вирішальне значення. Чітке правове регулювання суспільних відносин в інформаційній сфері забезпечує створення в суспільстві стабільного правового порядку, а також системи органів, інститутів, установ, здатних за допомогою адміністративно-правових засобів забезпечити захист й охорону від порушень прав, свобод і законних інтересів громадян та інших осіб, закріплених чинними нормами права.

З цього приводу, одним з найважливіших напрямів підвищення правового рівня забезпечення інформаційної безпеки в Україні є вдосконалення системи адміністративно-правових засобів у цій галузі. Адміністративно-правове регулювання у сфері інформаційної безпеки виступає невід'ємною складовою сучасної системи управління на шляху до правової держави. Сьогодні Україні потрібні діючі інструменти державного управління у сфері інформаційної безпеки, основними засобами якого є адміністративні заходи впливу контролюючих органів публічної влади і передбачена законом відповідальність за порушення законодавства у сфері інформаційної безпеки [57, с. 5].

За таких обставин існування значних недоліків та суперечностей у законодавчій регламентації основних параметрів інформаційної безпеки, протиріччя та прогалини у правозастосовній практиці в цій сфері ускладнюють процес впровадження у життєдіяльність нашого суспільства правових норм та інституцій, притаманних сучасному цивілізованому світу.

На думку А. Малько правові засоби є правовими явищами, які виявляються в інструментах встановлення суб'єктивних прав, обов'язків, пільг, заборон, заохочування, нагородження та діями, пов'язаними з технологією реалізації прав і обов'язків [57, с. 326].

В. Колпаков до засобів, які містять у собі адміністративно-правовий метод регулювання відносить приписи, заборони, дозволи.

Приписи – покладання прямого юридичного зобов'язання чинити ті чи інші дії в умовах, які передбачені правовою нормою. Заборони – покладання прямих юридичних обов'язків не чинити тих чи інших дій в умовах,

передбачених правовою нормою. Дозволи – юридичний дозвіл чинити в умовах, передбачених нормою, ті чи інші дії, або утримуватися від їх вчинення за своїм бажанням [57, с. 56 – 57].

І. Березовська виділяє такі групи адміністративно-правових засобів: дозвільні; реєстраційні; адміністративно-правового примусу.

Таким чином, змістовна сутність адміністративно-правових засобів правового регулювання та державного управління має розглядатися як сукупність правових механізмів та прийомів і способів встановлення і реалізації владних повноважень державними органами всіх гілок влади, спрямованих на забезпечення інформаційної безпеки особи, суспільства, держави. При цьому доцільно нагадати, що ми розглядаємо систему адміністративно-правового регулювання та державного управління в широкому розумінні змістовної сутності забезпечення інформаційної безпеки. Такий підхід передбачає застосування як загальнонаукових, так і спеціальних юридичних засобів. На наш погляд правове регулювання щодо системи державного управління, саме діяльність органів державної влади, має спиратися на довіру і підтримку народу України, що передбачає врахування зворотних зв’язків, тобто впливу громадян, їх об’єднань на формування і реалізацію державної внутрішньої і зовнішньої політики.

Політичні засоби мають сприяти вирішенню наступних проблем.

По-перше. Забезпечення реального волевиявлення народу України, як єдиного джерела влади, що здійснюється через вибори, референдум та інші форми безпосередньої демократії. Вирішення цих питань залежатиме від впровадження ефективних політико-правових, адміністративно-правових засобів регулювання правовідносин у цій сфері.

По-друге. Забезпечення цивілізованої політичної боротьби, які включають застосування брудних прийомів, способів дій опонентів (політичних партій, громадських організацій) у процесі виборчих кампаній, та в діяльності законодавчої гілки влади.

По-третє. Врахування у процесі формування внутрішньої і зовнішньої політики, в тому числі інформаційної безпеки та державного управління у цій сфері позитивних пропозицій і вимог політичних партій, громадських організацій, протестних акцій (мітингів, демонстрацій, пропагандистських кампаній тощо), які відповідають інтересам переважної більшості населення і підтримуються ним.

Ідеологічні засоби є важливими стосовно об'єднання народу навколо загальнонаціональної ідеї. Конституцією України (ст. 15) встановлено, що суспільне життя в Україні ґрунтується на засадах політичної, економічної та ідеологічної багатоманітності, що жодна ідеологія не може визнаватися державою як обов'язкова.

Слушними з цих питань є висновки Ю. Тодики, який пише: «До завдань науки належить вивчення ідейно-тематичної спрямованості нормативних актів, їх значення для державотворчого процесу. Без цього немає й аналізу ефективності цих актів, їх відповідності міжнародно-правовим стандартам, напрямам розвитку держави і суспільства. Конституційне закріплення ідеологічної і політичної багатоманітності – це теж ідеологія держави, шлях відходу від ідеологічного монополізму колишніх часів. ...саме конституційне право може закріпити у своїх приписах загальнонаціональну ідею, яка б об'єднувала, а не роз'єднувала український народ [57, с. 40 – 41].

Ми підтримуємо позицію Ю. Тодики і вважаємо, що національна ідея має бути визначена окремою статтею Конституції України в розділі «Загальні засади» і бути базовою основою засад як адміністративного права, так і державного управління у сфері забезпечення інформаційної безпеки.

Соціальні засоби, які випливають із змістовної сутності соціального управління. На думку В. Колпакова найбільш послідовне врахування характеристик соціального управління, специфіки керуючого впливу знаходить вияв у його поділі на такі два основних види: державне управління, де суб'єктом виступає держава в особі відповідних структур; громадське управління, де суб'єктами є недержавні утворення [57, с. 14].

У системі державного управління у державах, у тому числі, що орієнтуються на демократичні цінності, переважає застосування засобів соціально-владного та примусового характеру. Водночас державна політика та управлінська діяльність щодо її реалізації передбачають застосування засобів, спрямованих на підвищення рівня життя населення, охорони здоров'я і праці, освіти тощо. Високі соціальні стандарти життя людини і громадянина є однією із найважливіших умов довіри до владних структур, підвищення активності та відповідальності громадських інституцій щодо захисту національних інтересів.

В умовах будівництва демократичної, соціальної, правової держави та формування громадянського суспільства зростатиме роль виконавчих комітетів районних, міських, сільських і селищних рад, яким розширюється делегування повноважень; громадських рад та різного напряму самоуправлінських, консультативно-дорадчих структур тощо, діяльність яких здійснюється на добровільних морально-організаційних засадах.

Взаємодія державного і громадянського управління є однією з найважливіших умов соціально-економічного розвитку, державного будівництва та забезпечення інформаційної безпеки особи, суспільства, держави.

Інформаційні засоби – це засоби державної інформаційної політики, що спрямовані на забезпечення державної внутрішньої і зовнішньої політики інформаційної безпеки, а саме:

− формування у населення позитивного сприйняття напрямів, заходів і цілей державної політики інформаційної безпеки;

− викриття внутрішніх і зовнішніх джерел негативних інформаційних та інформаційно-психологічних впливів, що застосовуються проти України та відповідна їх правова оцінка на підставі як правових норм чинного законодавства, так і норм міжнародного права;

− координація діяльності інформаційних підрозділів і служб усіх гілок влади про інформування власного населення та світової спільноти щодо державної політики у сфері, що досліджується, та узгодження оцінок подій і

процесів у цій сфері.

Технологічні засоби – це сукупність організаційних, організаційно-технічних, інженерно-технічних, криптографічних, спеціальних засобів, спрямованих на формування і ефективне функціонування правового режиму системи забезпечення інформаційної безпеки.

Сукупність технологічних засобів, які доцільно застосовувати, залежатиме від напрямів забезпечення інформаційної безпеки, а саме:

− забезпечення безпеки функціонування усіх елементів (об’єктів і суб’єктів) національного інформаційного простору;

− забезпечення інформаційної безпеки у політичній, економічній, оборонній, державної безпеки і правопорядку, соціально-гуманітарній, науково-технологічній, екологічній, власне інформаційній сферах;

− створення системи охорони та технічного захисту інформації, віднесеної до державної таємниці та іншої інформації обмеженого доступу;

− виявлення інформаційних, інформаційно-психологічних впливів на особу, громадські і державні інституції, кібератак, застосування проти України інформаційної зброї та протидії і нейтралізації джерел внутрішніх і зовнішніх загроз.

Засоби кадрового забезпечення – це сукупність способів і прийомів вивчення і розстановки кадрів на посадах в органах державно-управлінської діяльності з урахуванням їх моральних якостей та професійного рівня. Система кадрового забезпечення передбачає створення ефективно діючої сукупності навчальних засобів, спеціальних програм підготовки кадрів для різного рівня державного управління та напрямів забезпечення інформаційної безпеки.

Засоби матеріально-технічного та фінансового забезпечення – це економічні засоби створення необхідних умов формування і функціонування державної системи забезпечення інформаційної безпеки, діяльності усіх гілок влади і місцевого самоврядування, їх спеціальних підрозділів і служб, що виконують відповідні функції у цій сфері та застосування заходів, засобів і сил інформаційного протистояння з метою захисту національних інтересів.

В умовах глобалізаційних інформаційних процесів, загострення інформаційної боротьби у сучасному світі, розширення спектру інформаційних загроз зумовлює необхідність застосування Україні всього комплексу засобів адміністративно-правового регулювання та державного управління у сфері забезпечення інформаційної безпеки.

Вважаємо, що реалізація владних повноважень суб'єктами державно-управлінської діяльності має опиратися на довіру і підтримку народу, як найважливіший фактор узгодженості дій суб'єктів України у сфері, що досліджується. Врахування 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.

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. В Україні упродовж останніх років напрацьовано низку законодавчих актів, які регулюють відносини, що виникають в інформаційній сфері, зокрема щодо забезпечення інформаційної безпеки держави. Однак, доводиться констатувати, що в сучасних умовах розвитку суспільства інформаційне законодавство потребує якісних змін. За всієї його розгалуженості воно залишається суперечливим, належним чином не систематизованим і не кодифікованим. Цілковито підтримуємо думку вчених про необхідність розроблення та прийняття Інформаційного кодексу. Водночас погоджуємось з тим, що розроблення національної правової бази, її гармонізація з міжнародними інституціями, тобто приведення відносин у сфері інформації у відповідність до міжнародних стандартів сприятиме зміцненню інформаційної безпеки України та підвищенню її міжнародного авторитету як демократичної і правової держави.

3. 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.

4. Встановлено наявність низки проблем організаційно-правового змісту у сфері інформаційної безпеки України, а саме:

− недосконалість державної політики з питань інформаційної безпеки: відсутність стратегічного рівня забезпечення інформаційної безпеки;

− неналежний рівень інформаційного супроводження зовнішньої та внутрішньої політики України;

− відомчу автономність державних органів та установ, на які покладено завдання забезпечення інформаційної безпеки України, дублювання їх повноважень та недостатня якість наявної координаційної складової;

− відсутність дієвих механізмів експертної оцінки інформаційної продукції, поширення якої створює загрозу інформаційній безпеці щодо прав людини, інтересам суспільства та держави;

− відсутність ефективних механізмів залучення громадськості та приватного сектору України до протидії негативним інформаційним впливам, міжнародної співпраці у цій сфері;

− наявність законодавчих та організаційних прогалин у сфері обігу інформації з обмеженим доступом.

Інформаційне суспільство може існувати тільки тоді, коли його члени оволодіють інформаційною культурою – будуть додержуватись етичних норм поведінки в інформаційному просторі. Це сформує інформаційний щит кожної людини та суспільства у цілому. Формування інформаційного середовища не у відповідності з глобальними законами функціонування природних систем може наблизити критичну ситуацію на планеті не менш, ніж ядерна загроза. Інформація вже стала стратегічним озброєнням. Тому кожна людина мусить знати, що коли вона вносить нову інформацію в інформаційний простір, вона тим самим керує формуванням інформаційного середовища решти людей, тобто безпосередньо впливає на їх свідомість та розвиток. Кожен новий блок інформації, який надходить в інформаційне середовище людства, повинен мати

правила безпечного користування. Таким чином, інформація може безпосередньо впливати на організм людини, змінювати її фізіологічний стан. Це якісні та кількісні характеристики інформації. Є ще глобальні характеристики інформаційного середовища, які визначаються тим, наскільки формування цього середовища відповідає загальним законам та закономірностям. Як окрема людина, так і суспільство у цілому має можливість запобігати інформаційних небезпек завдяки формуванню інформаційного щита: системи цінностей, яка орієнтована на глобальні принципи безпеки життєдіяльності людства.

5. Досліджено основні шляхи удосконалення інформаційної безпеки, серед яких є: удосконалення правового забезпечення інформаційної безпеки шляхом розробки її концептуальних основ; визначення або уточнення завдань, функцій і повноважень суб'єктів забезпечення інформаційної безпеки України; забезпечення інформаційного суверенітету України з метою недопущення інформаційної залежності та інформаційної експансії з боку інших держав чи міжнародних структур; сприяння розвитку міжнародного співробітництва в інформаційній сфері в умовах перегляду його принципів і механізмів, посиленню міжнародно-правової відповідальності за використання в інформаційній сфері сил і засобів, які негативно впливають або створюють загрози людині, суспільству, державі; зміцнення організаційних основ забезпечення інформаційної безпеки; вирішення питання координації діяльності суб'єктів забезпечення інформаційної безпеки, зокрема у сфері протидії інформаційній агресії, забезпечення кібернетичної безпеки України; налагодження системи державно-приватного партнерства у сфері забезпечення інформаційної безпеки; запровадження системи демократичного контролю за діяльністю державних суб'єктів забезпечення інформаційної безпеки; розвиток комунікаційної політики у стосунках «держава-суспільство».

В сучасних умовах необхідно вирішувати не лише такі важливі завдання, як формування власного інформаційного простору та його захисту від загроз, а й переходити від захисних стратегій до наступальних.

6. Окреслено засоби удосконалення адміністративно-правового регулювання та державного управління забезпеченням інформаційної безпеки, серед яких: правові засоби, політичні, ідеологічні, інформаційні, соціальні, технологічні, засоби кадрового забезпечення, засоби матеріально-технічного та фінансового забезпечення.

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. 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: 17.09.2022).

2. Про доступ до публічної інформації : закон України від 13.01.2011 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.

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

4. 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.

5. 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: 17.09.2022).

6. Про оборону України : закон України від 11.05.2007 р. № 1014-V. URL : www.zakon.rada.gov.ua/laws/show/1932-12 (дата звернення: 17.09.2022).

7. Про основи національної безпеки України : закон України від 19.06.2003 р. № 964-IV. *Відомості Верховної Ради України*. 2003. № 39. Ст. 351

8. 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.

9. Про телекомунікації : закон України від 01.11.2003 р. № 1280-IV. *Відомості Верховної Ради України.* 2004. № 12. Ст. 155.

10. 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: 10.10.2022).

11. 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: 15.09.2022).

12. 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: 17.09.2022).

13. Про рішення Ради національної безпеки і оборони України : указ Президента України від 21.03.2008 р. «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» від 23.04.2008 р. № 377/2008. *Відомості Верховної Ради*. 2008. № 4. Ст. 102.

14. Про стратегію національної безпеки України : указ Президента України від 12.02.2007 р. № 105/2007. *Урядовий кур'єр.* 2007. 7 берез. С. 4.

15. Стратегія національної безпеки України : указ Президента України від 26.05.2015 р. № 287/2015. URL : www.president.gov.ua (дата звернення: 17.09.2022).

16. Про Концепцію (основи державної політики) національної безпеки України : постанова Верховної Ради України від 18.07.1995 р. № 532-95-п (із змінами, внесеними згідно з Постановою КМ № 1849 (1849-98-п) від 23.11.1998 р.). *Відомості Верховної Ради України.* 1997. № 10. Ст. 85.

17. Лісовська Ю. П. Адміністративно-правове забезпечення інформаційної безпеки в Україні : автореф. дис. ... канд. юрид. наук : 12.00.07 ; Міжрегіон. акад. упр. персоналом. Київ., 2017. 19 с.

18. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ : Нац. акад. СБУ, 2018. 408 с.

19. Андреев В. І. Основи інформаційної безпеки / за ред. проф. В. О. Хорошка. вид., доп. і перероб. Київ : Вид. ДУІКТ, 2009. 292 с.

20. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи. Київ : ВД «СофтПрес», 2005. 316 с.

21. Баровська А. Інституційне забезпечення державної комунікативної політики : досвід країн Європи : аналітична доповідь. URL : www.niss.gov.ua /articles/1730 (дата звернення: 23.10.2022).

22. Беззубов Д. О. Суспільна безпека (організаційно-правові засади забезпечення) : монографія. Київ : «МП Леся», 2013. 425 с.

23. Беларусь : Национальный ИКТ-профайл. (Информационная безопасность и защита информации). URL : www.digital.report/belarus-informatsionnaya-bezopasnost (дата звернення: 17.11.2022).

24. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту : дис. канд. політ. наук : 23.00.04 Київ., 2018. 210 с.

25. В Евросоюзе приняли новый закон о защите данных. URL : www.threatpost.ru/v-evrosoyuze-prinyali-novyj-zakon-o-zashhite-dannyh/15749 (дата звернення: 17.10.2022).

26. Відбулось перше засідання Експертної Ради з розробки концепції інформаційної безпеки та з питань розвитку інформаційного простору. URL : www.kmu.gov.ua/kontral/uk/pullish/ article (дата звернення: 17.10.2022).

27. Галушко С. Інформаційна безпека України. URL : www.utz.tv/ telepzogramiutz/euroukraina/item/21953.html (дата звернення: 17.09.2022).

28. Горовий В. М. Правові перспективи національного розвитку. URL : www.uaforeignaffairs.com/ua/ekspertna-dumka/view/article (дата звернення: 17.10.2022).

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

30. Довгань О. Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації. *Правова інформатика.* 2013. № 4(40). С. 79 – 88.

31. 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: 17.09.2022).

32. Інформаційна безпека. URL : www.ukr.vipreshebnik.ru/entsiklopedia /55-i/1943-informatsija-bezpeka.html (дата звернення: 15.11.2022).

33. Інформаційна безпека держави: підручник. В. М. Петрик, М. М. Присяжнюк, Д. С. Мельник ; в 2т. / за заг. ред. В. В. Остроухова. Київ : ДНУ «Книжкова палата України», 2016. Т. 2. 328 с.

34. Інформаційна безпека. Практикум. В. М. Ахрамович., В. В. Козлов ; Націон. акад. статистики, обліку та аудиту. Київ : ДП «Інформ.-аналіт. агентство», 2018. 340 с. іл. Бібліограф. : 337 с.

35. Інформаційна безпека України: стан та перспективи розвитку. Я. Й. Малик. *Ефективність державного управління*. 2015. Вип. 44 (1). С. 13 – 20.

36. 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.

37. Конвенція про кіберзлочинність від 23 листопада 2001 року. URL : www.zakon5.rada.gov.ua/laws/show/994_575 (дата звернення: 17.09.2022).

38. Концепция сотрудничества государств-участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий : утверждена Решением Совета глав государств СНГ от 25 октября 2013 года. URL : www.e-cis.info/page.php?id=23808 (дата звернення: 17.09.2022).

39. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література, 2003. − 472 с.

40. Кравець Є. А. Інформаційна безпека держави. Юридична енциклопедія : в 6 т. Київ : Укр. енцикл., 1992. С. 744.

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

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

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

44. Марущак А. І. Інформаційне право. Доступ до інформації : навч. посіб. Київ, 2007. 280 с.

45. Медвідь Ф. Інформаційна безпека України: Виклики та Загрози. URL : www.nato.ru.if.ua/journal/2009-2-28.pdf (дата звернення: 17.09.2022).

46. Медвідь Ф. М. Інформаційна безпека України в системі національної безпеки. Модернізація України: проблеми та технології успішності (питання економіки, права, соціології, освіти і культури) : матеріали Всеукр. наук.-практ. конф., 12 листопада 2015 р. / редкол. : А. М. Подоляка (голова) та ін. Київ : ДП «Видавничий дім «Персонал», 2015. С. 194 – 199.

47. Молдова: Национальный ИКТ-профайл. (Информационная безопасность и защита информации). URL : www.digital.report/moldova-informatsionnaya-bezopasnost (дата звернення: 17.10.2022).

48. 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.

49. Нікішина Я. Інформаційне забезпечення політики європейської інтеграції України. Вироблення державної політики. Аналітичні записки. Київ : ІІС, 2003. С. 237.

50. О европейских критических инфраструктурах и мерах по их защите : Директива 2008/114/ЕС Европейского парламента и Совета Європы от 08 декабря 2008 года. URL : www.docs.pravo.ru/document/view/32671965 (дата звернення: 05.11.2022).

51. О мерах по совершенствованию использования национального сегмента сети Интернет : указ Президента Республики Беларусь от 1 февраля 2010 г. № 60. URL : www.pravo.by/document (дата звернення: 10.10.2022).

52. О признании утратившим силу постановления Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства

связи и информатизации Республики Беларусь от 29 июня 2010 года № 4/11 : постановление Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 г. № 7/7. URL : www.pravo.by/upload/docs/op/T21503058_1424811600.pdf (дата звернення: 10.10.2022).

53. Об оперативно-розыскной деятельности : закон Республики Беларусь от 15 июля 2015 г. № 307-З. URL : www.kgb.by/ru/zakon289-3 (дата звернення: 11.10.2022).

54. Об органах государственной безопасности Республики Беларусь : закон Республики Беларусь от 10 июля 2012 г. № 390-З. URL : www.kgb.by/ru/zakon390-3 (дата звернення: 12.10.2022).

55. Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность : указ Президента Республики Беларусь от 3 марта 2010 г. № 129. URL : www.oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm (дата звернення: 15.10.2022).

56. Олійник О. В. Стан забезпечення інформаційної безпеки в Україні. *Юридичний вісник.* 2014. № 2(31). С. 59 – 65.

57. Олійник О. В. Адміністративно-правові засоби забезпечення інформаційної безпеки. *Юридичний вісник. Повітряне і космічне право.* 2015. № 1. С. 65 – 69.

58. Онищенко О. С. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища : монографія ; НАН України, Національна бібліотекака України ім. В. І. Вернадського. Київ, 2014. 426 с.

59. Панченко В. М. Співвідношення понять: інформаційна та кібернетична безпека / В. М. Панченко. Інформаційна безпека людини, суспільства, держави. 2013. № 2 (12). С. 20 – 24.

60. Персональные данные: новые правила в Европейском Союзе. URL : www.habrahabr.ru/post/300348 (дата звернення: 17.11.2022).

61. Петрик В. Щодо визначення інформаційної безпеки та її різновидів. Форми та методи забезпечення інформаційної безпеки держави : зб. матер. міжнар. наук.-практ. конф. (м. Київ, 13 березня 2008 р.). Київ : Видавець Захаренко В. О., 2008. 216 с.

62. Пилипчук В. Г. Системні правові проблеми формування інформаційного суспільства. Інформаційне суспільство і держава : проблеми взаємодії на сучасному етапі : зб. наук. ст. та тез ; наукове повідомлення за матеріалами міжнародної науково-практичної конференції (Харків, 26 жовтня 2012 р.). Х. : НДІ державного будівництва та місцевого самоврядування, 2012. 214 с.

63. Питання концепції реформування інформаційного законодавства України / Р. Калюжний, В. Гавловський, В. Цимбалюк, М. Гуцалюк. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : зб. Київ : НТУУ КПІ, Міносвіти і науки України, СБУ, 2000. С. 17 – 21.

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

65. Правове забезпечення інформаційної діяльності в Україні / за заг. ред. Ю. С. Шемшученка, І. С. Чижа. Київ : ТОВ «Юридична думка», 2006. 384 с.

66. 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: 18.11.2022).

67. 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: 25.10.2022).

68. 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: 26.11.2022).

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

70. Солодка О. М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право.* 2015. № 3. С. 36 – 42.

71. 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: 17.11.2022).

72. Стан та перспективи реформування сектору безпеки і оборони України : матеріали міжнарод. наук. –практ. конф. (24 листопада 2017 року) : у 2 т. Київ : Національна академія прокуратури України, 2017. Т. 1. 476 с.

73. Стан та перспективи соціальної безпеки в Україні: експертні оцінки : монографія / О. Ф. Новікова, О. Г. Сидорчук, О. В. Панькова та ін. / Львівський регіональний інститут державного управління НАДУ ; НАН України, Інститут економіки промисловості. Київ ; Львів : ЛРІДУ НАДУ, 2018. 184 с.

74. Степко О. М. Аналіз головних складових інформаційної безпеки держави. Інститут міжнародних відносин Національного авіаційного університету. 2011. URL : www.nbuv.gov.ua/portal/Soc_Gum/Nvimvnau/2011_1/ 83-92.pdf (дата звернення: 25.10.2022).

75. Страны СНГ будут сотрудничать в борьбе с киберпреступностью. URL : www.ritmeurasia.org/news-2017-08-28--strany-sng-budut-sotrudnichat-v-borbe-s-kiberprestu pnostu-32043 (дата звернення: 25.10.2022).

76. 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: 25.10.2022).

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

78. NATO Bucharest Summit Declaration, 3 April 2008. URL : www.nato.int/docu/pr/2008/p08-049e.html/ (Last accessed: 11.11.2022).

79. North Atlantic Treaty Organization. Active Engagement/ Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. URL : www.nato.int/lisbon2010/strategic–concept–2010–eng.pdf/ (Last accessed: 11.11.2022).